swisscom

Cybersecurity Threat Radar 2026

Geopolitics and disruptive technology as threat drivers

Contents

Trust is not a promise you make once, it's a responsibility that we have to face up to every day. As Innovators of Trust, we not only protect data, but also Switzerland's digital reliability and sovereignty.

Cybersecurity Threat Radar

Geopolitics and disruptive technology as threat drivers

Every day, we at Swisscom not only protect systems, but we also promote the digitisation of Switzerland. Millions of people rely on stable networks, secure communication and digital resilience. As CSO, I see every day how geopolitical tensions and technological leaps have a direct impact on security. Nowadays, threats arise globally, but their effects can also affect us locally at any time.

This Cybersecurity Threat Radar is our early warning tool. It shows us where threats are shifting to, which new patterns are emerging and where action is needed. This year, I was particularly concerned about the fact that, for the first time, we had to include hybrid warfare, the mixture of traditional military means with cyberattacks, disinformation as well as digital and political influence, as a new threat vector. This development shows how closely physical and digital security are now intertwined.

Geopolitical uncertainties and economic conflicts of interest are leading to an increase in state-motivated cyberattacks. Attacks that challenge not only companies, but also the digital stability of the whole of Switzerland. As a telecommunications provider, we feel how crucial adaptability and resilience have become.

Disruptive technologies are also changing the playing field. Artificial intelligence, quantum computing and connected devices are opening up enormous opportunities for innovation – and at the same time new areas of attack. Protecting digital Switzerland and the people who rely on us every day remains a top priority for Swisscom.

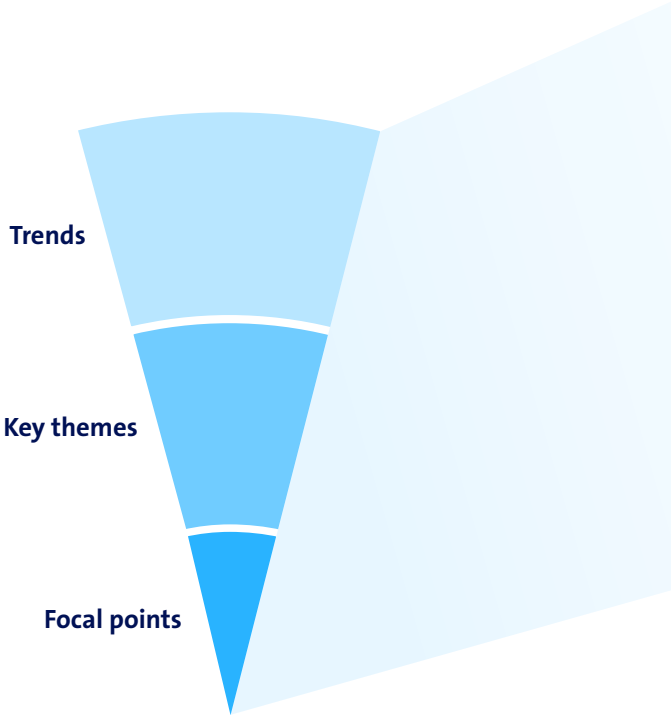
All this shows: Security is not a matter of course, but an ongoing process. It requires forward-looking action, the continuous analysis of new threats and a security culture that is practised throughout the company. Only if we continuously develop and consistently implement our safety measures will we be able to effectively counter the complex risks of our time and reliably strengthen digital Switzerland.

Marco Wyrsch
Head of Group Security
& Chief Security Officer

Situational awareness – threat radar

Being able to fall back on tried and tested security strategies and procedures at the right moment 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 Cybersecurity Threat Radar to map the current threat status and its evolution.




Environment/Social
Dominant Players
Technology Dynamics
Organisation
Physical
Security Job Market
Geopolitical Situation / State Level Attacks
Data-Centric Risks
Identity Theft & Impersonation
Disinformation & Destabilisation
Political Influence
Hybrid Warfare
Environmental Influence
Targeted Sabotage
Unsecure IoT/OT
Digital Transformation Risks
UAS Threats
Energy Instability
Manipulated Generative AI
Cloud Ecosystem Dependencies
Legacy Protocols
Infrastructure Integrity
Subscriber Compromise
Agentic AI
Increased Complexity
DDoS Attacks
Ransomware
AI-Based Attacks
Supply Chain Attacks
Targeted Attacks
Unsecure AI
Residential Proxies
Fraud
Security Skills
Insider Threat
Quantum Computing
Infrastructure Misconfiguration
Fragile Workforce
Decentralised Development & Operations
Workplace Heterogeneity
Challenges
Today
Tendency

