Concepts for IT security of the future

The way to innovative, transparent and effective security

swisscom

Publishing details
© November 2015
Published by: Swisscom Ltd
Author: Group Security
Editorial team: René Mosbacher, NASKA GmbH
Graphic: Petra Balmer, Bern

1	**About this publication**	3
2	**Trends in the economy**	5
2.1	Consumerisation of IT	5
2.2	Big data	6
2.3	Internet of Things	7
2.4	Decentralised development	8
2.5	Globalisation versus return to independent services	9
3	**Trends in private use**	11
3.1	Always on, sensors everywhere	11
4	**The threat landscape**	13
4.1	Actors	13
4.1.1	Vandals	14
4.1.2	(Organised) crime	15
4.1.3	Hacktivists	15
4.1.4	Terrorists	16
4.1.5	Secret services	16
4.2	What can we expect next?	17
4.3	Summary	18
5	**Security principles**	19
5.1	Good security practice must be implemented	19
5.2	Security is the next business driver	20
5.3	We are constantly under attack	21
5.4	Intelligence is the basis of detection	21
6	**The security organisation's areas of activity**	23
6.1	Basic principles	23
6.2	Prevention	24
6.3	Detection	24
6.4	Intervention	25
7	**What does this mean for a company?**	27
7.1	The security culture	27
7.2	The security organisation as co-pilot	35
7.3	Strategic management	39
7.3.1	Risk management	39
7.3.2	The Security business year	40
7.4	Organisational matters	43
8	**What does this mean for technology?**	49
8.1	Data-centric security	49
8.2	The Collaborative Security Model	51
8.3	Threat intelligence	54
8.4	Maturity model	55
9	**The role of the state**	59
	Appendix	61
	Threat radar	63
	Abbreviations and specialist terms	65
	Index of keywords	68

Foreword

When it comes to security – whether in the digital or the real world – we face the problem of how to safeguard certain desirable features, particularly in the presence of a potentially invisible attacker who is intent on hampering those very features. Since ancient times, individuals and societies have needed security. For generations we have learnt to identify hazards in the real world and take action to avert them.

The world of today also has many assets, which we must protect in order to guarantee the smooth running of our society. With the ever-growing influence on our society from digital communication and the Internet of Things, we are increasingly facing new hazards – mainly because the attackers can now also wreak havoc from afar.

Thankfully, great progress has been made in security research and its numerous applications. Not only has the research-based knowledge about security concepts increased, but the application-oriented areas have also established the issue of IT security as a focal topic. This development is largely due to many incidents – some of them serious – for industry and private users. In recent years there has been a productive environment for developing security solutions and putting them into practice.

Many fundamental concepts of IT security are explained in detail in this book. Actual ideas and models, which we can use to improve our current security, have been developed by Swisscom and set out in this book. I hope that you will be able to use many of these concepts in your business and privately.

Enjoy your read!

Prof. Adrian Perrig
Network Security Group, ETH Zurich

1 About this publication

With its transformation from telephone company to supplier of IT and communication solutions, security has become a central task for Swisscom in recent years. We have kept abreast of this by highlighting the profile of the security organisation within the company and by investing greatly in this area.

Security has become the cornerstone for implementing our guiding principles, vision and promise to our customers. However, it is not simply a matter of being secure, trustworthy or reliable. We also want to look at the issue creatively in order to come up with new and innovative solutions for the company.

This publication is intended, firstly, to provide interested parties with a concise overview of the general state and concepts of IT security. Secondly, it aims to show how we approach the subject and what experience has taught us. Some of the concepts and measures described are generic and can also be implemented in other companies. We also use case studies to show the thinking behind the various solutions and how effective they have turned out to be.

Choice of terminology

For the sake of simplicity we have used the term “company” to describe all organisations for which IT security might be relevant. The operational aspects of security we have named “security” and the organisational unit responsible for security is called the “security organisation”.

2 Trends in the economy

During the last five to ten years, the economy has experienced various trends which have an impact on ICT security. For example, before the first smartphones appeared it was clear that IT – and IT alone – provided the necessary resources for working with data. It was also clear that access to company data was cut off as soon as you leave the office. This has now changed dramatically.

2.1 Consumerisation of IT

In the beginning, it had to be possible to access the company infrastructure at the request of the management board, even from outside. This put many IT departments in a difficult position – but who would really want to hold out against the wishes of senior management? And so the "consumerisation of IT" was born, a trend we know today as "Bring your own Device (BYOD)".

The requirement to use a private device to work in the company network soon worked its way down through the hierarchies. Various companies have now made this into a virtue, by generally allowing their employees to bring their own devices into the office. In extreme cases this applies not only to smartphones, but to the whole range of processor-reinforced, network-ready devices up to and including the notebook.

If the concept continues to spin out, in future we will see companies giving their employees a budget instead of IT equipment. However, there are currently still legal hurdles to be overcome: for example, it would be necessary to regulate the division of investment and operating costs between the parties. It would also be necessary to find solutions in advance in the event of devices being lost or needing repair. However, it is clear from the trend that the longer BYOD continues, the more the user becomes the CIO. This means that he defines the IT strategy for his company. This will of course also have a significant effect on IT security – but more on that later.

At Swisscom, the use of private devices has been officially permitted for some time and is even encouraged. The Any Device strategy was approved by the Board of Directors, which means that every employee had the opportunity either to receive an official device, or to use their own.

On the basis of this decision, the IT infrastructure has also started to align itself accordingly. Since access to the internal company network is denied to Any Devices for security reasons, the necessary services are made available via the Internet. This does however place additional demands on security, for example in terms of authentication or encryption.

2.2 Big Data

The fact that various business processes generate a lot of data is not new. There is likewise nothing new in the consideration given to the business models that are based on it. Added to this, however, is the opportunity of processing these huge quantities of data effectively and efficiently.

The use of big-data analysis throws the issue of data protection into the front line. The same rules apply here in principle as for “normal” databases, and even the concept of anonymisation is actually not a new one. The real problem – which has existed even since the early days of data warehouses – is data correlation.

Studies have shown that – particularly when data in motion is involved – a maximum of four data points are sufficient to enable them to be traced back quite clearly to one person. There are already some good approaches that allow data to be effectively anonymised. What matters, however, is clear governance and strict controls, to ensure that the data is not open to abuse. Therefore, what we have to deal with here – as is so often the case – is not a technical task, but a procedural and, ultimately, an ethical one. Moderate and responsible handling is therefore essential for Big Data.

2.3 Internet of Things

Increasingly, it is not only people that are connected over the Internet, but machines as well. This is not new in itself. The industry has been automating and linking its systems for decades, resulting in what we now know as machine-to-machine communication. Unfortunately, networked devices are developed mainly to work as efficiently as possible – with (data) security often playing only a subordinate role.

Even while they are operating, networked devices are treated more as part of the building and not necessarily as part of a larger network. It is therefore not surprising that such devices can often be controlled on the Internet entirely without authentication or using standard user names and passwords. This means that anyone who wants can, for example, easily capture the air conditioning system from "outside" and manipulate it at will. This is of course a fatal shortcoming at premises where the temperature is important (for example in computer centres).

Furthermore, commercial software requiring regular maintenance runs on most such devices. This is state-of-the-art in IT systems – for production systems, however, patch management has remained a foreign word in many places. Even worse: Some manufacturers of industrial systems prevent the maintenance of system software by the operator, by threatening them with the loss of their warranty. This in turn results in security loopholes, which can be relatively easy to exploit.

Similar problems arise if there are large differences between the lifecycles of mechanical and electrical components. Industrial machines are often designed to be used for ten to 20 years, but are developed on the basis of standard software. Unfortunately, the life expectancy of such software is only about ten years. After that, the manufacturers rarely continue to supply security patches.

Yet this is just the start of the trend. In connection with the energy reform, there is now also the demand for more home automation. The concept: automated building technology is expected to reduce energy consumption. That is an excellent idea provided security is planned in from the start. Otherwise, we run the risk that our heating system or the power supply can be manipulated from the outside – either maliciously or through negligence.

2.4 Decentralised development

The governance of software development was and is still centralised in most companies. This means that the process by which the business moves from idea to solution is strictly prescribed and closely managed. This makes life easier for a security organisation (and many other central services), since it will sooner or later be involved in the project anyway. Under these circumstances it is sufficient to support the standard development process and thereby to influence the necessary security measures.

Recently, however, companies have been increasingly converting to decentralised development. This enables them to evolve more closely to the business, with small, efficient teams. This works more quickly and has the advantage, in the most fatuitous case, of failing quickly and with lower costs. This trend is therefore worth supporting – it puts governance before completely new challenges. In such conditions, line management must assume far more responsibility. Yet they need help for this from the security organisation. They must provide answers to how company risks can be sensibly managed in such circumstances. More on this in section 7.2.

Local or distributed development is actively encouraged at Swisscom. This creates new challenges for those involved: firstly, the divisions have to take over a responsibility they never had in the centralised structure. They are suddenly responsible not only for implementing the content, but also for ensuring quality and security. At Swisscom many technical aspects are governed by clearly defined interfaces (APIs).

From the security perspective, this means that it must always be clear who owns the risk, and that the security organisation must be closely related to the business. For more on the organisational aspects see section 7.4.

2.5 Globalisation versus return to independent services

The trend towards global sourcing was and is undeniable. It started with the outsourcing of development to India, and later to Eastern Europe. This trend has reached a provisional peak with outsourcing to the cloud. The aim was clearly to reduce costs.

What is not so clear, however, is where the journey will end. Here the industry is moving along a fine line between cost reduction and security requirements, and the unclear international legal situation is unsettled by this (keyword Patriot Act). And the revelations surrounding the activities of messaging services leave many feeling increasingly uncomfortable when it comes to moving ideas, data or services abroad. So it should not be surprising if different countries are tending to focus their regulations more and move towards local data storage. These developments are certainly still continuing.

3 Trends in private use

3.1 Always on, sensors everywhere

As far as private use is concerned, in recent years a permanent online connection with the network has become widespread. We have grown accustomed to having the information we need available at any time. This is certainly an exciting development, which opens up many possibilities. Yet at the same time it is also a worrying one, when it becomes clear to us which data tracks we leave behind us on the Internet and the affect this has on our privacy. We also need to ask which processes continue to operate if this "always on" functionality were to be lost.

Our life is increasingly measured by an armada of sensors. This is most obvious in the case of all the devices that record and transmit certain physical functions of sick or elderly people for medical purposes. Such sensors can be very helpful, for example by enabling elderly people to live in their familiar surroundings for longer. If the state of a person's health is monitored at home, it is possible for example for an alarm to be triggered or a doctor called automatically if a bodily function reaches a critical level.

It would need to be clear to most users of fitness apps that their activity status and location are being recorded and transmitted to a server somewhere in the world. However, the fact that many other ostensibly innocent-looking apps are continuously gathering data about us and our behaviour, is far less well-known.

