swisscom

Cyber Security Threat Radar
2022/2023

Living Security by Design

Contents

"We believe that Security by Design and human-centred security means thinking consistently about security from the outset and placing the focus on our employees. This is the only way we will succeed in keeping our companies on track when it comes to security."

Cyber Security Threat Radar

Are cyber risks here to stay?

The danger posed by cyber risks remains at a very high level. If you want to improve cyber resilience in your company, it is imperative to take a holistic view of cyber and IT security. Merely waiting out a crisis or hoping that the threat level will soon return to normal are not recommended. Instead, it is advisable to prepare thoroughly for possible crisis scenarios so that if emergency situations arise they can be dealt with as appropriately as possible while ensuring any damage is minimised. The multi-risks and cyber risks we are currently facing today are here to stay. Their impact is felt and visible in many countries around the globe. The danger is that due to collateral damage, they are becoming even more unpredictable.

By now, it should be clear to everyone that the topic of cybersecurity is not just the responsibility of IT departments and that it affects all areas of a company. Sound business continuity management is just as much a part of risk management as a stable IT service. In addition to technical precautions, well-trained and attentive employees also play a central role. Maximum resilience can only be achieved if these two elements exist in unison.

The purpose of the Cyber Security Threat Radar presented here is to help companies to identify and appropriately combat key cyber risks. It serves as a guideline to create a uniform awareness of cybersecurity problems so that a comprehensive security concept can be established.

This cross-organisational guide lays the foundations for successful cybersecurity – and therefore underpins the success of any company in the digital world.

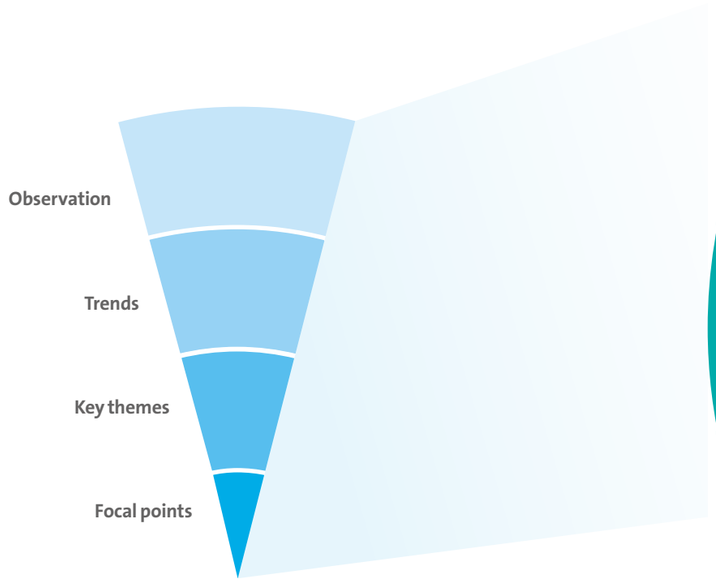
Marco Wyrsch
Head of Group Security
Swisscom (Schweiz) AG

In the introduction to last year's Cyber Security Threat Radar, my predecessor in the role of Head of Group Security at Swisscom Philippe Vuilleumier commented: "The war in Europe is changing our world." This statement is still highly relevant one year later as the war continues to maintain its grip on the world. The impact is felt in many ways: the threat of power shortages, gas shortages, the battlefield moving to cyberspace, acts of sabotage on critical infrastructure, a deluge of fake news and intense media coverage across all channels. The current situation clearly tells us that logical and physical security must go hand in hand in times of multiple crises. This makes it all the more important to have a heightened awareness of risk. The synergy between people, processes and technologies forms the foundation for creating corporate resilience and stability in uncertain times.