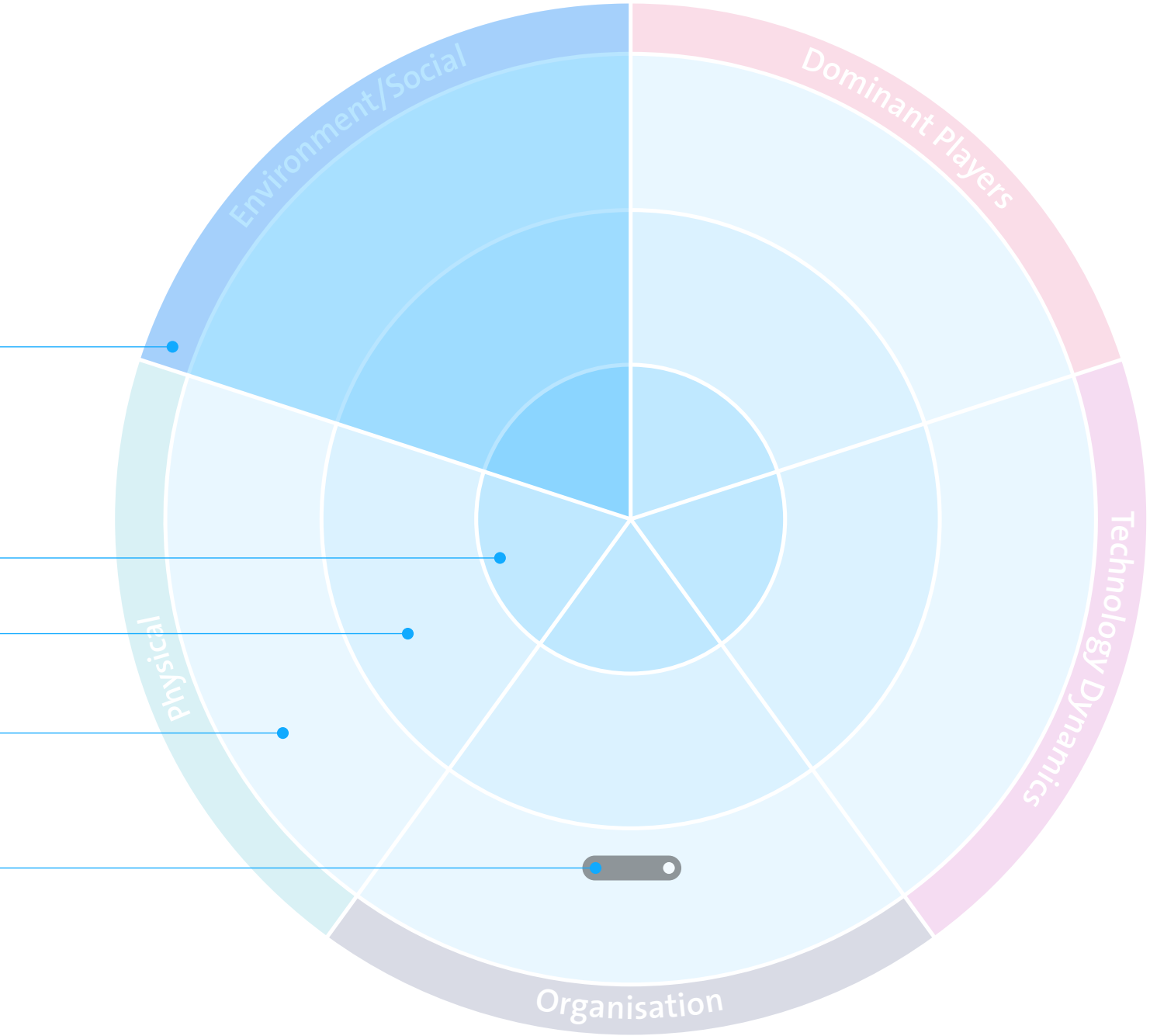
Method

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 three 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.

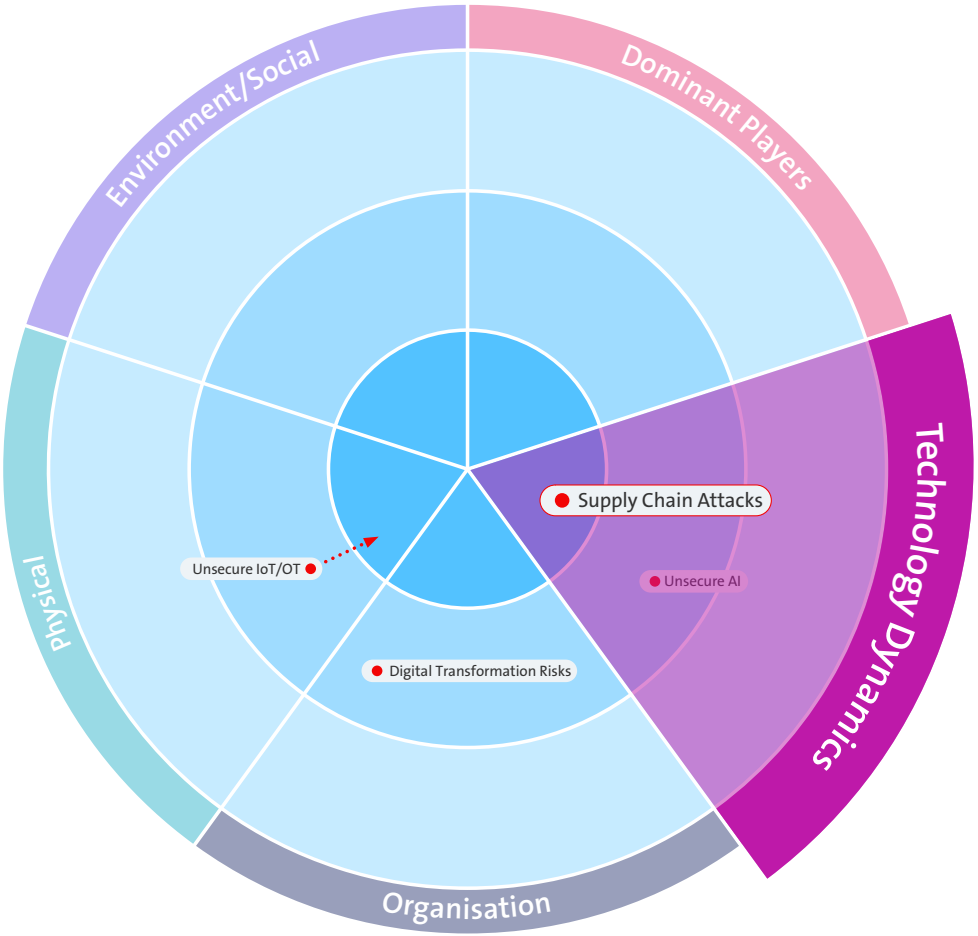
We identify the circles as:

- **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.