This does of course immediately raise questions about data protection and the preservation of our privacy. We should also ask ourselves how far such systems – for example through personalised advertising or tips – are able to influence or even manipulate our behaviour.

4 The threat landscape

To understand the development of the threat landscape, it is first necessary to explain the background. Essentially, the role of the Internet has increased greatly in recent years. As regards the security aspect: originally the network was often used by hackers to sell software and “toolkits”. Such programs can be used to exploit known weaknesses on computers. Since the hacker tools provide pre-designed malicious functions, they enable attackers to compromise systems, even if they have no in-depth technical knowledge. Such tools may therefore be behind almost each and every attack.

These corresponding tools were and are sold via relevant websites, often via the Darknet. However, a veritable underground market has arisen on these sites in the last few years, In the meantime, services such as the targeted attacking of specific systems or organisations are offered as well as attack software. Anyone who wants can also place instructions to send spam e-mails, and much more. This underground market is theoretically open to anyone who has a networked computer, some criminal energy and the necessary cash.

4.1 Actors

The attackers can be divided into different groups. First it is necessary to differentiate between those that act opportunistically, and those that carry out targeted attacks. The more opportunistic actors, such as script kiddies, can be assumed to seek out the weakest victims. Against such actors, it often helps simply to be “better” than other companies. Then, in most cases, the business model will not be worthwhile for attackers. To put it another way, the costs for an attack must be correspondingly high. Basic working protection can certainly help here.

The situation is different with actors that target their attacks. They set out to achieve a specific aim, which they pursue resolutely and, if necessary, using great personal and financial resources. with the use of substantial human and financial resources. It is becoming far more difficult and expensive to protect against such actors. Let's take a closer look at various examples of this type.

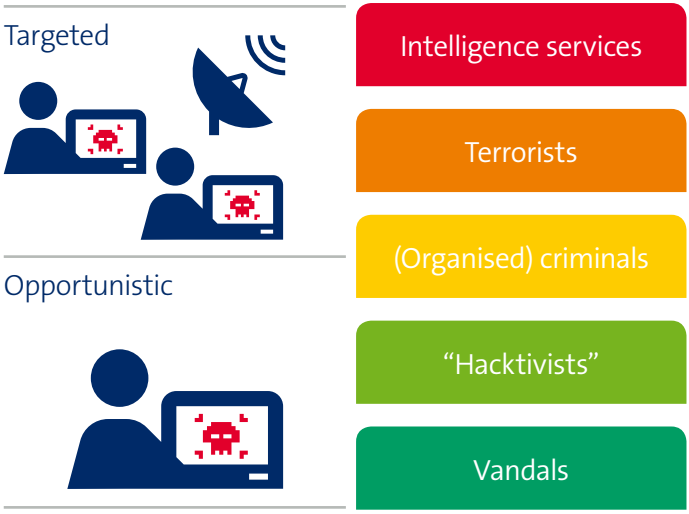


Fig. 1: The attackers and their methods shown in order of the effort and costs involved in protecting against their activities, with the lowest at the bottom.

4.1.1 Vandals

Digital vandals often have very little fundamental knowledge. They regard attacks on an infrastructure as something of a sporting challenge and use software and instructions they find on the Internet for this purpose. They use malicious software without any detailed understanding of how it works.

In the early days of the Internet, vandalism – mainly by young people – was one of the greatest threats. The basic protection mechanisms were non-existent or had not been rolled out then. Nowadays, vandals should no longer present a significant problem. Their attacks would very probably bounce off a well-maintained infrastructure – yet the risks from vandals should not be completely ignored, however.

The key issue as far as vandals are concerned, is which tools will be available to them in the future. Will they soon find resources on the Internet that are currently still the preserve of professional attackers? If so, they could once again become far more dangerous.

4.1.2 (Organised) crime

Crime always moves with the money. It is therefore logical that, with the ongoing commercialisation of the Internet, criminals will also turn up on it. Whether through fraud or theft – as long as there is money to be had, criminals will be there to wreak their havoc.

The criminals have continued to make massive technological and conceptual advances in recent years. Whereas they used to appear as individual perpetrators, these days we are more frequently faced with loosely associated gangs. They are found on underground markets and work on projects together. A criminal's reputation on the scene is important currency in this environment. The gangs look for members with the right profile. Technical skills are also in demand, such as the services of fencers, by means of which stolen data or credit card numbers can be sold. However, criminal organisations that operate according to a real hierarchy are still quite rare in the virtual world.

Cybercriminals have also clearly become more professional in recent years. One reason for this is the reduced costs and wider availability of powerful IT. In these circumstances our aim must be to drive up the costs for the criminals so far that their "business case" no longer adds up. However, to do this we must remain constantly on the ball, because the criminals themselves are also constantly upgrading their technology and improving their methods of attack.

4.1.3 Hacktivists

Hacktivists are a more recent phenomenon. In the last few years, spectacular campaigns by groups such as Lulsec and Anonymous have shown that they are a force to be reckoned with. They are able to recruit highly competent individuals, who manage time and again to paralyse entire infrastructures, or at least cause them serious problems. Their main motivation in this is to make a political or ideological point.

We must always assume that at least some of the people who are paid for their services on the above-mentioned underground markets. The hacktivists themselves, however, have neither the financial means, nor the need, to purchase services underground.

4.1.4 Terrorists

Opinion in the industry is divided when it comes to terrorism. Some believe that terrorists have no interest in attacking ICT infrastructures, since they use the Internet as a communication medium and recruiting channel. Others point out that it is precisely through targeted attacks on the ICT infrastructure that greater damage can be caused to the western world than by other means. This is countered by the idea that today's terrorists depend on maximum media impact. However, attacks on ICT do not have the same media impact as the attack on life and limb, for example. Furthermore, news of an attack on the critical ICT infrastructure can sometimes no longer be distributed, because the communication channels no longer work.

Until recently, it was assumed that terrorists lacked the expertise to carry out a successful attack on the ICT infrastructure, and they wouldn't be able to build it up quickly, either. However, this is no longer necessary because they can simply buy in the knowledge with sufficient cash. What's more, various governments have started to create military cyber units which can also lead attacks. If those units were to be affected by redundancies at some point, well trained experts would suddenly arrive on the market, who might possibly offer their knowledge underground.

4.1.5 Secret services

Targeted attacks by secret services have increased massively in recent years. Even if the news reports often convey a different picture, it should be made clear that such attacks come from all over the world. Whether secret services act aggressively depends on how they are organised in their countries. Depending on the legal basis, they are intended to protect the state only, or with the addition of the national economy – in other words, operate industrial espionage.

Governments that use their intelligence services for industrial espionage are currently a problem which needs to be taken very seriously. Their espionage organisations have the means and the opportunity to plan and carry out attacks over the long term using highly qualified staff. They are also able to compromise ICT products more or less as soon as they leave the factory. The company's IT department then purchases vulnerabilities and back doors together with the devices, without even realising.

A network that is compromised in this way can then be used for espionage and sabotage. And because different countries are building up offensive organisations for “cyber war”, we must assume that they will also use these opportunities in case of doubt. However, this is currently only supposition, but we must keep such scenarios in mind and assume that the threat is continuing to grow.

4.2 What can we expect next?

To assess the threat landscape, it is also necessary to observe the threat trends as well as the actors. A good aid for this are so-called threat radars, as they have been developed along the lines of national security services for assessing situations. Details of how a threat radar is built and what it means can be found in the Annex. The main trends that need to be monitored at present are explained briefly below.

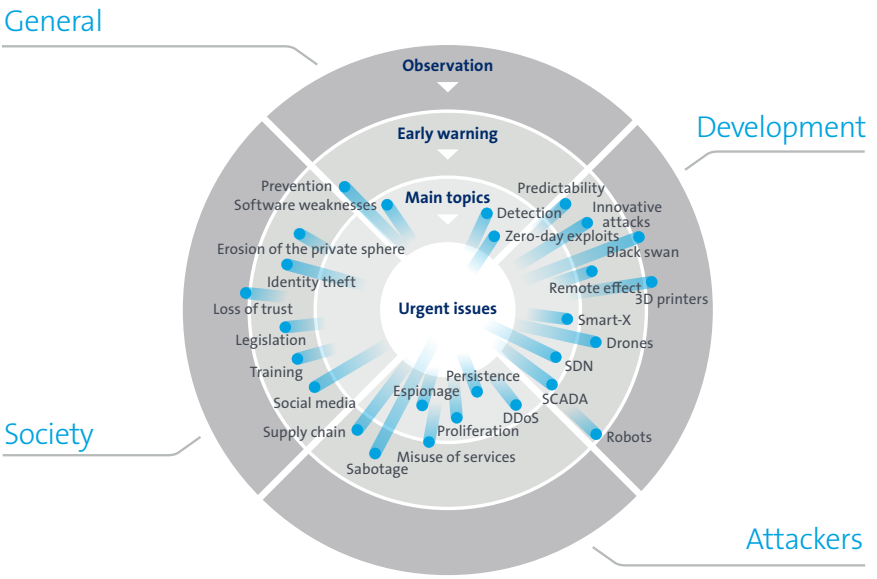


Fig. 2: The threat radar provides information about the development of the various threat types and channels.

4.3 Summary

Crime: We do not expect the number of criminally motivated attacks to increase substantially in the next few years. As already mentioned, criminal forces will also gain access to tools and attack techniques that previously were only available to well-trained organisations with a budget to match. Consequently, we must also prepare ourselves for more complex attacks. It is also clear that criminal organisations are taking more time over an attack, so that they can cause even greater damage. The attacks are becoming more professional.

Targeted attacks: We must therefore assume that targeted attacks are on the increase. These include attacks that aim to harm a particular organisation. We can also expect that such attacks will be more unexpected and will combine methods that could not previously be combined. Targeted attacks will therefore be more difficult to predict in the future.

Internet of Things: The Internet of Things offers enormous potential for automation – but also for attacks. The vulnerability of widely used software libraries is suddenly affecting not "only" traditional computers, but "things", such as cars, refrigerators or televisions. Only in rare cases are the manufacturers of such products involved in the life cycle of the device software. They are therefore also unable to respond quickly to critical vulnerabilities. If such weaknesses are present in different components, the potential for damage is enormous.

5 Security principles

In view of the above, we can derive four principles which should be used as the basis for any security strategy.

5.1 Good security practice must be implemented

Any new and ground-breaking ideas with regard to security must be based on solid and stable operational foundations. It therefore makes sense to implement and maintain traditional good security practice. This includes meeting a broad range of requirements, such as

- a stable and practised policy framework with corresponding security governance
- a stable and practical risk management system
- an organisation that aims for integrated security
- operational processes such as patch management, identity management, incident management
- training, awareness and communication
- secure software development

Further requirements may be added to this list, depending on infrastructure and organisation.

These issues are covered in their entire extent by the usual security frameworks. With ISO 27001, these tasks can also be certified by external companies. However, please note that this standard must be regarded as only the first step towards achieving a stable basis. After all, security is an ongoing process.