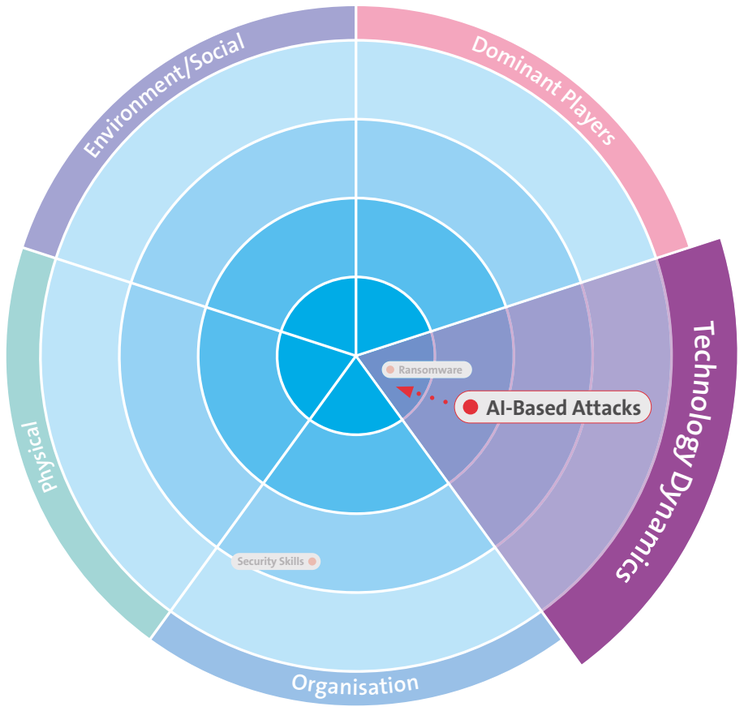
Situational awareness – threat radar

Being able to fall back on security strategies and procedures at the right moment that have been strengthened and tested helps us to cope with unpredictability – or what are sometimes called black swan events. When paired with a consistent safety culture, error transparency and well-trained employees, we can lay the foundations for organisational resilience.

To achieve this, potential threats must be identified at an early stage and systematically recorded. We use our well-known Cyber Security Threat Radar to map the current threat status and its evolution.



Challenges and tendencies:
AI-based attacks – the dark side of technological progress



What is the issue?

AI-based attacks are cyberattacks in which artificial intelligence technologies are used to make attacks more effective and efficient or to circumvent existing defences.

AI-based attacks have been talked about for a long time. In recent months, however, there has been a real evolutionary leap in the tools available. Tools such as the large natural language model ChatGPT, which was launched in November 2022, impressively demonstrate how the quality of attacks such as phishing campaigns can be significantly improved or used to detect vulnerabilities in programming codes. AI is currently a highly discussed issue in the media and its misuse for the creation of malware/malicious codes and phishing campaigns is certain to increase in the future. We are observing and analysing this development, but it has not yet become a “hot spot” topic.

How will the challenge evolve?

One of the first developments we expect to see is an increasing conflation of targeted attacks with AI-generated phishing emails. A language model AI can create a compelling storyline to continue a conversation based on an existing email exchange and cleverly link it to a phishing or social engineering attack. With the appropriate automation, targeted phishing campaigns can be created with completely individualised, context-dependent emails.

Another way language model AIs could be increasingly used in the future for malicious purposes is through their ability to analyse programme codes for vulnerabilities and to programme malware to exploit any vulnerabilities that are found, including applicable attack vectors. This means that cyberattackers no longer need to have as much knowledge to carry out complex attacks.

In addition, the rapid evolution of image- and video-generating AIs continues to enable deepfake cyberattacks and disinformation campaigns that are almost impossible to identify by conventional means.

How can the challenge be dealt with effectively?

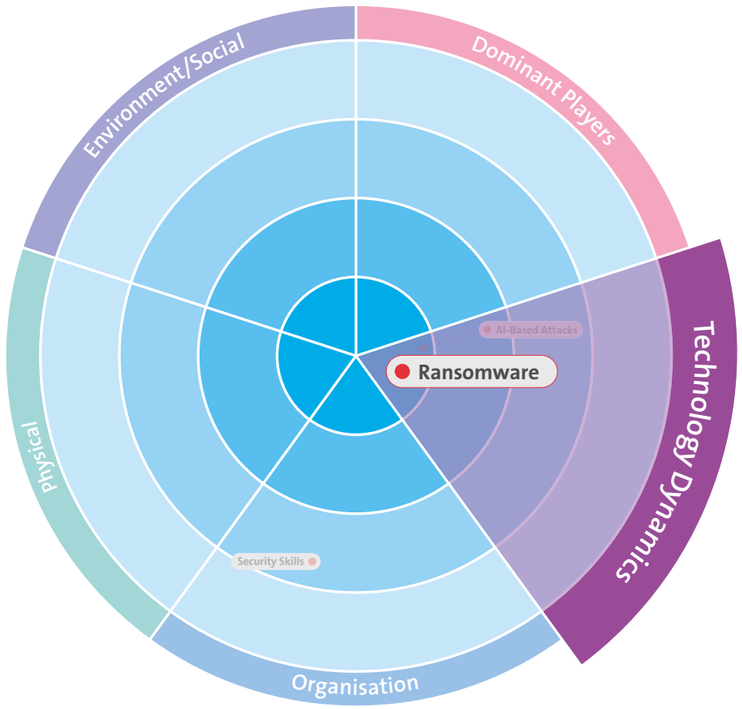
Although AI technologies can be used by attackers, they will also give defenders better ways to detect and defend against cyberattacks. For example, they can be used to recognise AI-generated texts or AI-generated images and video. Concepts such as Zero Trust for granular controlled and authenticated access to data and resources help to reduce the number of areas where companies can be attacked. However, established security best practices, such as multi-factor authentication, DevSecOps, vulnerability and patch management and security awareness among employees, also help prevent cyberattacks – and not just AI-based attacks, but those in general.