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.


Environment/Social
Dominant Players
Technology Dynamics
Organisation
Physical

The software supply chain in the supply chain: a house of cards made from foreign code



In an increasingly digital business world, companies are dependent on a variety of software solutions and services. The integration of external components and modules has long since become the standard – and this is precisely one of the greatest challenges of today's IT security: Supply chain attacks, i.e. attacks on the supply chain of software. One weak building block is all it takes to collapse the entire house of cards.

Modern software is created from hundreds of external components and automated build pipelines. The origin and quality of this third-party code are often not transparently traceable, which makes identifying vulnerabilities much more difficult. It is precisely this intransparency that makes the supply chain a preferred target for attackers: Even just one compromised library or one manipulated CI/CD system can affect thousands of companies.

It is a particularly delicate fact that many companies rely on components whose security level they cannot check themselves.

Current threat status: examples and development trends

In 2025, incidents in the npm ecosystem (npm is the largest registry for JavaScript packages) such as 'Shai-Hulud' made it clear that a new reality has dawned: Attackers specifically target open-source code and abuse the trust chain of popular packages to spread malware through seemingly legitimate updates. Because updates are often adopted without additional security checks or manual control and then distributed as dependencies, such attacks can spread particularly quickly along the entire software supply chain.

In addition, there are so-called single points of failure, central services or providers whose failure or compromission, as recently with CrowdStrike, Microsoft or Cloudflare, can have significant consequences for many companies.

Loss of data, business interruption and damage to reputation

The consequences of successful attacks on the software supply chain are serious: In addition to the loss of sensitive data, there is a risk of business interruptions, which in the worst case can lead to the standstill of business-critical processes. The damage to reputation caused by publicly disclosed security incidents should also not be underestimated and can permanently shake the trust of customers, partners and investors.

Strengthen verifiability and resilience
Technical and organisational measures are required to meet the challenges of the modern software supply chain. These include, but are not limited to:

- Consistent documentation and follow-up of all modules used and the associated updates
- Regular security reviews (audits) and penetration tests along the entire supply chain
- Establishment of clear processes for the selection, evaluation and approval of external software components
- Use of monitoring solutions that detect and report suspicious activities at an early stage
- Development and implementation of update strategies to close known vulnerabilities in a timely manner

In regulatory terms, the European Union's **Cyber Resilience Act (CRA)** and the **Network and Information Security Directive 2 (NIS2)** mark a turning point: Manufacturers must prove how their software was created, and operators must check this evidence. SBOM (Software Bill of Materials), reproducible builds, signatures and documented vulnerability management are therefore mandatory. Integrity and origin are no longer assumed, but technically proven.

Two concepts are central to this:

- **Integrity:** Is an update genuine and unchanged?
- **Provenance:** How, where and what was it built?

Standards such as SLSA (Supply-chain Levels for Software Artifacts) or signed SBOM provide for forgery-proof evidence for the first time. Since such checks are hardly possible manu-

> Only when each software artefact is cryptographically signed and its origin can be proven beyond doubt will the basis for genuine trust be in place.

Florian Lukavsky
Chief Innovation Officer, SignPath

ally, specialized platforms for software supply chain security adopt automated, cryptographically secured attestations directly in the build process. This makes security verifiable and no longer purely a matter of trust.

Organisationally, a rethink is also required. Companies must continuously monitor their supply chain, actively manage vulnerabilities, and require their partners to adhere to minimum standards in order to remain resilient to supply chain attacks. Raising employees' awareness of the risks and creating a safety culture are also key elements.

Resilience and continuous review are key

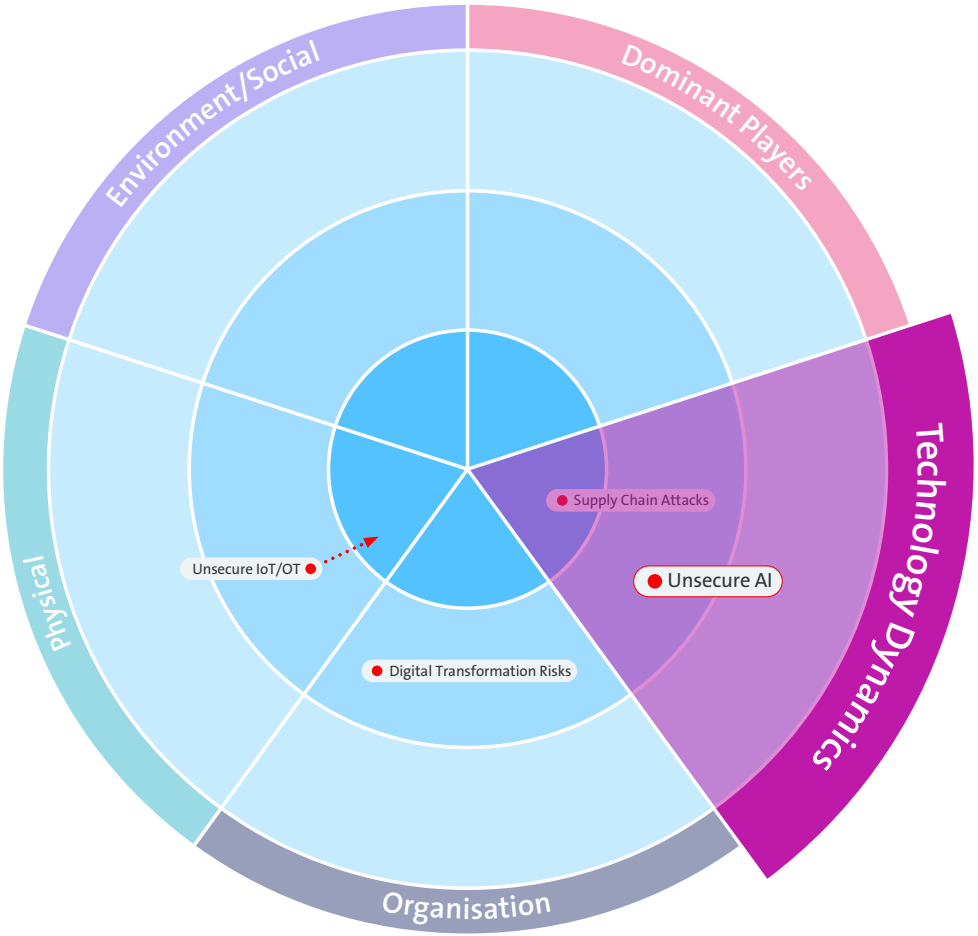
Companies will continue to be faced with the threat of supply chain attacks in the future and this threat will only increase. Anyone who relies on the benefits of modern, modular software must be aware of the risks and consistently invest in their own resilience. Continuous monitoring, transparency and holistic risk management are the cornerstones of keeping your own IT house of cards stable even in turbulent times and avoiding playing Russian roulette in the software supply chain.