5.2 Security is the next business driver

Security organisations were originally created to protect a company's assets. There is no doubt that this continues to be one of their main tasks – but it is not the only one. For too long, security organisations have worked on the basic principle that security is necessary and compliance is the greatest good. Yet they have overlooked the fact that the measures and concepts needed in order to achieve this were – and often still are – regarded as something of a necessary evil by many managers.

All too frequently, security organisations still play on the full gamut of catastrophe scenarios. They argue that bad things will happen unless you invest sufficiently. Even if this is indeed the case, few budget managers will be happy to talk about the necessary funds.

Anyone who adopts this viewpoint forgets that the term "ICT security" can have quite positive connotations. What's needed is a good dose of positivity. For example, it is worth pointing out that adequate IT security merely lays the foundations for working from home or BYOD. Or the argument could be made to the management that it is thanks to security that the risks of strategic decisions suddenly become transparent. This turns security into an enabler, and the chief security officer into a partner.

However, it requires new approaches on the part of the security specialists. Above all, they must move away from extrinsic and towards intrinsic security. The former case is where attempts are made to build security around insecure products. In the latter case, products are built safely securely from the outset. In extremely distributed systems, such as the Internet of Things, the second approach is clearly the more practical one for the purpose of guaranteeing security.

We have learned that business and budget managers are far from reluctant to spend money on security. However, they do so not because the security organisation demands it, but because they understand that it is necessary in order to meet planned objectives. It is pivotal that the security organisation acts as a partner in this, whilst at the same time showing why it thinks what it is thinking. A shared understanding of the threat landscape is an important starting point in this.

5.3 We are constantly under attack

It is true to say that networks are constantly under attack these days. What has changed, is the nature of the attacks. There was a time when you could still expect company networks and company computers to be clean and trustworthy. Today, however, we must assume that criminal elements or third countries have already compromised the supply chain. Furthermore, it would be unwise – given the quantity and complexity of the attacks – to assume that it would be possible to defend successfully against all of them. It is therefore advisable to construct an architecture as if the internal network were already compromised.

5.4 Intelligence is the basis of detection

Anyone who accepts the limits of prevention knows how important it is to reinforce detection and intervention accordingly. The aim should be for these two areas to operate in a way that is unpredictable to outsiders. Attackers must not know what awaits them. It is therefore necessary to pursue new paths, especially in the gathering of data for intelligence and also in detection.

Yet that is still not enough: clearly, it is not sufficient just to detect attacks – the company must also be in a position to respond to them. This in turn impacts on the technology (our own ideas on this are described in section 8.2). And, of course, this also has consequences for the processes and cooperation of the divisions (more on this in section 8.3).

6 The security organisation's areas of activity

A safety organisation's sphere of influence extends across the fields of basic principles, prevention, detection and intervention. We will look at each area in detail below, and show what is possible and feasible in a normal case. The information is by no means exhaustive – further points may be added or some points may not apply, depending on the infrastructure and the company.

*Fig. 3: **The security organisation's four areas of influence.***

6.1 Basic principles

By basic principles we mean the foundations upon which the further areas are built. It is therefore clear that the basic principles must function in a stable and reliable fashion. This mainly involves the basic protection standards, the processes and the technology that form "good security practice".

6.2 Prevention

The benefits of prevention are quite obvious, as it is there that the security organisation feels at home. Depending on the requirements, it is necessary here to take measures involving staff, technology and processes.

Here are some typical examples of this area:
> Training and improving awareness: what do the staff have to know or be able to do?
> Continuity management: how can we ensure that the business continues to function even in the event of an IT loss?
> Resilience (outage protection): this means ensuring that the system will continue to function even if a component fails or has been compromised.
> Security risk management: often confused with risk reporting. The aim is not (only) to identify risks, but also to actively manage them.
> Other, depending on organisation and infrastructure.

6.3 Detection

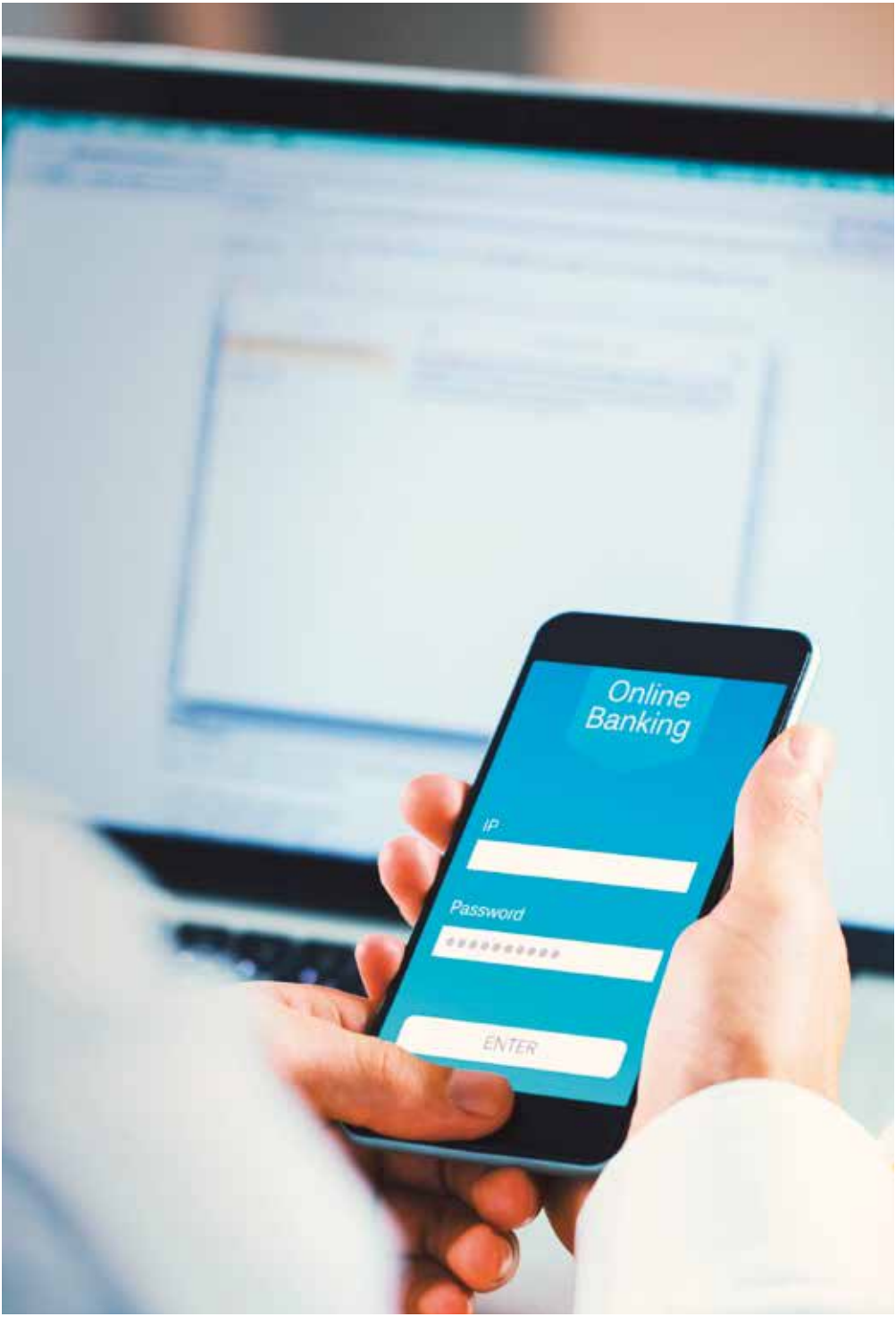
We have already found that prevention has its limits. These may be technical, financial or structural in nature. In extreme cases, for example, a criminal can gain access to the network simply by bribing an employee. We must also concede that we will experience successful attacks. The object of detection is to identify the attacks at an early stage.

Typical measures for this would include:
> Data Leakage Prevention: this includes the detection (and prevention) of unwanted data leakage.
> Security Information & Event Management (SIEM): this means correlating system events in order to detect attacks. Later we shall see that SIEM currently has its limits – which means that the next point is particularly important.
> Threat Intelligence: gathers information on a broad basis and evaluates it in order to detect attacks at an early stage.
> Honeynet: this is a network which is not commercially used but which appears productive from the outside. As soon as traffic appears on it, it means an attack is probably in progress.
> Data exchange with third parties.
> Other, depending on organisation and infrastructure.

6.4 Intervention

Unfortunately, companies often invest a lot of time and money in detection, and then do not know how they intend to react when an incident occurs. For the intervention to work, however, it must be fast, efficient and effective, while interfering with the business as little as possible.

Intervention is primarily (but of course not only) a matter of defining processes. As a general principle, the intervention processes must be documented and also put into practice. Following a serious incident the reproducibility of the steps taken may also be important, so that the incident can be subsequently analysed. Experience shows that this is not a strength of the parties involved.


Online
Banking
IP
Password
ENTER

7 What does this mean for a company?

Once we have looked at the action areas and possibilities of security, the question arises of what it means for a company to put a modern security concept into practice. This can be discussed on the basis of three sub-areas:

> what does this mean for the security culture?
> how can security be strategically controlled?
> what does this mean for the security organisation?

At Swisscom, trust in our employees is a key value, which is also put into practice accordingly. It forms the basis upon which security is built, since it requires that employees should fundamentally wish to act in the interests of the company and the customers.

The security organisation has the task of constructively supporting this behaviour. It helps employees to fulfil their responsibilities efficiently and securely. It is also crucial to avoid punishing the majority for the misconduct of a minority, following an incident. Our security culture also demands close monitoring for the really critical information. And it also requires that any misconduct is punished promptly and effectively.

7.1 The security culture

Above all, a company that wishes to reinforce its (data) security in the long term requires a corresponding security culture. In order to establish such a culture, it must be remembered that security is primarily intended to help people, not hinder them. The security organisation should be perceived as a companion, which communicates risks transparently and effectively supports the business at the same time. In this way the security organisation becomes a partner that helps people to carry out their work securely. In such a culture, security is able gradually to become established as a central concept in the activities of the employees.

Of course, we are still a long way from that situation in reality. Today, if someone talks about IT security, all too often they mean the conditioning of employees. Training, raising awareness and communication are doubtless important tasks that are worth safeguarding. However, they are only part of the whole story. If a security organisation is viewed primarily as the company police, it is hardly surprising that it is always the first port of call when an incident has already occurred. It would be better to see it as a service provider, as this would do away with much of the resistance and misunderstanding from the start. However, this often requires a complete overhaul of the security organisation's own perspectives and ways of working. In other words, its culture must be adapted from within.

Human-centred security

A concept such as the one described above can be summarised under the term human-centred security. This is where the security organisation takes on the role of an internal service provider which works and mediates in all directions (Fig. 4). Its duties can essentially be divided into two areas: providing the basic security functions and carrying out security projects.