"While AI technologies are developing rapidly, we need to be aware that they are not good or evil per se. Rather, it is a tool that can be used for both purposes. The challenge is to continue to strengthen defences in such a way that AI-based attacks can also be successfully defended against – and in the future increasingly with the help of 'good' AI."

Florian Leibenzeder
Head Swisscom Security Operation Centre

Challenges and tendencies:

Ransomware – blackmail through data theft instead of ‘just’ encryption



What is the issue?

Ransomware is a type of malware (malicious software) that aims to encrypt the victim’s data after infecting a computer, server or network, making it unusable for the victim. Victims only receive the decryption key that will enable the data to be recovered if they pay a ransom. Last year, this form of attack was also recognised as an acute challenge and addressed separately in the Cyber Security Threat Radar.

Since then, however, many companies and organisations have upgraded and developed in technical terms, so fewer and fewer ransoms are now being paid due to ransomware attacks. The attackers are either successfully blocked when they try to encrypt the data or the data can be recovered by other means. For instance, it is now the case that attackers are often not able to make backups unusable. Instead, they are increasingly relying on data exfiltration and the subsequent threat that it will be made public. Unlike encrypted data, which can be restored from backup, it is almost impossible to prevent exfiltrated data from being published without paying a ransom.

Cyberattackers are financially motivated. Ransomware attacks and the associated data theft are the easiest and most direct way for them to make financial gains from a compromised corporate infrastructure. The sum demanded usually depends on the size of the company and amounts to around three per cent of turnover. However, it is important to note that the ransom paid is often only a fraction of the costs caused by the attack itself.

Although there are no official statistics on the amount of payments actually made, estimates suggest an average yield of 950,000 Swiss francs per successful attack. Globally, the economic losses caused by ransomware attacks is expected to exceed 240 billion Swiss francs by 2031.

The prospect of making big money from such attacks is leading to an increased level of professionalisation among attackers. This has led to the rise of so-called ransomware unicorns. It is known from various sources, such as the Contileaks, that many attackers now have access to financial resources similar to those of well-funded IT start-ups.

These operations sometimes employ several full-time developers and hackers and offer their victims multi-level ‘customer support’. They use agile development methods and continually develop their business models and infrastructure. They also maintain their own bug bounty programmes, which help keep cybercriminals aware of any security vulnerabilities in their own IT infrastructure.

Some hacker groups also value having a degree of notoriety. For instance, a guerrilla marketing campaign conducted by the hacker group Lockbit called on people to get a tattoo of the Lockbit logo for a fee of 1,000 US dollars. Many photos were then posted on the internet showing people with a freshly inked lockbit tattoo.

How will the challenge evolve?

Ransomware is and will remain a hot topic. We expect a significant increase in multiple extortions, which involves linking several forms of attack such as ransomware, data theft and denial of service, as this form of ransomware attack has already become established among cybercriminals. Managed service providers are also increasingly becoming the focus of attackers. Experience shows that they are very willing to pay a ransom, and their customers can also be attacked directly in order to make even more profit from the attack.

The greatest future challenge is the fact that cyberattackers are becoming increasingly specialised and so their attacks are becoming increasingly complex. Even now, the greatest threat comes from ransomware-as-a-service offerings. In this case, ransomware groups no longer attack companies themselves but rent out their encryption malware, servers and support infrastructure to other attackers. The ransom that is received is then divided 'fraternally' between the attackers and the ransomware group. There are 'initial access brokers' who specialise in attacking companies and then selling the access opportunities they have gained.

Gaining initial access can either occur via human means or on an infrastructure level: On the infrastructure level, publicly accessible servers are attacked via vulnerabilities that have already been identified or via 'zero-day exploits'. Zero-day exploits are often no longer developed in-house but purchased from other parties.

On the human level, some attackers use targeted (spear) phishing campaigns on the end users of a company. Other ransomware groups contact their victims' employees directly and try to bribe them by paying large sums of money. Attacks on private infrastructures used by employees are also being seen more and more frequently, most recently during the attacks on LastPass when a system administrator's home network was first hacked in order to steal the access data for the company's VPN.