> Today, this is not yet possible entirely without trust. However, it is imperative to deal with possible weaknesses in the software supply chain, for example by means of targeted threat modelling of the entire supply chain.

Simon Röthlisberger
Security Architect

Challenges and trends

All-out AI offensive – the risk multiplier



Artificial intelligence has spread at an impressive rate in many areas of our society and economy. The hype surrounding AI technologies is so great that critical questions about security, transparency and sustainability can take a back seat. In particular, the threat vector 'Unsecure AI' shows how quickly ignorance can become a dangerous system architecture – with effects that extend far beyond IT.

This article explores why we need to address unsecured AI, how these risks arise, and what specific actors can do to address the challenges positively and responsibly.

Why Unsecure AI is becoming a risk

Enthusiasm for AI often leads people to introduce innovations without a sound understanding or sufficient security considerations. AI systems are deployed without knowing where and how they influence operational decisions, what data they were trained with, or who was involved in the development process. Low-code and no-code solutions are often used whose origins and architecture are not traceable to users. It is particularly critical that partner companies also integrate AI, which creates supply chain risks (see page 10) that are difficult to control. In addition, malware is increasingly being implanted directly into systems during coding – for example, through generative AI.

However, technology is not the only thing that poses a danger. A lack of expertise on the part of users and cyberexperts exacerbates the problem. The fallacy that junior specialists could be replaced by AI will lead to a skills gap that could weaken the entire security structure in the medium term, including areas such as data quality management or supply chain management.

How do the vulnerabilities arise?

Insufficiently secured AI arises when security processes are neglected, transparency requirements are ignored, and governance rules are not adhered to. AI models are used in productive systems without their functionality, data base or decision logic being checked and documented.

Low-code tools and platforms make it possible for even less experienced people to create AI applications – an innovative advantage that also increases the area of attack if you rely 100% on AI outputs. In the supply chain, models and data are often adopted from third parties without being aware of security risks and implementing uniform security standards in advance.

The use of AI in bug bounty management, where reports become automated and thus more numerous but qualitatively inferior, clearly shows how challenging it is to distinguish between real vulnerabilities and fake reports. All in all, this creates a patchwork of systems in which no one has an overview of how, where and with what integrity AI is used.

Positive strategies for greater security
The risks are great, but there are numerous ways in which companies and private individuals can respond constructively to these challenges:

- **Create transparency:** Every AI application must be documented – including the origin of the data, the algorithms used and the decision logic. This is the only way to understand and control risks.
- **Training and awareness-raising:** Continuous training for everyone involved is essential. AI expertise must not only be reserved for experts, but must also be anchored throughout the organisation.
- **Multidisciplinary teams:** Teams from IT, Legal, Ethics and other departments should also be involved in the development and implementation of AI. In this way, different perspectives and skills are used to identify risks at an early stage.
- **Accountability and governance:** Clear responsibilities for AI systems and rules for using AI should be defined. This also includes audits and reviews being carried out by independent bodies.
- **Error culture and dialogue:** Errors and security loopholes should be communicated openly in order to learn from them and continuously improve processes. Dealing with weaknesses transparently strengthens the entire organisation.

> In a world of low-code chaos and AI automation, a bug bounty program becomes a seismograph for real risks.

Antoine Neuenschwander
Head Bug Bounty

- **Ethics and sustainability:** In addition to technical and economic criteria, every AI application must also be evaluated from an ethical and social point of view.
- **Promoting young talent:** The promotion of young talent in the security sector remains key. Juniors and seniors must work together on solutions – AI can supplement expertise, but not replace it.

Involve employees
It is important to openly address ethical, moral and sustainability-related aspects of AI. In order for employees to keep pace with the rapid development of AI, an appropriate environment must be created. Employee skills can be strengthened through targeted training, for example through awareness-raising formats such as promptathons.

This corresponds to active and conscious change management.

> If we want to launch an all-out AI offensive in companies, we need above all leadership that puts humanity before speed in digitalization. Culture is not created by tools, but by role models. And before we scale AI, we first have to empower people.

Marcus Beyer
Security Awareness Officer

Digital sovereignty: Who has the last lifeline in the transformation vortex?

Whether in day-to-day life or at work: Digital transformation has long been implemented everywhere and brings with it completely new rules for companies in Switzerland. Data is becoming increasingly important, IT is migrating to the cloud and many processes are now run externally. This is precisely why the issue of digital sovereignty is so popular at the moment. And the geopolitical changes are increasing the level of urgency. More than ever, companies need to keep track of their data and digital processes – not an easy task in a connected world.