Fig. 4: Concept of human-centred security. The co-pilot represents the tasks of the security organisation.

The basic security functions

The basic security functions include the fundamental tasks and processes of the security organisation. What matters is that the traditional elements such as security policies and governance, training, awareness and communication are also placed alongside a solid and implemented risk-management practice. Otherwise, the security organisation runs the risk that decisions will be made in other areas (mainly in projects) that could lead to unacceptable risks and hazards. The way to avoid this is outlined in section 7.2.

As important as these basic functions are, they often consist of highly standardised processes which are to be handled as efficiently and cost-effectively as possible. Many functions have a standardised input, clear tasks and a standardised output. They are therefore ideal for processes which are to be optimised and automated as far as possible. This applies in particular for process steps which do not generate any real value – e.g. those in which information is simply copied from one spreadsheet to another.

Last but not least, such processes should also be measured and managed. At first glance this is relatively simple, and it can, should and will form part of a score card for the security and the processes. The measured variable here is the Key Security Indicator (KSI). In contrast to operational Key Performance Indicators (KPIs), this relates solely to security. Every company must find its own measured variables for the KSI and define them as a score card. What is really difficult here is obtaining meaningful variables from operations that are also recognised by the management.

At Swisscom the main processes are defined by procedures. We have decided not to record broad and complex processes, but to focus here on the normal case. A procedure takes up no more than one A4 sheet and typically shows the five to eight most important steps. Each of these steps is categorised according to RASCI (Responsible, Accountable, Supportive, Consulted, Informed), with the responsibilities also being clearly defined. The objectives as well as the input and output are also stated.

These procedures have proved to be a highly efficient instrument. A procedure can be defined in a workshop within 30 to 60 minutes at most. At the same time, this helps the teams to clarify the processes for themselves. It is also necessary here to define measured variables that enable the efficiency of the process to be measured and controlled. We have now written around 30 such procedures. This approach enables us to improve the efficiency of certain processes, sometimes by a factor of three to four. This has enabled us to free up capacity so that we can carry out other, often more interesting, tasks.

Projects

The security organisation should support projects efficiently and purposefully from the start. This is the only way to guarantee that it is involved at an early stage and can help find solutions to the problems of the business. Yet this is where it must depart from pure compliance work. It does not create a positive culture if it simply tells those involved what rules they must comply with at the start of the project, and reappears at the end to check that they have done so.

This may be sufficient for projects with a low security risk, or those in which "standard security" is enough. For all other projects, however, this is the wrong approach. After all, a division starts a project in order to solve a problem or tap into a new business area. A security organisation that sees itself as a service provider will help the division to achieve these goals – and, in doing so, will of course also act as guardian of security.

Such an approach can be encouraged, for example, by forming small, cross-divisional teams within the security organisation These teams then work on the project independently and are measured according to its success. If the main security roles are represented in such a team – governance, architecture, physical security, monitoring – decisions can be made on the spot. This means that, if necessary, assistance can be provided to the project quickly. However, to ensure that such decisions are made in the overall context and that no unacceptable risks are taken, a solid and stable risk management system is required.

In day-to-day business, it has been found that the cross-divisional teams occasionally have trouble with their dual role. The balancing act of representing governance within the project on the one hand and participating in the content on the other, can lead to issues of identity. In this case the system needs to be designed so that it is transparent, but also offers specific guidance.

So much for the main roles in a security organisation. There are, of course, many interfaces in connection with this which must be defined and observed. We shall describe the main ones briefly below.

What the management needs

In many executive committees and boards, it is now accepted that security is a matter for the most senior management levels. But how should these bodies control security? Basically, the answer is relatively simple: by using an instrument which they also use in normal day-to-day business: risk management. Yet that is precisely where the difficulty often lies. The security organisation often makes life unnecessarily difficult for the management, by projecting an unnecessary degree of complexity and importance onto this topic.

Risks are frequently overestimated by security organisations. A large proportion of the risks processed daily scarcely reach the magnitude that merits their being referred to the company's senior management - and rightly so. Often, risks are not even reported at the appropriate level. Before the monthly report is written for the company management, it is first necessary to ask what risks are really relevant for it. Then it is a matter of placing the consequences of security incidents in this context. Of course, there are risks that absolutely must be communicated up to CEO level, but these are (hopefully) usually fewer than you think. In this case, quality trumps quality.

A further sensitive issue is the question of the projected, financial effects of a security risk. There are different formulas and approaches for quantifying risks. Provided these do not also involve financial figures, they can deliver quite useful results. Formulas can help to prioritise risks. However, if you attempt to calculate only the financial damage from an actual incident, you will founder. For example, it is impossible to put a price on loss of trust and therefore loss of customers. If this cannot be done in the case of a real incident, how then should it be possible for a “mere” risk? Unfortunately, people still sometimes attempt to lend virtually more importance to security. Usually, however, the result is the exact opposite, because the security organisation loses trust as a result and from then on the management no longer sees it as a partner on an equal footing.

In summary: the security organisation should communicate risks to the management clearly, openly and transparently, without dramatising them. This is the only way that the divisions can assume their responsibility in matters of security.

Partners

A security organisation has various partners – internal and external. For the external ones in particular, it is necessary to communicate the risk tolerance, the structures and the culture within the company.

At Swisscom we endeavour to keep the number of partners to a reasonable level, but this is to build closer relationships with them. This enables the partners to understand how we operate our company and what the rules of play are here. This makes cooperation easier for advisory functions and is also particularly useful for audits. In this environment we often wish to obtain an external opinion, and that demands a close relationship. We may even go as far as forming joint ventures.

It is of course different for internal partners. Besides the business, depending on whether it is viewed more as a customer than as a partner, development and operations are the main stakeholders. They are ultimately essential, if security is to be effectively implemented. Nor should the security organisation operate while pointing the finger, but should actively create added value. We may safely assume that nobody knowingly builds and/or operates insecure environments. However, if the business does not understand the requirements or the security organisation misjudges the problems of operation or development, it is difficult for a genuine partnership to be created. Also needed are good communication, empathy and consistent risk management.

We vehemently endeavour to find solutions jointly with the business, development and operations. There are clearly requirements here which cannot be negotiated. These include those specified by law or by contracts, and also those that are simply a matter of good security practice. In these latter cases the position is clear, and the security organisation feels responsible and at home. In all other cases, however, there are negotiable grey areas. These should also be used in the search for creative solutions. However, it is necessary for the risk owner to understand the risk and be able to accept it, and for the security organisation to be in agreement.

A typical example is patch management. Even at Swisscom there is a conflict between the security organisation ("We have to roll out this patch immediately, because the vulnerability is highly critical!") and the operation ("Never touch a running system!"). In such cases, efforts are made to find solutions jointly, based on the objective Common Vulnerability Scoring System (CVSS). Three areas are transparently evaluated in CVSS:

Base: describes the basic metrics of a vulnerability and its impact on the availability, integrity and confidentiality of a system.

Temporal: includes metrics that can change over time (for example the quality and availability of malware), but are independent of the company and are therefore universally valid.

Environmental: describes the vulnerability in the context of the company. This division allows the security organisation to determine the first two parameters. The third is ideally handled by operations. This means it is possible, efficiently and on the basis of an objective evaluation system, to decide jointly whether a patch needs to be rolled out quickly or can be integrated at the next, regular release cycle.

Our experience shows that this approach often results in practical solutions, which are sustainable and acceptable for all involved. In particular, it is a way of creating comprehensible transparency, where previously risks were overestimated or underestimated. What matters, however, is that the question of whether a risk is acceptable is answered at the right management level. The security organisation must really be able to justify it.

Customers

The customers – regardless of whether they are internal or external – should always be at the forefront as far the security organisation is concerned. Particularly in the ICT industry, this also includes customers from its own company, who are somehow affected by security. This applies even if they have nothing to do with the security organisation itself. There are, of course, other stakeholders – especially in the area of critical infrastructures, for example, the population has a strong interest in professionally implemented security.

Customers are also always people. We should make it possible for them to solve their problems easily, purposefully and securely. It is therefore important that security matters are transparent and easy to grasp. In fact, how the information is protected should not concern the users – it should just happen.

A typical problem, familiar to many companies, occurs when confidential information is exchanged via Dropbox, Box, OneDrive, etc. The employees do not use such services with any ill intent, but for lack of any alternatives. If a security organisation is to get to grips with this, it must ask itself how employees can transfer large files to external suppliers and partners easily and reliably. What sort of files are they? Should the company provide its own user-friendly option, or can it buy in a solution?

If the security organisation adopts such an attitude when tackling the problem, it will gain much in terms of transparency. It also quickly becomes clear where the risks really lie: just because a policy prohibits the use of Dropbox and similar services, this does not mean that everyone obeys it. The only thing that is achieved by this, is that the security organisation quickly has someone to blame in a crisis…

One aim of Swisscom's security organisation is to organise security in such a way that it is as user-friendly as possible. For example, a simple, streamlined and practical policy on BYOD is being developed with this in mind. Once this policy is adopted, the security organisation will think very hard about how to put it to the employees in simple terms. For example, how can the policy be designed so that it is fun to read?

In addition, we are also looking for a technology, which – for example – greatly simplifies authentication and encryption for the users. If we are able to solve these two problems, we will also be able to address the risks sustainably for BYOD. Section 8.1 shows how we intend to approach this.

7.2 The security organisation as co-pilot

Based on the above, we can now derive the role of the security organisation in a company. The overriding principle here is that the security organisation must develop in a constant, systematic and targeted way to ensure that the firm places adequate importance on security.

The core activity of the divisions is to develop business strategy. The security organisation, meanwhile, is tasked with supporting the divisions in the implementation of this strategy and keeping risks at an acceptable level. To put it another way, the business decides the flight path and destination of the plane, while the security organisation ensures that the biggest thunderstorms and mountains are given a sensibly wide berth. To do this, it must of course know where these thunderstorms and mountains are.

*Fig. 5: **The security organisation helps the plane negotiate thunderstorms and mountains safely.***

Policy and governance

Security traditionally focused very clearly on policies and compliance. Guidelines were drawn up and implemented based on good practice, then checks were made to try and determine how closely these were adhered to. The security organisation was therefore seen as a kind of police force within the company. The experts knew that policies were often difficult to understand and therefore also difficult to comply with. They were also aware that policies occasionally prevented employees from carrying out their work, but for a long time no better alternatives were offered.

Today, we know that while policies and governance are certainly key aspects of security, they have to strike the right balance between security requirements and business needs. In this context, it is vital to perform good, solid work in partnership with the divisions and the other units within the security organisation.

Monitoring and review

A company should essentially live a culture that requires its employees to behave in a correct and loyal manner. This culture of trust should also be reflected in the security strategy, of course without naively putting one's faith solely in people's inherent goodness.