How can the challenge be dealt with effectively?

The most important protective measure is to follow established best practices. These include, among other measures:

- Patch and vulnerability management
- The use of modern air-gapped backup solutions and regularly created (offline) backups, as well as regular recovery testing
- Develop security awareness within the company
- Consistently use multi-factor authentication (MFA) and secure against MFA fatigue
- Comprehensive monitoring of IT security by means of endpoint detection and response (EDR)
- Specialised security teams such as Security Operation Centres (SOC) and Cyber Security Incident Response Teams (CSIRT)
- Network segmentation and safety zone concept
- Define incident response and crisis communication processes and introduce regular training sessions to prepare for potential crisis scenarios

"When attackers are becoming increasingly specialised, it can be very helpful to also rely on specialised companies and the use of external expert teams to shore up your own defence."

Tim Trinkl
Senior Security Analyst & Incident Responder B2B

Challenges and tendencies:

Security skills – preventing the shortage of skilled workers and a loss of knowledge

What is the issue?

Regardless of their size, many companies often face the same challenge: Their security teams are understaffed and/or overworked. The increasing number of security incidents, the challenge of prioritising them and the lack of skilled staff can overwhelm companies, leading to increased risk. To keep pace with cybercriminals, companies do not necessarily need higher budgets but employees who have relevant IT security expertise. And here is where we focus on two of the attack vectors addressed in the Cyber Security Threat Radar: security skills and infrastructure misconfiguration. Due to a lack of skills and personnel, cyber risks increase exponentially through the exploitation of misconfigured infrastructure components.

Swiss universities, universities of applied sciences and other training institutes have massively expanded their study programmes in recent years but are not yet in a position to meet the current high demand for cyber-security specialists.

In a constant battle for talent, a company can expend vast amounts of time, resources and energy fishing for suitable candidates in a heavily depleted skilled labour pool. Another option is to look inwards and invest in the further education and training of your own employees. With the increasing number and complexity of attacks by cybercriminals on government and private sector targets, the global shortage of cybersecurity experts is already being acutely felt in many companies and organisations.

However, the problem does not just centre on the utter lack of cybersecurity experts, but also on the fact that some security experts no longer wish to continue working in this field. Numerous studies show that many cyber-security professionals are considering changing jobs.

How will the challenge evolve?

"As a result of geopolitical tensions and macroeconomic instability, as well as high-profile data breaches and growing physical security challenges, the issue of cybersecurity is coming more into focus and the demand for skilled professionals in this field is increasing," explains Clar Rosso, CEO of (ISC)², the International Information System Security Certification Consortium.

Many companies rely on training platforms for cyber specialists to specifically strengthen in-house education and training. However, there is often a lack of meaningful integration in terms of the education and training of employees who increasingly need security skills to carry out development, operational and innovation processes. Questions such as "How do I make training and development so attractive that they are taken up by tech employees and also used alongside day-to-day business activities?" or "What opportunities does this also open up for an active training programme in the specialist environment?" often remain unanswered. The actual training on offer is quickly accompanied by questions concerning the right organisational setting.

Today, applicants repeatedly complain that there is not enough focus on them as human beings during the recruitment process: long response times on the part of companies following applications, rigid policies and entrenched salary bands, lack of transparency in the recruitment process, and many more factors are cited as negative examples. This suggests that unprofessional recruitment processes are being followed in some of the companies that were criticised. In order to be perceived as a sustainably attractive employer for cyber talent, a rigorous employer journey needs to be part of the recruitment process.

How can the challenge be dealt with effectively?

Improve working conditions: Money alone does not make you happy – but it is definitely a decisive factor. Apart from adequate remuneration, companies can also score points in terms of working environment and work-life balance. And there are many options in this regard: flexible working hours, remote working models, reduced working hours with the same salary, etc. Companies must evaluate and decide for themselves which options are realistic for them.

Adjust expectations of applicants: Entry-level or junior candidates with both a degree and at least five years of professional experience do not match reality. Many companies should rethink their expectations in this respect – unless they do so, the search for good employees is likely to be very difficult.

Offer further training and develop internally: Through relevant training and further education – ranging from on-the-job training to DevSecOps boot camps and university courses – employees can acquire the necessary cybersecurity skills and take on new tasks. To ensure that their own staff take advantage of these opportunities, companies must create appropriate incentives, such as by contributing to the costs of further training and development.

Use outsourcing and reduce workload: To reduce the workload in cybersecurity departments, certain tasks can be outsourced to external and specialised service providers. External service providers can help to close specific gaps in the company's expertise (knowledge gap).

