

RESEARCH AT A GLANCE

ICT SECURITY: A MAJOR ISSUE IN COMPANIES

ICT security is not just a question
of technology

SEPTEMBER 2022

Powered by



MSM Research AG - Postfach 191 - CH-8201 Schaffhausen
www.msomag.ch - Telefon 052 624 21 21 - info@msomag.ch

CONTENTS

Page 2-3	Companies are facing major challenges
Page 4	ICT spending and the major importance of ICT security
Page 5	Spending on ICT security is being increased massively
Page 6-7	The threat situation and the human factor
Page 8-9	Dealing with the greatest security risks
Page 10-11	The big shift – support from external providers
Page 12	Summary
Page 13	Conclusion
Page 14-15	How can companies successfully prevent ransomware attacks? Interview with Swisscom
Page 16	Copyright

IMPRINT

Sources/basis for the study

Study: "ICT security in Swiss companies", MSM Research AG, 2022. Within the context of the study, in summer 2022, 82 companies in Switzerland were questioned extensively on the topic.

Note on the charts/results:

Unless otherwise specified, multiple responses were possible for the survey participants in each case.

Author

Philipp A. Ziegler, CEO, MSM Research AG

Design / layout

Corinne Jost, Head of Marketing, MSM Research AG

Publication

MSM Research AG - Postfach 191 - CH-8201 Schaffhausen - www.msomag.ch
Telefon +41 52 624 21 21 - info@msomag.ch

COMPANIES ARE FACING MAJOR CHALLENGES

Current global developments are confronting many companies with major challenges: rising energy costs, the war in Ukraine, geopolitical conflicts, chip shortages, supply chain problems, climate change and inflation concerns are again causing planning uncertainties after the end of the pandemic measures.

Even though Swiss companies are now much more robust and proactive than when the pandemic began in early 2020, planned investments and projects are currently being approached more hesitantly and cautiously again. Resistance on the planning front is likely to increase further. In addition to economic challenges, ICT security and business continuity management issues are at the top of the worry barometer from the perspective of the companies surveyed in our new study.

In calendar week 30 of the current year alone, 684 new cyber incidents were reported to the National Cyber Security Centre (NCSC). These were not only in the top categories of fraud, ransomware and phishing, but also in a list of cyber threats that now encompasses 18 categories.

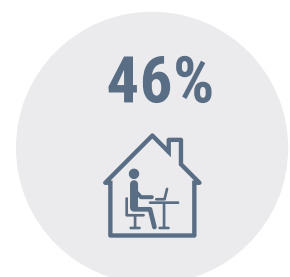
What general issues are you most concerned about in the company at the moment?

«Making ICT secure is currently one of the biggest challenges companies face»

Four out of five companies surveyed regard ICT security threats, or the increasing threat of cyber attacks/cyber crime, as the current top issue. This is due to the increasing number of attacks and the fact that they are becoming increasingly professional.



Increasing efficiency, optimising business processes



Employee mobility, home office, workplace of the future

Securing business processes and value creation

The current high importance of ICT security is also reflected in the number of projects: in more than 80% of the companies surveyed, security is the top priority in ICT departments.

This is a clear indication of strong awareness and the clear focus of project work on the secure operation and high availability of processes and applications.

But for nearly half of the companies, security issues and the somewhat broader topic of risk management are also at the top of the agenda in business departments.

Risk management in business departments not only includes purely legal risks associated with the handling of data, but also questions relating to ensuring the continued operation and high availability of the ICT infrastructure and applications in the event of a disaster.