Just as in air travel, the security organisation must continually monitor operations and projects and identify any deviations. As such they must be represented in steering committees, especially those for projects, and play an active role with regard to reaching milestones and checkpoints.

Fig. 6: The security organisation must continually monitor operations and projects and identify any deviations.

In projects
Create solutions, not problems

Areas
Security officers are strategic partners

Fig. 7: A security officer should be able to identify with the objectives of the business.

Customer support

Policies provide the framework, while monitoring reveals breaches of guidelines. During all this, appropriate customer support (internal and external) by the security organisation ensures that missteps are avoided wherever possible. Successful customer support requires consultants and security officers who provide added value for customers. For example, this means that they identify with the projects and are interested in bringing them to successful and secure completion. Security consultants should therefore feel that they are jointly responsible for the success of the project.

The same applies to security officers, whose aim must be to enable the business, as the customer, to achieve its objectives in a secure way. As a result, security officers are also measured by the business success of their unit.

Security – the place to be

All this can only become a reality if the security organisation has the right employees on board. They must be motivated to travel along a common path and share a common conviction. A framework has to be put in place making the security organisation "the place to be" for top people.

There are a number of ways to achieve this. First and foremost, the security organisation should be located as high as possible within the company hierarchy and independent of operations. It can then convey the image that is is genuinely able to make a difference. This difference should then be communicated via suitable showcases – both internally and externally. One such showcase is regular security or risk management reporting for customers and partners. Within the company, security bulletins or regular meetings with management or the Board of Directors help shed a favourable light on the security organisation. It goes without saying that it always operates with the latest knowledge and technology, but this fact also needs to be communicated in an appropriate form.

Always keeping an eye on the big picture

It should also be noted at this point that however well a security task is executed, it will have only limited impact in isolation. Regardless of whether it relates to policy and compliance, monitoring and review, project management, training or other areas, a measure only become fully effective in combination with others. The security eco-system can only be lived through a collective approach. Once everyone has taken that on board the security organisation can deliver continuous improvement and contribute to a company's overall success.

7.3 Strategic management

Security should be managed at two levels. Firstly through the strategic use of risk management, and secondly through structured planning.

7.3.1 Risk management

Experience has shown that on paper risk management is simple. In principle the processes are clear and can also be precisely defined in theoretical terms. Unfortunately, however, the theory is often caught up by practice. Risks are seldom easy to identify, and their impact can hardly be assessed with any degree of reliability.

But what is the actual aim of risk management? Fundamentally, it should enable a company to identify and actively manage its biggest risks. The potential financial implications are secondary. It would clearly be interesting to compare the relative monetary cost of risks and security measures. In a culture in which risks are communicated transparently and managed actively, however, complex operational considerations are of little benefit in any case. Qualitative scenarios that realistically demonstrate what actually could happen and under what conditions are much more important.

The key element is the process that defines how risks are dealt with. The role of the security organisation is to be aware of the threat landscape and develop corresponding scenarios that allow risks to be identified and assessed. The divisions, for their part, bear the majority of the risks and must also fund the measures taken to reduce them.

It is important that decisions are taken at the correct management level as to which risks are deemed acceptable and which are not. The correct level is generally that of the person who, in the event of an incident, will have to explain to the customer why the incident occurred. Ideally, therefore, senior management will be involved in larger-scale projects. If this takes place as part of a constant dialogue, a very constructive process can result.

7.3.2 The Security business year

Planning in the security organisation should follow the business planning cycle. Fig. 8 shows how this might look at a high abstraction level.

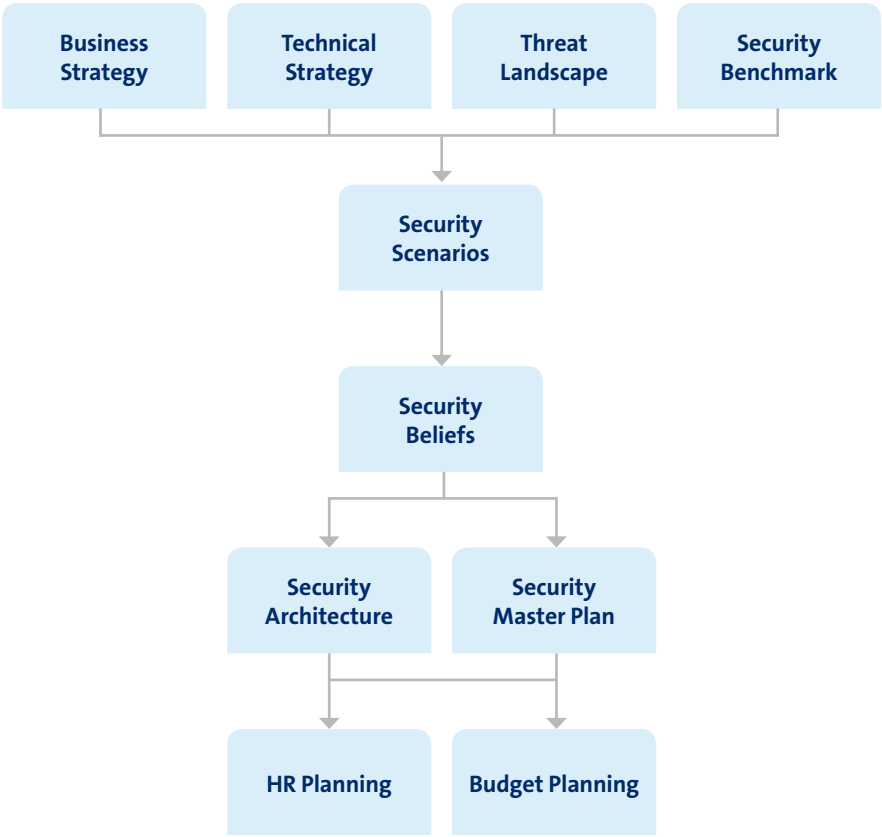


Fig. 8: How planning in a security organisation might look if coupled with business planning.

At the start of the planning process, companies consider their strategy and planning for the next few years. This must also form the basis for security organisation planning, given that it is intended to support the business. The security organisation should also be in a position to create a sound base for the business in respect of IT. In some cases this may require preliminary structural or architectural work to be carried out. The same obviously applies for the technical strategy or architectural vision, which serve as the basis for security.

From the threat landscape…

The threat landscape must be clearly defined and realistic. It must also include statements on future developments, as business planning is placed in this context and business strategies are protected in this environment. When communicating the threat landscape, the security organisation should use clear, simple images that are understood by the business and by management. It is important to operate on the basis that the threat landscape is the same across the whole company and draw up uniform plans. It is also clear, however, that events may call everything into question again and make corrections necessary.

A benchmark for evaluating the security situation would of course be very useful. Unfortunately there is very little material on the market that could serve as a valid basis for neutral and objective evaluation. Nevertheless, we should attempt to develop a suitable benchmark based on existing concepts. The most interesting ones are the ISF Benchmark and the ISF Healthcheck.

…through scenarios…

Building on this preliminary work, scenarios can be developed that offer hypotheses as to how the world might look in the future. Since it is impossible to make any definite statements, it is worthwhile considering various scenarios. This makes it easier to understand how the security organisation can support the business successfully under different conditions.

The principles – referred to as beliefs – for the company are derived from these scenarios. The question of what needs to be taken into account and under what conditions an architecture and an implementation plan should be established can then be answered.

...to the security architecture

Now things finally get serious. Based on the information above, a company's security architecture can be revised (or established for the first time). It shows what must be done for the company (and also the security organisation) to be successful in the various scenarios. It also provides information on the most cost-effective way to implement the beliefs. The same applies for the masterplan, which sets out the situation in broad terms with scenarios and beliefs, demonstrating which projects and tasks need to be implemented in order to further the architecture and rectify any deficiencies identified (from the benchmark) without threatening the strengths.

It goes without saying that the budget can be derived from this. It is interesting, however, that the discussion over how much a company wants to spend on security is now much easier to manage. The background is now very clear and can be communicated transparently. The parties involved are informed in comprehensible terms where and why things need to be done.

One thing many firms overlook is strategic HR planning. The master plan and architecture provide a good basis for determining what know-how will be required in the future and how urgently, and where investment and divestment activity should be targeted.

Once the described planning process has been completed, everything starts again from the beginning. This procedure allows companies to manage security in a structured and strategic way and adopt a proactive approach. It is crucial that the security organisation is already incorporated into the business strategy. However, it primarily performs a listening role. The main aim is not to influence strategy (although it can highlight risks where necessary). Rather, it is an opportunity for the security organisation to learn what contribution it can make towards helping the business achieve its objectives. With this kind of basic ethos in place, you are often knocking on an already open door.

7.4 Organisational matters

The various ideas and concepts of course influence security organisations themselves and their integration into the organisation. Two principles have to be observed:

1. Security is a management issue. It cannot be delegated and must be located at the highest level. This is the only way to guarantee that top management receives unfiltered information and allow security to be fully effective. And ultimately, this concept also ensures that the CEO and their colleagues on the Executive Board are able to fulfil their duty of care.

2. Integrated security is the key to success. An integrated security concept can be implemented more easily if the various tasks such as policies, governance, physical security, architecture and the CSIRT are brought together under one roof. In this way, unconventional solutions can also be sought in which logical measures can if necessary compensate for physical weaknesses – or vice versa.

Of course, this approach also entails weaknesses and risks. If all security functions are brought together at top management level, for example, there is a danger that the security organisation could construct an ivory tower for itself. This has to be taken into account.

At Swisscom, the CEO decided that security is of strategic importance. With this in mind, he integrated the Chief Security Officer – referred to at Swisscom as the Head of Group Security – into his own organisation. This position was subsequently recreated and filled. It was originally assumed that the associated organisation would be small and would focus predominantly on policy and governance tasks. Over the course of discussions, however, the benefits of a central organisation became increasingly clear, with the result that security was eventually centralised directly with the CEO.