"We urgently need to close the talent gap in cybersecurity. To achieve this, we need to break down barriers to entry, retain people with meaningful work in cybersecurity and ensure that employees stay for the long haul. Targeted training in the internal DevSecOp environment also proactively supports the 'battle for talent'."

Marcus Beyer
Security Awareness Officer

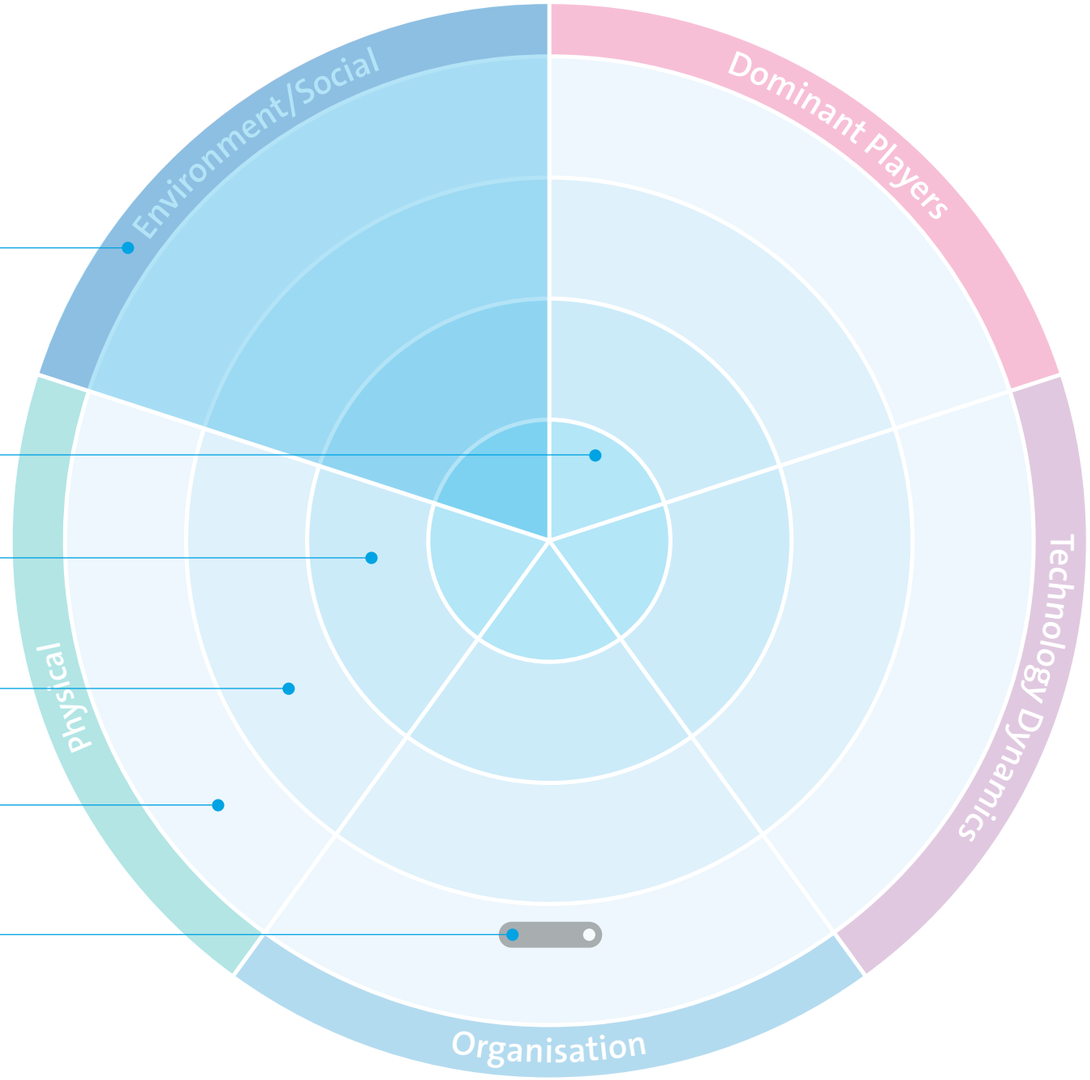
Method

The threat radar is divided into five **segments**, which distinguish the different threat domains from each other. In each **segment**, the associated threats can be assigned to one of four concentric circles. The circles indicate how current the threat is and therefore also any vagueness in the assessment of the threat. The closer the threat is located to the centre of the circle, the more concrete it is, and the more important appropriate countermeasures are.