«Business is dependent on secure and highly available ICT operations»


The 3 hot topics from the business and ICT environment

(44% of projects are ICT-driven, 56% are business-driven, total of 316 projects)

Projects driven by the business areas

 **48%** **Data protection**
(Risk Management, GDPR)

 **40%** **ERP**
(Enterprise Resource Planning)

 **37%** **Workplace**
Mobile solutions, remote & home office, UCC/video solutions

Projects driven by the ICT department

 **85%** **ICT security**

 **39%** **ICT operations, cloud & hybrid architectures**

 **34%** **Multi-Cloud**

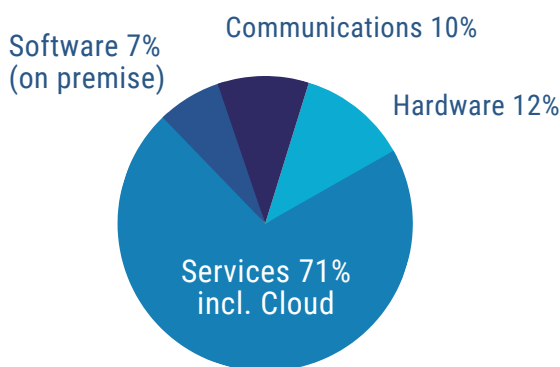
ICT SPENDING AND THE MAJOR IMPORTANCE OF ICT SECURITY

The effects of the current crises are also impacting the economic situation and development in Switzerland. According to the KOF (ETH Swiss Economic Institute) spring forecast 2022, the Swiss economy will grow by just under 3% this year in the most favourable scenario. And the EU has meanwhile lowered its growth forecast to 2.7%. Further corrections are impossible to rule out.

Despite the tense economic situation and rather uncertain outlook, Swiss companies are planning to increase their budgets this year as well.

We expect ICT spending (B2B) to grow by 4.5% in 2022 in a favourable scenario. This would take spending to over CHF 20 billion for the first time, which corresponds to a volume of more than CHF 84 million in project spending and orders per working day.

The lion's share of ICT spending (B2B) today is accounted for by ICT services, i.e. the service sector in the ICT market. Based on our current spring forecast, we expect services to account for 71% of the total ICT market in the current year 2022. This means that significantly more than two thirds of ICT spending will be transferred to service suppliers and providers.



Total ICT spending 2022: 20'064 million CHF

Growth 2021/2022: +4.5%

Total project spending of 84 million CHF / day

«The ICT market is a service market»

This is a trend that is expected to continue; the gap between services and other spending will continue to widen in favour of services. This is also with a view to the increased shift in ICT security spending towards external service providers.

MASSIVE INCREASE IN SPENDING ON ICT SECURITY

Swiss companies spend a lot of money ensuring the security and high-level availability of ICT. In 2021, 2.7 billion Swiss francs was spent on appliances (hardware), solutions (software) and services. And in the current year too, the majority of companies expect an increase in external expenditure for ICT security. We expect ICT security spending in Switzerland to increase by 8.3%.

The highest growth rates are currently being seen in expenditure for services due to the increasing utilisation of services from external providers. For the current year, we expect an increase of just under 10% in funds for external services.

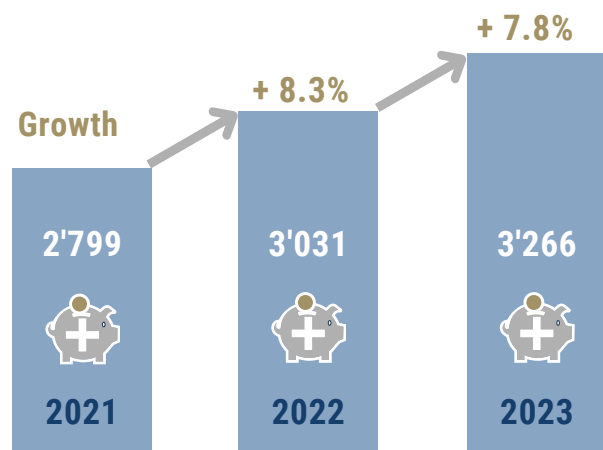
More than 12% of ICT spending is now on ICT security and high availability.

A separate ICT security budget

But even for ICT security, there is not always endless money available. What makes things more difficult in some companies is that planned budgets, expenditure and projects often fall victim to so-called "moving budgets" or are postponed by them. In the short term, other projects from business departments may be given preference, or expenditure for the modernisation and expansion of infrastructure may be prioritised.

One way out of this dependency dilemma could be to separate the security budget from the ICT budget in order to define and manage security spending in an isolated and autonomous way with an independently managed pot of money.