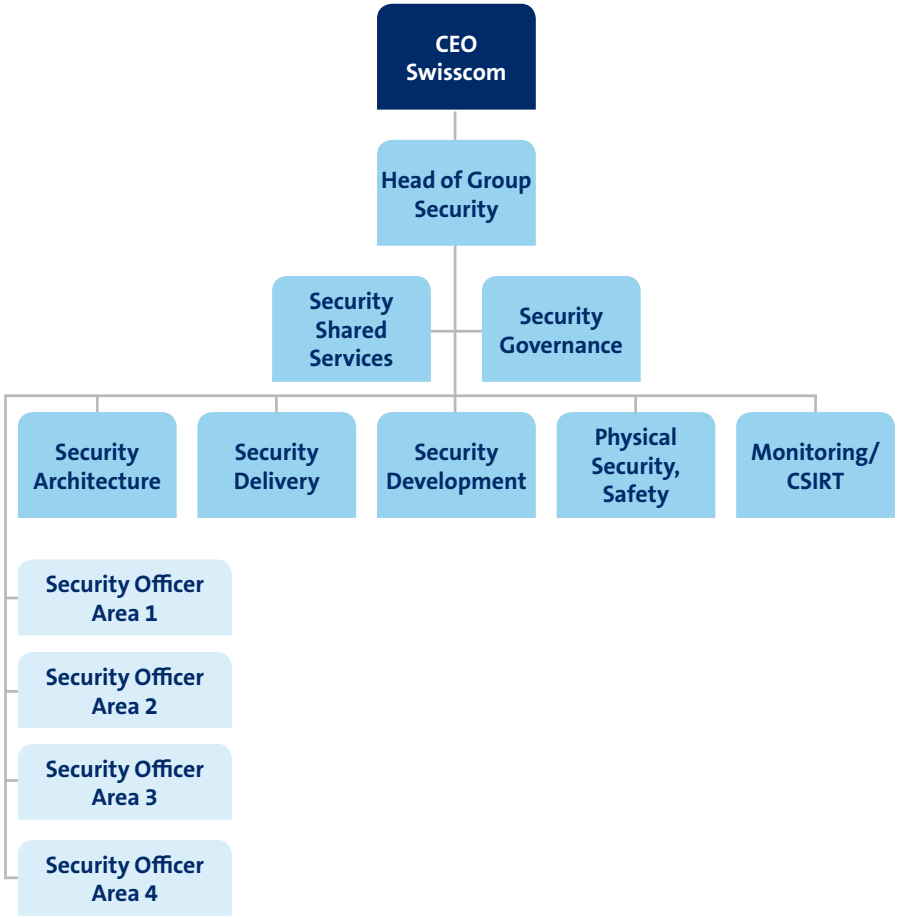


Fig. 9: The current organisational chart shows the key importance of security at Swisscom.

The Head of Group Security reports to the CEO and is a guest of the Group Executive Board. He is called upon when required, or can approach the Group Executive Board at any time to discuss agenda items that he believes are important. This means that security features regularly on the agenda at meetings of the Group Executive Board and Board of Directors. Both boards value this, as it ensures that they are always kept informed about the current threat landscape and how any threats are developing. They are also kept in the picture about activities in connection with security.

The security organisation itself is a traditional matrix structure comprising seven teams and four specialist managers:

Security Architecture The name says it all. This team is responsible for the company's security architecture. It not only defines the architecture but also implements it. In addition, the team is responsible for ensuring that the architecture is lived and implemented in projects. This ensures that no ivory towers are constructed. Security Architecture has close interfaces with the Enterprise Architecture team. As such, it is essentially the extended arm of architecture in security.

Security Delivery In simple terms, Security Delivery is the internal consulting unit. This team handles projects (where they fall under the responsibility of the security organisation) and supports business projects. It is managed as a traditional consulting/engineering organisation and has the corresponding responsibilities.

Secure Software Development This team is a consequence of the fact that software is becoming ever more important at Swisscom. This trend is based on the growing need for the divisions to develop their own software in the most decentralised and agile way possible. It was prompted above all by the emergence of app development. However, the trend is also boosted by the need to be able to react quickly to the market – or to actually create a market in the first place. Given these conditions, ensuring that software is created that already has security built into it calls for intensive support from the security organisation during the development process. The team also develops the vital reporting environment that measures compliance with technical controls on the servers.

Physical Security, Safety This team is responsible for physical requirements and their implementation. It also has the job of integrating IT security into other areas of security and seeking creative solutions for producing new products in a more efficient and cost-effective manner. A typical question might be whether expensive static data centres will still be necessary for certain services going forward, or whether container data centres will be sufficient. The team also covers workplace safety, in other words the measures we put in place to protect our employees – especially those performing dangerous work.

Monitoring/CSIRT The current and future threat landscape illustrates that detection of and intervention in the event of attacks is set to become increasingly important going forward. Incorporating the CSIRT into the security organisation completes the circle of information. What we learn from detection and monitoring can feed directly back into policies and architecture. It is clear that the CSIRT maintains a very close interface with operations, which means that integration into operational processes is of fundamental importance. As such, a security incident should in principle be handled no differently to any other operational incident, except that in such cases the technical lead is a member of the CSIRT rather than an operations employee. This concept has so far proved to be very successful at Swisscom.

There are also two staff units within the security organisation. The first is called **Security Governance and Policies.** This important central team is responsible for the policy framework, security governance, risk management, crisis management and all ISO certification activities. The team works closely with various other units such as Legal Compliance, enabling it to tackle many key topics horizontally in terms of both hierarchy and technology.

Security Shared Services The second staff unit acts as a kind of hub for security matters. When employees have questions for the security organisation, this is generally where they end up. Security Shared Services tackles cross-sectional processes such as exception management, communication and awareness. This unit is also home to the Security CIO , who helps us bring together and network the various tools and software packages we use for security.

One might naturally have concerns that a security organisation that reports directly to the CEO and is located close to the Group Executive Board runs the risk of constructing an ivory tower for itself. To guard against this, we have created the role of **Security Officers** who look after the various areas of the security organisation and act as the interfaces between it and the business. The Security Officers work closely with the divisional heads from the various businesses. They have a wide-ranging remit. On the one hand, the main risks should be tackled transparently by division management or accepted. This calls for a close and trusted partnership. On the other, it is the job of the Security Officers to carry the requirements of the business back into the security organisation. This ensures that security develops in the right direction. Last but not least, the Security Officers are also responsible for the security organisation's projects and deliverables in their divisions. They therefore perform a similar role vis à vis the individual divisions as the Head of Group Security vis à vis the Group Executive Board. To date this has proved to be a great success.

8 What does this mean for technology?

At this point we should highlight three concepts that help deal with threats in a sustainable way.

8.1 Data-centric security

In the past, information protection was geared primarily to the data carriers and the mode of transmission used. Typically, where information is confidential both the data carriers and the data transmission must be encrypted. The result, however, is that control of the data is lost at the moment they are received by the recipient. In addition, if you focus solely on data carriers and transmission then there is no way to prevent the uncontrolled distribution of critical information.

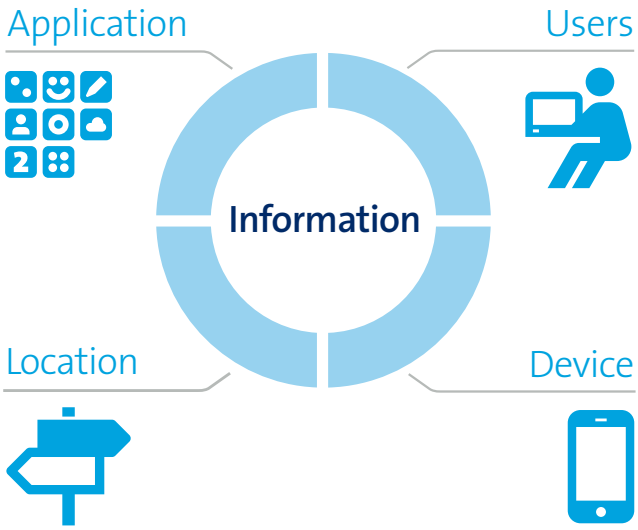


Fig. 10: In IT security it is not enough to just encrypt the data carriers and the transmission. The information itself must be the central focus.

This has to change. The focus has to shift from data carriers and transmission to the information itself. The key to this concept is that the information must protect itself over the long term. To put it another way, the information is encrypted and remains so wherever it goes. Some manufacturers have laid the foundations for an approach of this kind with rights management services, but have not yet gone the whole way.

With data-centric security, the information itself decides on access (or from a technical perspective, a policy server) based on four criteria:

The user: The key issue here is not simply who the user is and what role they perform, but also how they have authenticated themselves. In the case of public comments on a website, it can be sufficient to use Facebook as an authentication service. In the case of internal company information, a user name and password may be enough for the company network. Where content is confidential, however, the information also requires a second factor such as a card, mobile phone or biometric data.

The device: The requirements in terms of the device also depends on the classification of the data. Many companies make a distinction between own devices and external devices. This distinction is not really appropriate, however. The only requirement is that the device complies with the policy for access to the data in question. The difference between devices managed by IT and those managed by employees themselves relates to responsibility for compliance with the policy. In the first case IT is responsible, in the second it is the employees themselves. Device requirements may include conditions such as memory encryption, patch status, operating system version, etc.

The location: Location can be understood in two different ways. The first relates of course to the geographical location in which a computer is situated. This approach is typically used in the financial industry, where certain data may only be accessed within national borders. Depending on accuracy, the location could of course be narrowed down to the building in which the server runs. The second meaning of location is based on technical network criteria. For example, a distinction could be made between computers on a company network, those connected via a VPN or even those on a public network.

The application: The application should also play a role. The version and patch status can influence the decision on data access.

User behaviour could also be taken into account as an additional criterion. This is something that the credit card industry already carries out as a matter of course in the form of behavioural analysis. If it were possible to provide support for technology that monitors user behaviour on all standard devices, the security problems associated with BYOD could be largely solved. If an employee leaves the company, access can immediately be limited or prevented entirely.

Installing behaviour-based security software on private devices is problematic, however, since support also has to be provided by the manufacturer or the "shop around the corner". If the security software were to intrude too deeply into the operating system, this concept would be invalid. The result would be high support costs for the company or widespread dissatisfaction among employees.

All in all, it is fair to say that systematically implemented data-centric security solves a lot of problems. Even cloud storage solutions such as Dropbox would only be problematic to a limited extent, as the location of the data is actually wholly irrelevant – they are protected whatever. Public cloud services would also no longer represent a risk. One limitation, however, is that even with data-centric security it is not possible to carry out searches in encrypted data.

This approach may well seem futuristic, but the individual components for such a solution already exist, and as such it can be considered to be an entirely feasible objective.

8.2 The Collaborative Security Model

Many companies generally work on the assumption that the most reliable way of identifying security incidents is to use the best security products. One consequence of this is that very different consoles and techniques have to be used for detection and response. In addition, the decision on the "best" product is based purely on a snapshot of the technology available at the time of selection. This can change at very short notice, however.

To overcome these hurdles, Swisscom has launched the Collaborative Security Model. It addresses both of the weaknesses outlined above, based on the assumption that the divisions themselves decide on the most suitable product for solving a problem at any given moment. In the case of a mail server, for example, they may opt for the virus protection that delivers the best detection rate. The required security technology can thus also be licensed on a "pay per use" basis.

The model also takes account of the fact that most companies combine their logs in a single environment (logging & monitoring platform, Fig. 11) and also use them for security evaluations. Comprehensively consolidating logs in this way can significantly increase the detection rate for opportunistic attacks. Intervention remains complicated, however. If a port needs to be blocked or a computer denied access to the Internet, for example, the corresponding rules have to be configured manually in the proxy servers and/or firewalls. This takes up valuable time.