However, what exactly does digital sovereignty actually mean and why is it so important for Swiss companies at this specific point in time? As digitisation progresses steadily and more and more processes are being shifted from the hands of companies to the cloud or external service providers, the question arises as to how organisations can secure their ability to act and maintain control. It therefore requires a clear understanding of what digital sovereignty entails and the specific challenges and opportunities associated with it.

As a general rule, companies and organisations must always be able to control, manage and protect their digital assets – especially data and IT infrastructure – autonomously and independently. Dependence on external foreign service providers, in particular with regard to cloud and outsourcing services, must not exceed an appropriate level.

Digital sovereignty is relevant to Swiss companies for several reasons:

- Data protection laws such as the revised Swiss Data Protection Act (rev-FADP) and the European GDPR require companies to know where their data is stored and who has access to it.
- Control over data and systems is a key factor in information security. The more dependencies there are on third parties, the larger the area of attack.
- If you do not control your data, you lose access to your most important capital in the worst-case scenario and run the risk of losing your innovative strength and market position.

Outsourcing and cloud: loss of control as a risk – illusion of data sovereignty?

The outsourcing of IT services and the use of cloud platforms offer enormous benefits in terms of scalability, cost and flexibility. For Swiss companies in particular, outsourcing to specialised providers often makes economic sense. At the same time, some control over data and processes is lost with every outsourcing step.

Many companies underestimate the risks associated with disclosing data to third-party providers:

- **Dependence on provider:** Switching costs and technical hurdles make it difficult to switch or retrieve providers ('vendor lock-in').
- **Loss of transparency:** It is often unclear where and how data is actually processed, especially with international cloud providers.
- **Legal uncertainty:** Different jurisdictions (e.g. due to storage in the EU or the USA) make it difficult to enforce your own data protection and security requirements.
- **Cybersecurity risks:** The concentration of sensitive data in large cloud platforms makes them attractive targets for cybercriminals.

The frequently invoked data sovereignty often remains an illusion in practice – especially when companies do not have the necessary control mechanisms and skills to manage their data flows and dependencies.

With the revised Data Protection Act (revFADP), Switzerland has had one of the most modern data protection regulations in Europe since September 2023. Swiss companies must implement the principles of 'privacy by design' and 'privacy by default', respect the rights of data subjects and fulfil notification requirements in the event of data breaches.

Of particular relevance is the question of whether and how data may be transferred abroad. Strict requirements apply here for transmission to third countries – especially if they do not have an adequate level of data protection. For many companies, this raises the question of whether cloud and outsourcing partners should be based in Switzerland or abroad.

> Today, all companies must be aware of their digital sovereignty and actively manage it.

Lukas Hebeisen
Senior VP Cloud & Datacenter Solutions

Major Swiss providers such as Swisscom explicitly position themselves as trustworthy partners for digital infrastructure and offer cloud solutions with data storage in Switzerland. In doing so, they address the specific requirements of data protection and sovereignty that are decisive for many companies.

In addition to data storage in Switzerland, the question of which law the provider is subject to is also relevant. You should be aware that US providers are subject to US law, even if the data is stored in Swiss data centres.

'Plus AI or Minus AI?' – impact on digital sovereignty

The current debate around artificial intelligence is increasingly dominated by a field of tension that can be roughly divided into two camps: Plus AI – the optimistic view of the technological possibilities – and Minus AI – the realistic to critical view of risks, dependencies and loss of control. This area of contention is particularly relevant for Swiss companies, as it has an impact on the issue of digital sovereignty to an unprecedented extent.

On the one hand, the use of AI promises enormous benefits: automation of repetitive tasks, increased efficiency, data-driven decision-making and new innovation models. Companies that use AI systematically and responsibly create a significant competitive advantage and can strengthen their digital resilience. In this context, AI can even be a driver of sovereignty – provided companies retain sovereignty over their data, models, and value chains.

> Digital sovereignty arises where critical data and applications are identified and trusted, local solutions are selected for them. This does not exclude the use of innovative global services for less critical areas.

Thomas Stemmler
Head of Regulatory & Policy

On the other hand, AI technologies are exacerbating existing risks of digital transformation. With each new generation of AI systems, dependence on large, often international, technology providers increases. Models, training data, infrastructure and maintenance are often beyond the direct control of companies. The risk of 'shadow AI', i.e. the use of unauthorised or uncontrolled AI tools in day-to-day work, is increasing and undermines existing governance structures. This is compounded by the increasing complexity of regulatory requirements, which makes the legally compliant use of AI even more difficult. In this 'Minus AI' scenario, digital sovereignty quickly becomes a challenge – or even an illusion.

It is not the technology that decides whether AI strengthens or weakens digital sovereignty. Rather, it is about the way companies deal with it. Conscious choice of partner, transparent data flows, clear AI governance, internal competencies and technical protection mechanisms are decisive in determining whether AI leads to a gain in sovereignty or a loss of control. Companies that invest in these capabilities can use AI as a strategic lever – not only for efficiency and innovation, but also for protecting their digital independence.

Actionable recommendations: What can companies actively do to remain digitally sovereign?