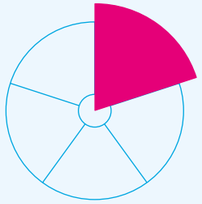
We identify the circles as:

- **Focal points** for threats that are already real and can be managed with a relatively large input of resources.
- **Key themes** for threats that have already occurred sporadically and can be managed with the normal use of resources. Regulated processes often exist to efficiently counter such threats.
- **Trends:** Early detection for threats that have not yet occurred or are currently very low. Projects have been launched at an early stage to counter the growing significance of these threats in the future.
- **Observation** for threats that will not occur for several years. There are still no concrete measures for dealing with these threats.

Furthermore, the individual **threats** marked by specified points show a **tendency**. This can be increasing, decreasing or stable in terms of criticality. The length of the tendency line indicates the expected speed with which the criticality of the threat will change.

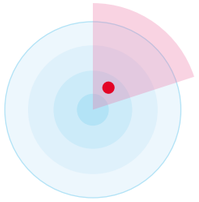


Details including tendencies and comparison with the previous year



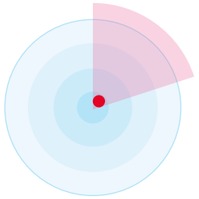
Dominant players

This segment subsumes threats that emanate from dependencies on dominant manufacturers, services or protocols.



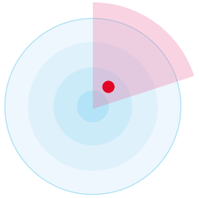
Concentration Data & Cloud Services
Intensively centralising data in the cloud leads to cluster risks. The failure of a service or central service can have an impact globally.

▲ Increased



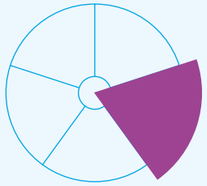
Infrastructure Integrity
Vulnerabilities may have been negligently or deliberately built into essential components of critical infrastructures, jeopardising system security.

► Unchanged



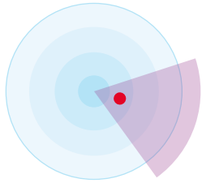
Legacy Protocols
Due to software dependencies, completely outdated and vulnerable protocols are still used (e.g. NTLMv1, SMBv1, RC4), resulting in a few applications endangering the security of entire infrastructures.

► Unchanged



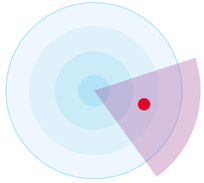
Technology dynamics

This term refers to threats that emanate from rapid technological innovation and those that benefit from the increasingly easy and cheap availability of IT media and expertise. This leads to more areas of attack, increases the availability of attack tools and offers attackers new opportunities to create new threats through their own development.



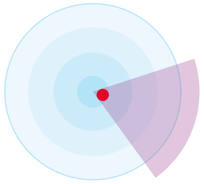
5G Security
5G is still a new mobile telecommunications technology. Its introduction will bring many opportunities as well as still unknown threats.

► Unchanged



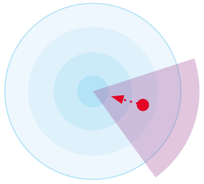
Quantum Computing
Quantum computers can render existing cryptographic methods useless because they can bypass them in a very short time.

▼ Decreasing



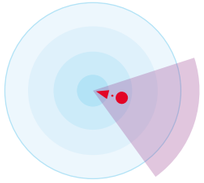
Ransomware
Critical data is encrypted on a large scale and (possibly) decrypted again in return for a ransom payment.

▲ Increased



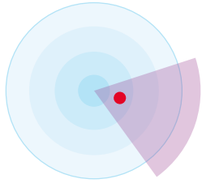
Increased Complexity
The complexity of systems, especially across technology and company boundaries, is constantly increasing. IT landscapes are becoming more complex, especially in the hybrid/multi-cloud environment with its many cloud providers. This increases risk exposure and makes troubleshooting more difficult.

▲ Increased



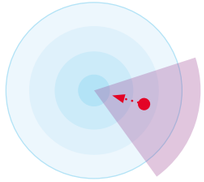
AI-Based Attacks
AI-based attacks are more targeted and therefore more difficult to detect. They can be carried out more efficiently on classic attack vectors such as ransomware, phishing, spear phishing and occasionally also in new scenarios such as deep fakes, disinformation and similar.

▲ Increased



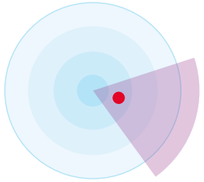
Targeted Attacks
Targeted and complex attacks to achieve a specific goal. Key people are identified and targeted directly or indirectly (lateral movement, social-engineering methods) in order to obtain relevant information or cause maximum damage. One essential aspect is persistence, which means the attackers operate undetected for as long as possible and they switch up the type of attack channels (email, SMS and even by traditional mail).