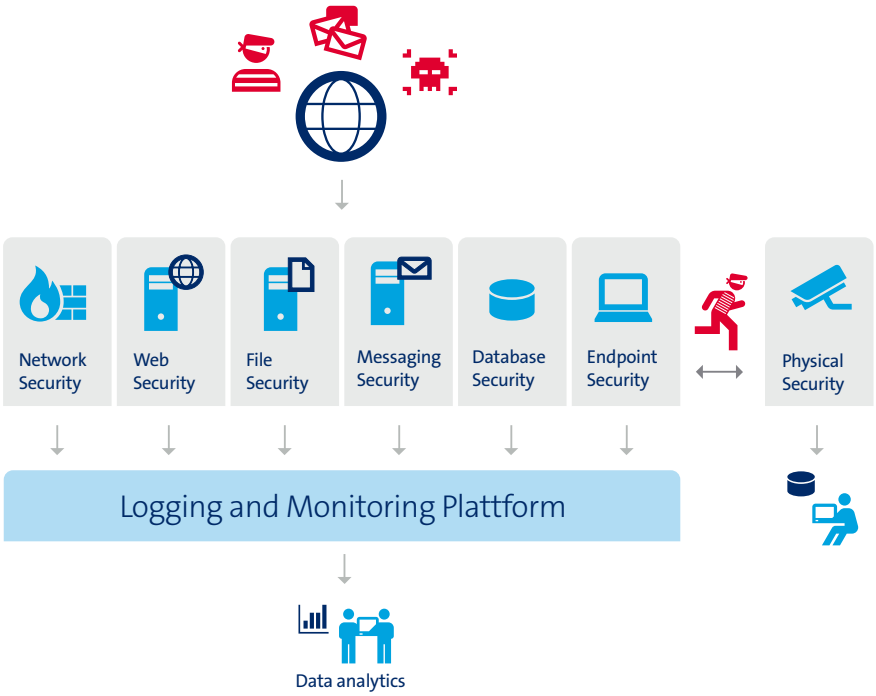


Fig. 11: The Collaborative Security Model gives the divisions a certain amount of freedom when choosing security solutions and consolidates the logs to make them suitable for regular security evaluations.

Swisscom wants to solve this time problem by introducing an additional abstraction layer between the security products and the logging & monitoring platform. It is called the abstraction layer (Fig. 12) and is defined and managed jointly with the manufacturer of the logging & monitoring platform. The abstraction layer allows actions in respect of the various security layers to be triggered directly. Although this concept is still at the implementation stage, it has already become clear that it may significantly reduce response times.

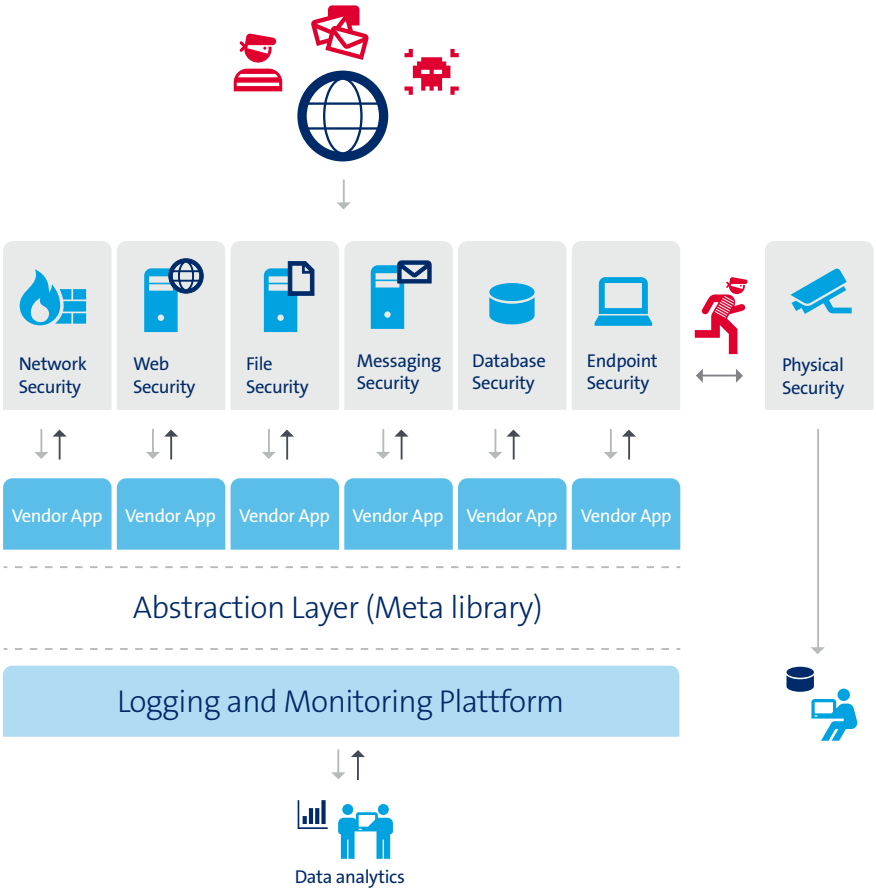


Fig. 12: Concept for a meta layer that permits a rapid response to attacks.

8.3 Threat Intelligence

It has already been mentioned that detection will become even more important in the future. This is based on the fact that no prevention is perfect and that attacks will sometimes be successful. As a result, new methods of detection are required. Current approaches based on security information and event management (SIEM) systems have enjoyed only limited success. The challenge inherent in these systems is that they can also answer the questions that you already know. In other words, the criteria under which an alarm is triggered are defined in advance. There are various problems with this approach:

- It is extraordinarily static and thus of only limited use in the fight against dynamic attackers.
- It is only scalable to a very limited degree.
- It requires highly qualified staff who are difficult to find.
- It is predictable for attackers.
- It often proves more complex than expected.

A dynamic and less predictable solution is therefore called for. Unfortunately there are currently no approaches available on the market that could be incorporated directly. As these concepts and ideas are very new, there is not yet a universal panacea.

Certain elements of dynamic detection have already been implemented at Swisscom. The process began with two relatively simple measures:

1. Every employee in the CSIRT team has a certain amount of time officially available to them each week to search for APTs (advanced persistent threats) independently and at their own discretion. Experienced analysts who know the network have a very good chance of sensing when something smells slightly off. Even though this approach does not seem especially structured, it has nevertheless already achieved a degree of success and will be retained despite all the technical alternatives.

2. To ensure that all parties have access to the same level of information in the event of an incident, a separate permanent chat room is set up for every larger-scale incident. Employees who do not work in the CSIRT are actively invited to join the chat room if the incident is of relevance to them. This ensures that information is shared rapidly, transparently and consistently, while documentation essentially takes care of itself. This in turn addresses the problem that incident handlers are often not very motivated to keep documentation up to date.

We have also started to use big data to detect anomalies in data traffic. Metadata from traffic in the company network (no customer data!) is recorded for a certain period of time and then evaluated. Since attacks on IT systems often follow similar patterns, these can be used to identify them. If a pattern is known, the security components can be programmed accordingly in order to prevent further damage.

8.4 Maturity model

Clear basic requirements remain a key pillar of good security. With regard to the level of abstraction, these requirements (policies) range from company-wide guidelines to the implementation and hardening of the objects that make up the IT landscape, in other words servers, workstations and network components, but also applications such as databases.

From a technical perspective, a mature framework that has grown up over a period of years and is based on common standards such as the Standard of Good Practice or ISO is indispensable. This framework is known as IT Security Level Basic (ITSLB) and describes at a technical level how an object, for example, must be configured securely. This is just one aspect, however; the other defines how patch management, malware protection, IAM and proxy analyses need to be set up and managed. The Deming cycle (named after the US physicist and statistician William Edwards Deming), which comprises the four steps "Plan", "Do", "Check" and "Act", maps the entire maturity model based on the ITSLB framework.

The "Plan" step and parts (technical implementation specifications – fact sheets) of the "Do" step are mapped in the ITSLB framework. Operations is then responsible for the implementation aspect of the "Do" step. The "Check" and "Act" steps are covered through reporting and the resulting corrective measures.

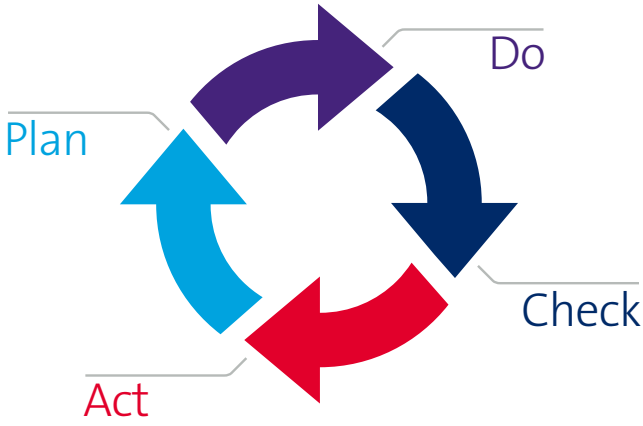


Fig. 13: The Deming cycle maps the entire maturity model based on the ITSLB framework.

As shown, end customers such as those of an outsourcer are very interested in how security is implemented by the service provider. The "Check" step is therefore also relevant for them, as it provides them with a transparent "security barometer". To enable this, the service provider requires customer-compatible reporting. However, it should also use this reporting for internal purposes such as initiating corrective measures.

Swisscom has developed "Sophia" to monitor the maturity of internal and external users. It allows up-to-date status on patch status, malware protection, ITSLB and other aspects to be called up via the web. It is used primarily for the server landscape, but also for managed workplaces and various other sensitive objects.

"Sophia" can be seen as a storage basin for security information. It also provides an inventory that is put together and consolidated from a diverse range of sources. As such it offers a benefit that should not be underestimated, since a correct inventory is vital to ensure effective coverage of the IT landscape and thus present the business in respect of security. Integrated exception management offers the opportunity to spot discrepancies in a wide range of areas and report them in a transparent way. By linking to various external providers of security information (e.g. weakness bulletins), "Sophia" receives additional content that also feeds into the reports.

Technologies such as big data or REST API interfaces are used and made available for “Sophia”. Finally, a multi-client web portal provides the interface to the security officer, who can monitor the maturity of security in a detailed manner and in real time.

Fig. 14: The Sophia web portal allows you to monitor the maturity of security in real time (screenshot does not show a real evaluation).

9 The role of the state

Even the most sophisticated security concept and the fittest security organisation cannot protect a company against all currently conceivable threats. And this is where the state should be making its contribution. There are essentially two areas in which the state can support companies – particularly with regard to protecting critical infrastructures. Firstly it can provide information, and secondly it can offer technical support in certain areas.

As far as information is concerned, in today's fast-paced world it is fanciful to think that the state can act faster than the private sector. Exploits and indicators of compromise are generally circulated very quickly and efficiently by the world's computer security incident response teams. These bodies are extremely well networked, and it is standard practice for findings to be shared quickly and simply. Since states generally do not have these informal channels, they will only rarely be quicker than the private sector. At best they can ensure that operations has a relatively clear picture of the situation. This can also then show, for example, where a similar attack is taking place and how those affected can mutually benefit.