To ensure that digital sovereignty does not become an illusion, Swiss companies should take the following measures:

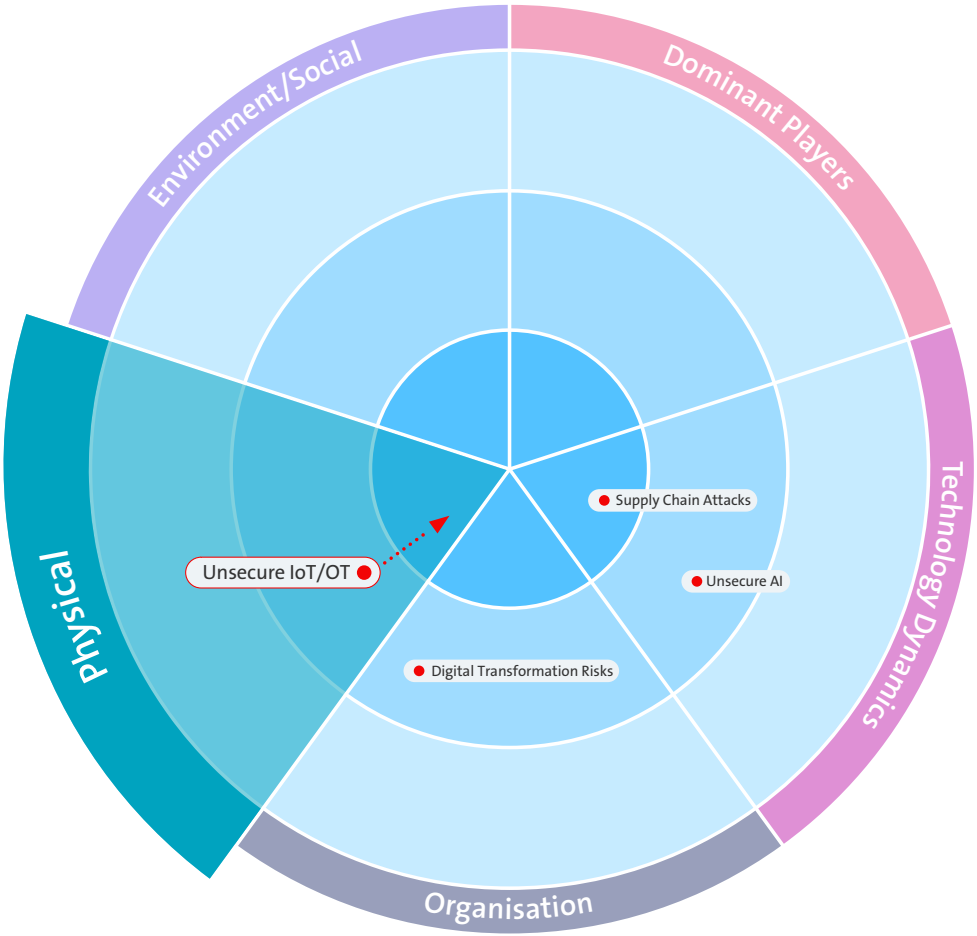
- **Strategic management:** Define a clear digitalization and data strategy that also governs how to deal with external service providers and cloud services.
- **Risk assessment and management:** Regularly analyse the risks of outsourcing and cloud usage and develop contingency plans in case of data loss or misuse. Also assess the impact if you lose access to your IT systems at short notice or if a manufacturer changes the general conditions at short notice.
- **Technical and organisational measures:** Use encryption, access management and monitoring to make data throughput and access transparent and controllable.
- **Contractual protection:** Ensure clear contractual rules on data protection, data access, data portability and exit strategies when switching service providers.
- **Careful choice of partner:** Rely on providers that guarantee data storage and processing in Switzerland. Regularly check compliance with the agreed standards.
- **Training and sensitisation:** Train employees regularly on how to handle sensitive data and the risks associated with digital transformation.
- **Regulatory monitoring:** Follow developments in data protection and continuously adapt your processes to new legal requirements.

Sovereignty as a goal

Full control over all digital processes and data is hardly realistic in a globalised, digitised economy. Digital sovereignty remains a challenging goal that companies can only achieve through a combination of strategic management, technical expertise and careful selection of partners. Outsourcing and cloud use are not inherently associated with a loss of control, provided companies take the right measures and actively manage their risks. This task is complex and requires very specialised knowledge. The decisive factor is to consciously determine which competencies are developed internally and which are acquired externally.

Those who are aware of the risks, act proactively and rely on trustworthy partners can make the digital transformation successful and secure – and thus emerge stronger from it rather than being lost in the vortex of transformation.

OT security: the elephant in the room that is slowly becoming visible



What do production facilities, supply infrastructure, traffic systems, medical devices and building automation have in common? Many of these systems, which are important for the operation of companies, have been heavily neglected from a cybersecurity perspective in recent years – and are now increasingly exposed to threats. The ongoing digitisation of production, the growing interest of cybercriminals in 'easy prey' and the changing global security situation have led to an increase in attacks on critical infrastructure.

The resulting risks for companies are manifold: high costs due to damaged machinery, unusable production, reputational damage, environmental damage and even immediate danger to life and limb of employees.
For a long time, these risks were the proverbial elephant in the room that no one really wanted to talk about. That's over, the elephant is becoming increasingly visible and can no longer be ignored.

Operational Technology (OT) encompasses all systems that control, monitor, automate and interact with physical processes in the real world: from building technology, production lines and energy supply networks to medical devices in hospitals. With increasing connectivity – keywords Industry 4.0 and IoT – the boundaries between IT and OT are becoming increasingly blurred. The interface between IT and OT is the most critical point of modern system architectures. While the paradigm of confidentiality dominates in IT, availability and immediate response time are paramount in OT. A system restart after a security update, which is routine in IT, can lead to a production stop in OT, which can have a direct impact on the balance sheet.

The biggest challenges are:

- **Protocol diversity:** OT systems often use proprietary or outdated protocols that were not originally designed for networking with the Internet.
- **Different life cycles:** While IT hardware is replaced every three to five years, OT systems are often in use for decades – including outdated operating systems for which there are no longer any security patches.
- **Malware transit:** Insecure interfaces enable ransomware to move directly from the office network to the control level (PLC) and physically manipulate production.
- **The 'air gap' does not offer absolute protection:** A compromised technician's laptop is all it takes to send malicious code straight into the heart of production. This direct access allows attackers to bypass traditional IT defence mechanisms and directly exploit vulnerabilities in industrial components.