► Unchanged



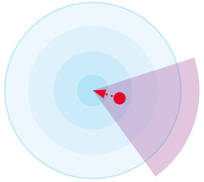
DDoS Attacks
A denial-of-service (DDos) attack is a malicious attempt to disrupt the normal data traffic of a target server, service or network by flooding the target or surrounding infrastructure with a deluge of internet traffic. DDoS attacks achieve their effectiveness by using multiple compromised computer systems as sources of attack traffic. The types of machines that are exploited can include computers and other networked resources such as IoT devices. Strong growth along with the insufficient protection of equipment such as IoT devices leads to more 'takeover candidates' for botnets.

▲ Increased



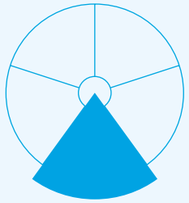
Supply Chain Attacks
Supply chain attacks aim to exploit trust and commercial relationships between a company and external parties. These relationships may include partnerships, supplier relationships or the use of third-party software.

▲ Increased



Subscriber Compromise
Malware gains access to the private data of mobile users or is used to attack the telecommunications or IT infrastructure. Phishing, Smishing, vishing and MFA-bypass-attacks target subscriber credentials. Entire digital identities are consequently stolen and taken over during the follow-up attacks.

▲ Increased



Organisation

Organisation means threats that emanate from changes in organisations or that exploit weaknesses in organisations.

Workplace Heterogeneity
In addition to the many opportunities that new working models bring, the uncontrolled use of models such as Bring Your Own Device (BYOD) or the increased use of remote workplaces, leads to greater risk exposure.

► Unchanged

Decentralised Development & Operations
Traditional development departments are ‘dying out’ and application development is gradually being undertaken by business units themselves while release cycles are becoming shorter. This makes it more difficult to control/manage security.

► Unchanged

Insider Threat
Partners or employees manipulate, misuse or sell information negligently or intentionally.

► Unchanged

Digitalisation
The way the real world is increasingly connected to the virtual world in both private and business domains is creating more avenues of attack. The ‘New Work’ concept and the shift to remote working also increase cyber risk and the vulnerability of the IT infrastructure via unsecured end devices.

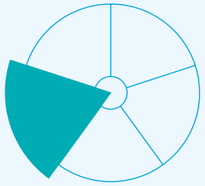
► Unchanged

Security Skills
Due to the complexity of cyberattacks and advancing digitalisation, security skills and the deployment of cyber professionals within organisations are becoming indispensable. The threat of 'downskilling' – the unlearning of knowledge – through automation in IT can lead to new attack vectors. For example, SCADA systems can no longer be operated and maintained by skilled workers.

▲ Increased

Infrastructure Misconfiguration
Exploitation of misconfigured infrastructure components and/or vulnerabilities that are identified and fixed late. The fact that technical operating processes are automated more than ever before will have a greater impact if there are successful attacks or misconfigurations.

▲ Increased



Physical

This term covers attacks on infrastructure in cyberspace that will cause increased damage in the physical world. But it also includes threats that emanate from the physical environment, which are usually aimed more at physical targets.

Device Theft
The theft or other loss of end devices such as smartphones and laptops as well as relevant IT components can lead to data loss or affect the availability of IT services.

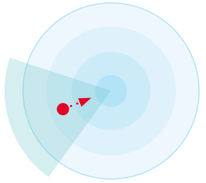
▼ Decreasing

Energy Instability
Attacks on critical infrastructure such as power grid operators. Safeguarding against failure is essential and business continuity is increasingly being discussed in the cyber resilience debate. Power shortages, blackouts (widespread power failures) or even blueouts (widespread failure of water supply) are important issues. According to the media, the vulnerability of critical infrastructures to cyberattacks has increased considerably.

▲ Increased

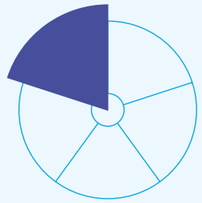
Unsecure IoT/OT Devices
Whether operational technology (OT) for monitoring and controlling physical processes, devices and infrastructures, or IoT devices – the Internet of Things is forever present. A wide variety of tasks – from the simple to the complex – are performed here, ranging from home entertainment applications, controlling robots on a factory floor to monitoring critical infrastructure (CI). Poorly protected devices – of whatever kind – can be compromised and sabotaged. This means their functions can be restricted in terms of availability or data integrity.