ICT security spending in Switzerland	2021 in CHF million
Security solutions (on premise)	949
Security appliances	362
Security services	1'488
Total ICT security market	2'799



THE THREAT SITUATION AND THE HUMAN FACTOR

In 2021, some 30'351 crimes with a digital component were recorded by the police in Switzerland, which corresponds to an average of 83 digital crimes per day. This represents a 24% increase from 24'398 in 2020. Almost 88% concerned "cyber economic crime". (Source: Police Crime Statistics (PCS), Federal Statistical Office).

Cyber crime and attacks on companies can not only cause significant financial and image damage, but can also have consequences for the management, the board of directors or the owner.

«The human factor is the biggest hurdle in ICT security compliance»

Our new study has made it clear that the most significant threat currently facing over 65% of companies is the lack of awareness and sensitisation among employees. The biggest hurdle to implementing and complying with appropriate security requirements is therefore people.

The companies surveyed stated that a lack of time to deal with security issues, a lack of awareness of the risks and consequences of misconduct, and ultimately a lack of expertise and of the corresponding specialists in the company are the greatest security threats.

What are the most important inhibiting factors and hurdles to implementing and complying with ICT security in your company?



52%

Too little time and capacity / chronic overburdening of employees



34%

Insufficient security know-how / lack of specialists



24%

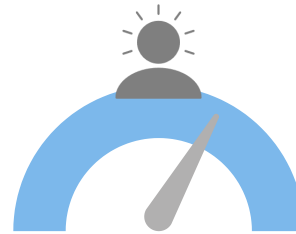
Insufficient support from management

In terms of security, the trend for workplace hybridisation and shifting work to home offices is a particular challenge for those responsible for security and for employees.

«Digitalisation, the hybrid workplace and the cloud create new targets»

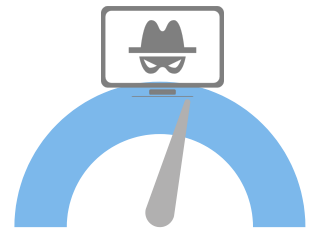
Furthermore, the proliferation and use of cloud services and the large number of data-collecting devices encountered in the course of IoT projects create further targets for cyber attacks.

Which sources and areas currently pose the greatest security threat in your opinion?



65%

Insufficient awareness among employees



57%

Malicious attacks by hackers

DEALING WITH THE GREATEST SECURITY RISKS

From the companies' point of view, one major source of danger and security risks is how employees deal with e-mails or social media messages. Thus, the deliberate or accidental opening of unsafe, unknown links or clicking on infected attachments from so-called "phishing e-mails" is regarded as the greatest source of danger.



**Greatest risk for companies:
dealing with e-mails (e.g. phishing,
clicking on unsafe links, opening
infected attachments)**

Another major source of danger involves the use of the Internet. By visiting manipulated websites or entering data on unsecured websites, Trojans or ransomware can be smuggled onto the user's computer.

Such manipulations and attacks by cyber criminals always aim to illegally access the user's personal data or intellectual property (espionage), gain access to financial accounts, demand extortion money or otherwise cause damage.

«Ransomware, phishing e-mails and the general use of the Internet are the greatest sources of danger»

In terms of security, the consequences of the pandemic in particular, such as the shift of workplaces to home offices, have opened the eyes of many companies to existing vulnerabilities and security gaps.

But simply becoming aware of the new risks will not be enough to ensure the most comprehensive protection possible. Prevention includes both technical and organisational measures as well as proactive and security-conscious cooperation on the part of employees.

The top three technical and organisational measures to minimise risks include regular sensitisation and training of employees on the secure use of e-mail and the Internet, limited user rights and access management (e.g. personal logins) as well as multi-factor logins.

However, the complete implementation of security measures and ensuring high ICT infrastructure availability requires more than just the comprehensive use of technology. It would be delusional to assume that higher security can be achieved by this alone.

ICT security is not just a financial or technological issue, but also a question of the culture and discipline practised by all employees in the company.

How do you deal with security risks in the company and what measures do you take?