OT systems that have evolved over time date from an era before networking. They are often based on outdated software without modern authentication, while rigid certification processes block necessary security patches. The result: Standard IT security mechanisms are often not technically feasible in these environments or can lead to incalculable failures.

What is at stake for companies?

The risks range from production downtime due to sabotage or manipulation to reputational loss and – in critical infrastructure such as energy, water or the healthcare system – even endangering human lives. Legal and regulatory consequences must also be taken into account, as non-compliance with security requirements can result in significant fines or liability risks.

Many companies underestimate this risk because 'nothing has happened' so far. However, particularly spectacular attacks such as Stuxnet, BlackEnergy, the Colonial Pipeline and the attacks on hydropower plants in Poland and Norway prove that OT systems are in the sights of hackers and that the threat is very real.

Regulatory pressure

Legislators and regulators are taking the risks to critical infrastructure increasingly seriously. Examples of this are the updates to the Swiss Electricity Supply Ordinance, which requires energy companies to align themselves with the minimum ICT standard. Or the EU's NIS2 regulation, which also applies to many Swiss companies with customers in the EU.

What can companies do?

The good news is that there are proven approaches to improve OT security: Identify, Protect, Detect, Respond and Recover – these well-known steps from the NIST framework help and give the whole thing a structure in OT security.

Identify: The first step is – as almost always – transparency. Companies should have a clear overview of which OT systems are in place, how they communicate with each other, with IT or the Internet, and which system has critical vulnerabilities. Such a continuously updated inventory forms the basis for any risk management.

Protect: The best possible separation of OT from IT, fine-grained segmentation in the OT network and – where possible – endpoint protection and vulnerability management are important preparatory measures for minimising risks. This also includes limiting access to OT systems through stringent access management.

> Long life cycles and proprietary systems are no longer an excuse – with increasing connectivity, the responsibility to protect OT systems just as consistently as traditional IT increases.

Thomas Dummermuth
Head of Physical Security

A decisive factor is raising awareness among employees. Those who are familiar with the specific risks and best practices can actively contribute to security in their day-to-day work.

Detect: At the same time, continuous monitoring makes sense. OT networks should always be monitored for irregularities and attack indicators in order to be able to react quickly in an emergency. Intrusion detection systems (IDS) specialising in OT are available for this purpose, which trigger an alarm in the event of abnormal behaviour. The definition of what is considered 'abnormal' is highly industry-specific and requires appropriate expertise from the security partner.

Respond & Recover: However, in an emergency, you also need the ability to react – even outside office hours. A convergent IT/OT SOC is a helpful approach, but it usually also requires procedural adjustments in the company, such as clarification of responsibilities or alarm chains. These must also be coordinated with the most important suppliers in order to ensure prompt recovery in the event of an incident.
In order to be able to address these steps, the OT, IT and management levels must be closely involved in the security strategy. The management of OT security risks is on the agenda of the Executive Board or the Board of Directors.

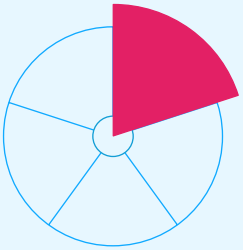
The time to act is now

Neglecting OT Security is no longer an option. If you keep your company's production at yesterday's security level, you not only risk production downtime and economic damage, but you also risk your reputation and – in the worst-case scenario – human lives. The challenge is great, but it can be solved. It is crucial that companies approach the issue proactively and understand OT security as an integral part of the digital transformation. The elephant is in the middle of the room – it's high time to approach him and take the right measures.

> OT security means taking advantage of the benefits of IT without jeopardising the stable operation of production. The interface between IT and OT is decisive here.

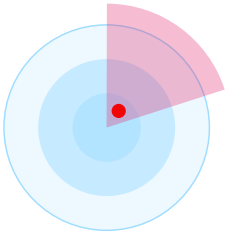
Tobias Balcon
Strategic Program Manager

Details including tendencies and comparison with the previous year



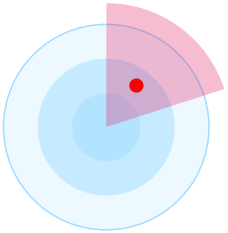
Dominant Players

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



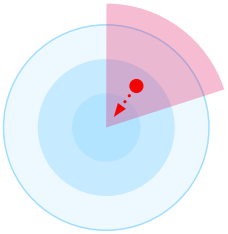
Infrastructure Integrity
Vulnerabilities may have been negligently or deliberately built into essential components of critical infrastructures, jeopardising system security.

- Unchanged



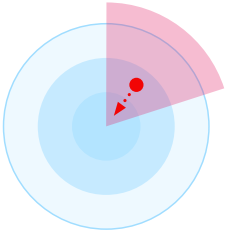
Legacy Protocols
Due to software dependencies, completely outdated and vulnerable protocols are still used (e.g. NTLMv1, SMBv1, RC4), resulting in a few applications endangering the security of entire infrastructures.

► Unchanged



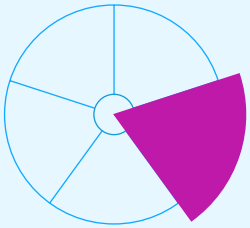
Cloud Ecosystem Dependencies
Centralised cloud ecosystems create cluster risks and dependencies that can massively impair digital sovereignty and availability in the event of disruptions or political pressure.