► Unchanged



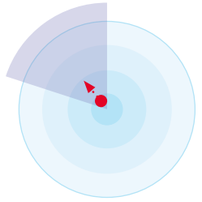
Targeted Sabotage
This concerns targeted attacks on important critical infrastructure, utilities and connections, which can significantly restrict the functioning of the internet. The targeted sabotage of critical fibre optic cables is increasing and is a danger that needs to be monitored. Countermeasures are difficult to implement, so rapid detection and fallback solutions need to be relied upon.

▲ Increased



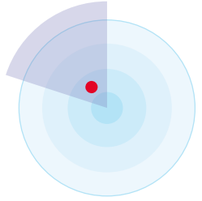
Environment/Social

This refers to threats that emanate from socio-political changes or is when misuse becomes easier due to these changes, which makes it more valuable to attackers.



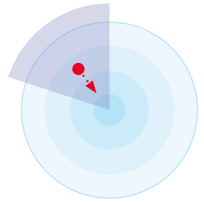
Security Job Market
The demand for security professionals is enormous and can only be met with great difficulty. This leads to decreasing levels of expertise that are needed to combat increasingly complex and intelligent attacks.

► Unchanged



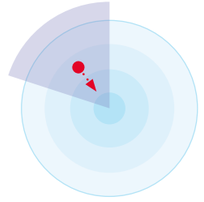
Digital Identity
Authenticated, personal digital identities can be misused or stolen. For example, this information can be used to sign off contracts under someone else's name.

▲ Increased



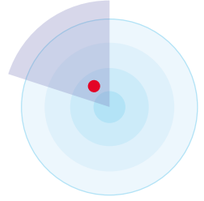
Disinformation & Destabilisation
The deliberate dissemination of false information can lead to economic and social destabilisation and is increasingly being used in a targeted way via cyberspace, especially in crisis scenarios.

▲ Increased



Political Influence
Political trends can influence technological or economic decisions, such as in the selection of technology suppliers. This can lead to new risks.

► Unchanged



Big Data Analytics
More data and better analytical models can be misused to influence people's behaviour. Decisions are increasingly left to autonomous systems. Data from 'big data lakes' is used specifically for disinformation, fake news, social and psychosocial analyses and to create movement patterns. Privacy violations accompany the latter.

► Unchanged

Conclusion

Security by Design viewed as a consistent consideration that integrates security aspects into all phases of software development – that is from the idea to the introduction and use of products – is not only becoming increasingly important but also forms the backbone of stable cybersecurity within companies and organisations.

In combination with a human-centred security approach, which involves continually sensitising employees to security issues, companies can become more secure and prepared for impending crisis situations.

Anyone who takes the time to identify possible risks will quickly realise that there are all kinds of conceivable crisis scenarios that could jeopardise their company. These risks must be discussed and analysed. Burying your head in the sand is certainly not a sustainable option and is not recommended.

Dealing with cyber risks is challenging. However, it is immensely important to keep the risk profile in mind and to be generally aware of the various cybersecurity risks – and also the associated default risks.

So when existing ways of thinking, concepts and technologies no longer provide satisfactory answers, new ways of thinking, approaches, roles and technologies have to be tried out, introduced and established. And that requires a well-thought-out vision, a strategy, courage and a lot of perseverance.

This investment in the future therefore poses a huge challenge for companies. And that is precisely the issue.

Re-examining and rethinking existing thought patterns and processes within IT departments is often very difficult and requires a lot of effort and patience. But it is precisely these kinds of changes that are sometimes acutely necessary in order to protect your company from threats. Because there is no doubt that cyber risks are evolving at a fast pace. Only companies that keep pace and have agile security will continue to be adequately protected against cybercrime in the future.

“The synergy between people, processes and technologies forms the foundation for creating corporate resilience and stability in uncertain times.”

Notes

Imprint

Publisher	Swisscom (Switzerland) Ltd, Group Security
Concept / Realisation	Agentur Nordjungs, Zurich
Editors	Swisscom (Switzerland) Ltd Marcus Beyer (Group Security) Manuel Bühlmann (Group Communications) Claudia Lehmann (B2B Communications)
Translation	Apostroph Bern AG
Copyright	© May 2023 by Swisscom (Switzerland) Ltd, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Print	OK DIGITALDRUCK AG, Zurich
Edition	200 copies

Swisscom is leading the way and developing innovations that people can build on and trust. As 'Innovators of trust'.

Are you looking for a cybersecurity role at Swisscom? Take a look at our current vacancies and apply today: swisscom.com/securityjobs

For further information about our products, services and our commitment to security in Switzerland, visit swisscom.ch/en/about/security.html

#BeTheStrongestLink