73%



Regular sensitisation of employees on the safe use of e-mail and the Internet

67%



Restricted user rights / access management (e.g. personal logins)

56%



Multi-factor logins

THE BIG SHIFT – SUPPORT FROM EXTERNAL PROVIDERS

In order to be able to counter the increasing number of cyber attacks, many companies today work with external service suppliers and providers in the area of ICT security. In addition, the rapid development of new technologies is pushing many companies to their limits.

«External support is the order of the day»

Today, attacks are becoming more and more complex and existing protective measures can be circumvented by attackers. An attack can thus go undetected for several days, weeks and even months. It is therefore necessary to set up modern detection systems in order to recognise and ward off an attack as quickly as possible.

However, companies often lack the specialists with the specific expertise for comprehensively preparing for such incidents (incident response). Here, experienced and specialised service providers offer professional support with their know-how.

In which areas do you currently use the services of an external ICT security service provider?



Four out of five companies already use the services of external service providers or plan to do so in the next two years. To begin with, these are services in the areas of risk/vulnerability analyses as well as audits, employee training and penetration testing.

The further increase in cyber crime and the complexity of the attacks, the lack of or inadequate security expertise (incl. threat intelligence knowledge) and the increasing use of multi-cloud services are the most important key drivers for companies to use external managed security services (MSSs).

For sub-areas or entire sections of the ICT infrastructure and networks, managed security services involve systematic and continuous security monitoring for vulnerabilities, gaps and attacks. Relevant managed security service providers (MSSPs) are able to react quickly, competently and in an agile manner to changing threat situations, with transparent costs that can be budgeted for, coupled with clearly defined services.

«Managed security service providers (MSSPs) are able to react quickly, competently and in an agile manner to changing threat situations»

Over 64% of the companies surveyed plan to work more with external service providers and MSSPs in future due to the increasing cyber threats and rising security requirements.

And over 20% are speeding up the evaluation of external service providers due to the current risk situation and a lack of in-house resources.

The paradigm shift (from internal to external) or big shift that has been observed in ICT operations for some time now is also gaining momentum in the area of security. The outsourcing of tasks, work and services previously performed in-house to external providers has also clearly picked up speed in the area of ICT security.

What are the key drivers for using external managed security services (MSSs)?



93%

Increasing cyber crime / complexity of attacks



41%

A lack of or inadequate security skills (including threat intelligence knowledge)



18%

Use of multi-cloud services, increase in targets

SUMMARY – KEY FINDINGS

- Cyber crime and attacks on companies can not only cause significant financial and image damage, but can also have consequences for the management, the board of directors or the owner.
- For over 65% of the companies surveyed, the most significant threat at present is the lack of awareness among employees. One major source of danger is how employees deal with e-mails or social media messages.
- The top three technical and organisational measures to minimise risks include regular sensitisation and training of employees, limited user rights and access management as well as multi-factor logins.
- Despite the rather uncertain outlook, Swiss companies are planning to increase their budgets in 2022; we expect ICT spending (B2B) to grow by 4.5%.
- The highest growth rates in the area of ICT security are currently being seen by expenditure for services due to the increasing utilisation of services from external providers.
- In 2021, Swiss companies spent 2.7 billion Swiss francs on appliances (hardware), solutions (software) and services for ICT security and high availability. In 2022 the majority of companies expect an increase in external expenditure for ICT security. We expect a rise of 8.3%.
- In order to be able to counter the increasing complexity and number of cyber attacks, many companies today work with external service providers in the area of ICT security. Four out of five companies now use the services of external service providers or plan to do so in the next two years.
- The further increase in cyber crime and the complexity of the attacks, the lack of or inadequate security expertise (incl. threat intelligence knowledge) and the increasing use of multi-cloud services are the most important key drivers for companies to use external managed security services (MSSs).

CONCLUSION

No company is immune to cyber attacks. Even though the pandemic and its aftermath have raised awareness of security risks and vulnerabilities, appropriate concepts are not yet consistently enforced everywhere. Measures shouldn't only be implemented responsively in the event of an incident. Such patchworks are not an adequate response.

ICT security must not be allowed to become a mere cost issue, and budgets planned accordingly should not fall victim to other project priorities.