Providing information when something is awry

The state does have access to information sources that are unavailable to the private sector, however, so can offer support in this respect. This does not have to relate to immediate threats – it can be extremely useful for security organisations to merely find out about indications of potential threats. This helps security organisations within companies to develop some initial thoughts about risk management.

"What would happen if?" is a question that companies have to ask themselves on an ongoing basis in any case. If they can already do this on the basis of potential threats, they are prepared in the event of an emergency. Such scenarios can also be used as an ideal basis for exercises in the crisis management team.

To ensure that the exchange functions as desired, however, both sides have to learn that such information does not need to be precise. Even if four out of five such scenarios never materialise, you still have a vital head start with the fifth and the considerations regarding the other four have not been in vain.

The second aspect as regards the role of the state is the supply chain. Nowadays we have to assume that even this is not always trustworthy. However, it is nigh on impossible for companies to check supplied products for built-in backdoors. Some manufacturers forbid reverse engineering in order to protect their intellectual property. This means that customers of these manufacturers are venturing out onto very thin ice if they start looking for backdoors. Not doing so is not an option either, however, particularly in the case of critical components.

Checking critical components for backdoors

It is here that the state could provide assistance. It should actually be in a position to carry out detailed checks on components that are vital for critical infrastructure and search for any backdoors they may contain. In some circumstances it would also be interesting to publish these results in order to send out a message to the world: "We are watching very closely."

Besides this, the state obviously assumes a controlling role. It has to have an interest in ensuring that the operators of critical infrastructures in particular fulfil their missions. In Switzerland, the federal government's cyber security strategy is dependent on the responsibility of individual companies. This is in line with the country's culture and the way in which people treat each other. Relying wholly on individual responsibility would be too risky, however. There must and should be a certain degree of control.

However, governments must be careful not to over-regulate or regulate incorrectly. There have been examples of regulators, chiefly in the area of incident response, imposing rules that limit companies' freedom to act. In this case, the regulators perhaps focused on easily measurable factors in the interests of implementable control, which ensures compliance but not security.

It would make sense for the processes to be regulated and audited. In other words, to ask questions such as whether the company fulfils its risk management obligations, or whether security risks are recorded and processed systematically. This would check whether a company's management is fulfilling its fundamental duty of care in respect of IT. Business risks have always been recorded and managed.

The breadth of impact of an information security management system could also be checked. Many companies already work in accordance with industry frameworks such as COBIT or ISO 27001. The latter is certifiable and can easily be demanded by a government. While it is fanciful to assume that ISO 27001 certification guarantees universal and high-quality security work, it can nevertheless ensure that all topics are addressed in one way or another. This would certainly be a step forward compared with the current situation.

Annex

Threat radar

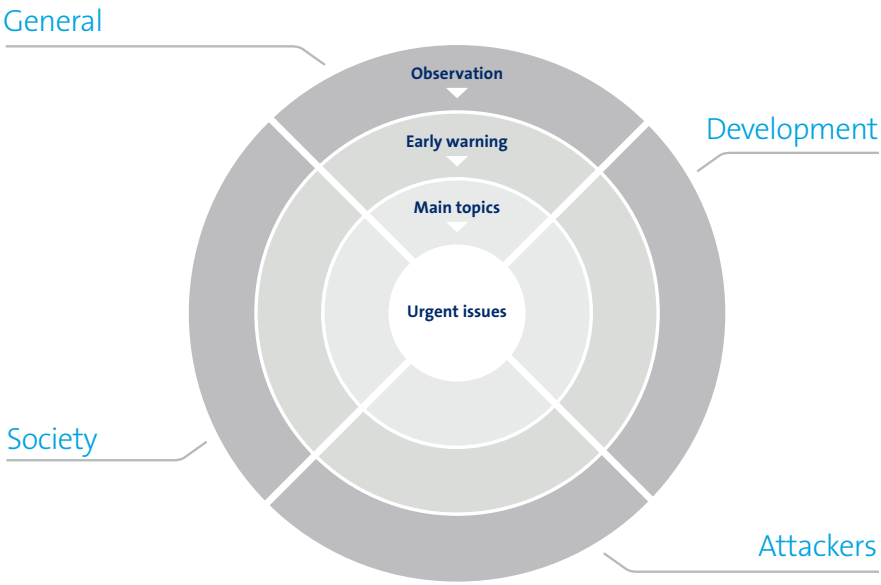


Fig. 15: ***Sample threat radar structure.***

The threat radar is made up of various sectors and circles. The sectors group the threats, thereby creating a certain structure. The circles describe the importance and urgency of threats based on the following hierarchy:

Observation: Threats that could become current in the next few years are recorded here. The security organisation keeps an eye on them, but for the time being devotes only a very reduced amount of time and money to them.

Early warning: Such threats must be kept in mind, with indicators possibly being established to identify any movements at an early stage.

Main topics: Threats in this ring are current and must be addressed.

Urgent issues: Such threats are highly topical and are also generally preceded by events.

Part of the daily work of the security organisation is to record threats and monitor the direction they move on the radar based on the observations made. The trail they leave provides an insight into where they might develop over the next 12 to 18 months.

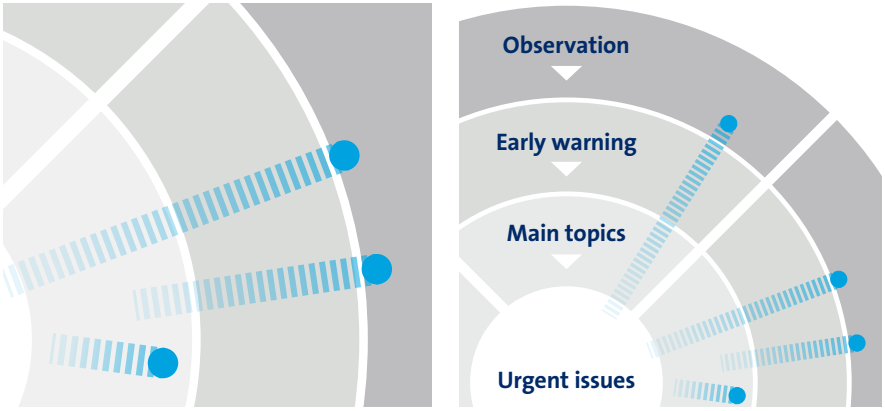


Fig. 16: The trail that a threat leaves on the radar shows the direction in which it might develop.

Abbreviations and specialist terms

APT Advanced Persistent Threat is a complex, targeted and effective attack on the critical IT infrastructures and confidential data of companies who are potential victims due to their technological advantage. Alternatively, attacks target companies who merely serve as a springboard to the actual victims.

Architecture Describes all static and dynamic aspects of a company's IT. This includes the > infrastructure and the associated management thereof (configuration and capacity planning, load distribution, data backup, availability, failure safety, disaster response planning, etc.). It also encompasses functional aspects such as the interfaces required to allow IT support for processes.

Big Data This is now generally understood to refer to the techniques for collecting and evaluating loosely structured mass data.

BYOD Bring your own Device describes the concept of integrating private mobile devices into the company network.

COBIT Control Objectives for Information and Related Technology is an internationally recognised IT governance framework. It breaks down IT tasks into processes and control objectives. COBIT does not primarily define how the requirements are to be met, but instead mainly what has to be implemented.

Continuity Management In business economics, continuity management refers to the development of strategies, plans and actions to protect the activities or processes that are crucial to a company's survival or to permit alternative workflows.

CSIRT Computer Security Incident Response Team describes a group of security experts who act as coordinators in the event of specific IT security incidents or focus on computer security in general, warn about security loopholes and propose solutions, and analyse malicious software.

CVSS The Common Vulnerability Scoring System is an open industry standard for assessing the severity of potential or actual security loopholes in IT systems.

Governance This describes the control and management system of a company or division.

IAM Identity and Access Management, in IT this generally refers to software components that manage identities and associated system access rights.

Infrastructure This comprises all buildings, communications services (network), machines and software provided at an underlying level (infra is Latin for "below") for the purpose of information processing.

ISF The Information Security Forum (ISF) is an independent, not-for-profit organisation with a membership comprising many of the world's leading companies. It focuses on the principles and concepts of IT security and provides tools.

ISO 27001 The international standard, subtitled "Information technology – Security techniques – Information security management systems – Requirements" specifies the requirements for establishing, implementing, monitoring, maintaining and continually improving a documented information security management system, while taking IT risks in a company into account.

ITSLB IT Security Level Basic is a framework that describes at a technical level how an object, for example, must be configured securely.

KPIs In business economics, Key Performance Indicators are ratios used to measure or determine the progress or degree of fulfilment of an organisation's key objectives or critical success factors.

KSI Common IT security indicator, used in the same way as > KPIs in business economics.

Logging Generally used in IT to refer to the (automatic) saving of process data or data changes in log files.

Monitoring A generic term for all types of immediate systematic recording (logging), observation or surveillance of an event or process by means of technical resources or other observation systems.

Policy An internal guideline documented formally by a company and for which management is responsible. In IT, policies can also be seen as framework provisions for permissions and prohibitions.

RASCI Technique for analysing and presenting responsibilities in a company. The name is taken from the initial letters of the words Responsible, Accountable, Consulted and Informed.

REST Representational State Transfer is a programming paradigm for distributed systems, and in particular for web services and machine-to-machine communication.

Risk Management Comprises all measures for the systematic identification, analysis, evaluation, monitoring and control of risks.

SIEM Security Information & Event Management refers to a software or service that analyses security warnings from a network's hardware and software components in real time.

Threat Usual term used to refer to danger in an IT security context.

Index of keywords

Actors	13
Always on	11
Threat landscape	13, 17
Threat radar	17
Big data	6
Bring your own Device (BYOD)	5
Collaborative Security Model	51
Common Vulnerability Scoring System (CVSS)	33
Consumerisation of IT	5
Data-centric security	49
Darknet	13
Detection	21, 24
Decentralised development	8
Secret services	16
Globalisation	9
Basic principles	23
Good practice	19
Hacktivists	15
Human-centred security	28
Intelligence	21
Internet of Things	7
Intervention	25
ISO 27001	19

Maturity model 55
Machine-to-machine communication 7
Monitoring 36

(Organised) crime 15
Outsourcing 9

Patch management 33
Policy and governance 35
Prevention 24
Procedures 29
Project management 30

Review 36
Risk management 39
Role of the Internet 13
Role of the state 59
Role of the security organisation 35

Script kiddies 13
Security business year 40
Security reporting 56
Security architecture 42
Basic security functions 29
Security principles 19
Security culture 27
Security organisation 38
Strategic management 39

Terrorists 16
Threat intelligence 54

Notes

Notes

Swisscom Ltd
Alte Tiefenaustrasse 6
3048 Worblaufen