One way out of this dependency dilemma could be to separate the security budget from the ICT budget in order to define and manage security spending in an isolated and autonomous way with an independently managed pot of money.

However, ICT security is not just a financial or technological issue, but also a question of the culture and discipline practised by all employees in the company.

Security that is all-encompassing and as comprehensive as possible not only includes an external view and measures based on current threats and risks, but also requires precautions based on a critical view of the organisation and the human factor.

After all, responsible, security-conscious behaviour by all employees and the sensitive handling of data are ultimately the most effective line of defence and "firewall" in the fight against cyber attacks and ICT failures.

HOW CAN COMPANIES SUCCESSFULLY PREVENT RANSOMWARE ATTACKS?



«Every company needs effective measures against ransomware»

Stephan Rickauer heads the CSIRT Service and CSIRT Rapid Response team for business customers at Swisscom

Why is ransomware such a big threat for companies?

Stephan Rickauer: Probably because the threat is so specific and comprehensive. I don't know any CEO who would calmly tell me in a rapid response case: "Mr Rickauer, there's no need to rush. We can carry on with our core business without IT." These days, you can't even sell a croissant without IT. That makes every company vulnerable to blackmail.

In addition, many companies are inadequately prepared for a ransomware attack. This can be seen in the almost daily media reports. Most of the time, not even the most basic measures are taken. For example: a company connected a system that had not been patched for two years directly to the Internet to solve a problem "in the short term". Shutdown was forgotten and the server was contaminated and served as a gateway for company-wide encryption. The consequences were damage amounting to over 100,000 Swiss francs and several days of downtime.

What are the latest developments in ransomware?

We are observing that attacks are becoming increasingly professional. Individual jobs are split up. There are access brokers who only sell access. And there is malware as a service, whose developers even offer SLAs for attackers. We are dealing with an entirely new industry here, not just creative unemployed people. The good news is that the defenders are continuing to develop ways to counter such attacks.

What was once a virus scanner is now "endpoint protection" and is always the first thing we roll out in an emergency in the incident response team. The issue of security is also much more present than it was six or eight years ago. A new, large industry has also emerged on the defence side. Critical infrastructure operators, like us at Swisscom, are investing significantly more in cyber defence measures today.

What do companies need to do to improve protection?

Stephan Rickauer: Management is responsible for ensuring the viability of the company. Today, protection against ransomware is as important as seat belts in a car. But the topic often appears daunting and complex, and the market is labyrinthine. I therefore advise companies to commission an external security audit and then proceed step by step in a risk-based manner. This is affordable and should be on the agenda of all decision-makers.

The good news is that there are many providers of managed security services that even SMEs can afford. Not every company needs to train its own cyber security specialists. But the dangers must be known and the measures against them must be effective.



About Swisscom Business Customers

The Business Customers unit at Swisscom is one of the largest integrated ICT providers for key accounts and SMEs in Switzerland. The core competences of Swisscom Business Customers are integrated communication solutions, IT infrastructure, IT security and cloud services, workplace solutions, SAP services, IoT as well as comprehensive outsourcing services for the financial industry and healthcare. Swisscom Business Customers supports a good 2'500 key accounts and over 250'000 SMEs with the help of around 5,000 employees.

Security at Swisscom Business Customers

Swisscom Business Customers is the leading provider of security services in Switzerland according to independent studies. Our security specialists work to ensure the information security of Swiss companies day after day. Swisscom offers customers a large range of dedicated and proven managed security services, including a 24/7 security operation centre with access to security specialists.

Further information on Swisscom managed security products can be found at

<https://www.swisscom.ch/security>

COPYRIGHT AND TERMS OF USE

This white paper was created by MSM Research AG, powered by Swisscom, for distribution to its customers.

The information and details contained within it were established conscientiously and with the greatest possible care and accuracy.

Assumptions and estimates are unavoidable and are based on our current knowledge.

However, no guarantee can be provided with respect to their completeness and correctness.

The copyright and all data rights remain with MSM Research AG. The duplication or further processing of the contents in whole or in part is not permitted. Publication is only permitted with the written approval of MSM Research AG.

Copyright by MSM Research AG, 2022