▲ Increased



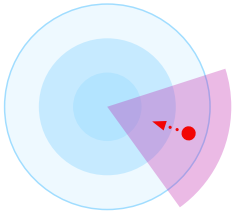
Manipulated Generative AI
Targeted manipulations can alter the output of an AI system. This may involve the infiltration of malicious, false or corrupted data during the training phase, the theft of LL models, as well as prompt manipulation, which may result in adverse and legally binding ramifications. We are talking about AI security risks and not about the risks associated with the use of AI (see AI-Based Attacks).

▲ Increased



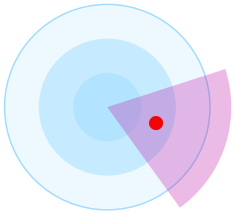
Technology Dynamics

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.



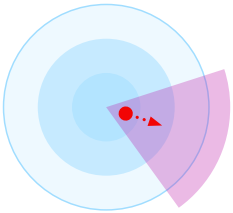
Quantum Computing
Quantum computers can render existing cryptographic methods useless because they can bypass them in a very short time.

▲ Increased



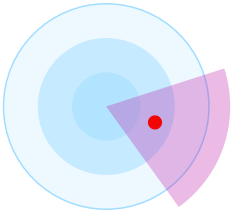
Unsecure AI
Unsecure AI systems endanger supply chains and data protection, as generative models can disclose confidential data in an uncontrolled manner. This can not only affect business continuity, but also significantly damage a company's reputation. In addition, there is a risk of regulatory consequences, particularly as a result of the AI Act, if AI decisions violate applicable regulations.

► Unchanged



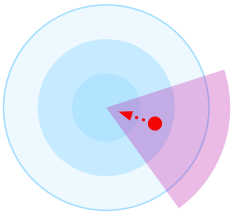
Ransomware
Critical data is encrypted on a large scale and (possibly) decrypted again in return for a ransom payment.

▼ Decreasing



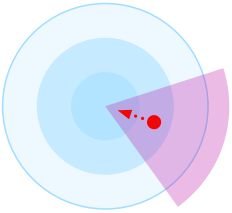
Increased Complexity
The complexity of systems, especially across technology and company boundaries, is constantly increasing. IT landscapes are becoming more complex, especially in the hybrid/multicloud environment with its many cloud providers. This increases risk exposure and makes troubleshooting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

► Unchanged



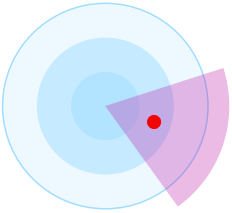
AI-Based Attacks
AI-based attacks are more targeted and therefore more difficult to detect. They can be carried out more efficiently through classic attack vectors such as ransomware, phishing, spear phishing and occasionally also in new scenarios such as deep fakes and disinformation.

▲ Increased



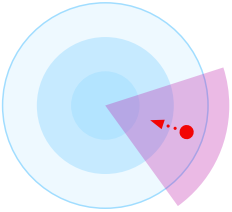
Agentic AI
Agentic AI is proactive and able to make autonomous decisions and adapt strategies. This increases the area of attack, as self-learning and adaptive systems can develop unpredictable behaviours and independently interact with peripheral systems. If these agents are compromised, this can result in unauthorised access to sensitive data and system components, which drastically increases the likelihood of escalation and fraud. Even a seemingly harmless AI assistant can cause considerable damage through incorrect instructions or manipulation on the part of the attackers.

▲ Increased



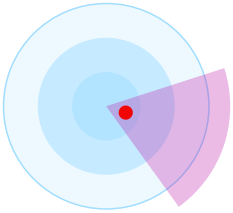
Targeted Attacks
Targeted and complex attacks to achieve a specific goal. Key people are identified and targeted directly or indirectly (lateral movement, social engineering methods) in order to obtain relevant information or cause maximum damage. One essential aspect is persistence, which means the 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



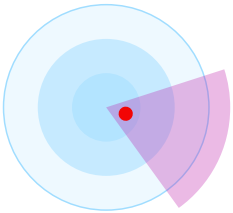
Subscriber Compromise
Malware gains access to the private data of mobile users or is used to attack the telecommunications or IT infrastructure. Phishing, smishing, vishing and MFA bypass attacks target subscriber credentials. Entire digital identities are consequently stolen and taken over during the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

▲ Increased



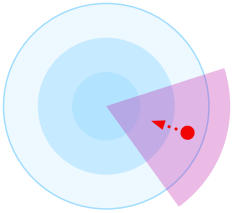
DDoS Attacks
A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal data traffic of a target server, service or network by flooding the target or surrounding infrastructure with a deluge of internet traffic. DDoS attacks achieve their effectiveness by using multiple 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.

► Unchanged



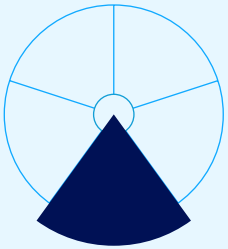
Supply Chain Attacks
Supply chain attacks aim to exploit trust and commercial relationships between a company and external parties. These relationships may include partnerships, supplier relationships or the use of third-party software. Attacks on partners' software ecosystems have reached a new dimension in this context.

► Unchanged



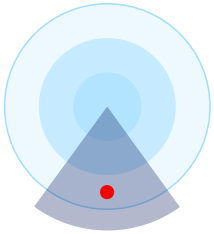
Residential Proxies
Residential proxies are connections via real IP addresses that are used to disguise the origin of data traffic. As a result, security controls that rely on IP reputation or geolocation become less effective. This promotes risks such as credentials and information theft or the circumvention of geoblocking. This also makes DDoS mitigation more difficult.

▲ Increased



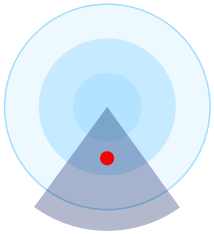
Organisation

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



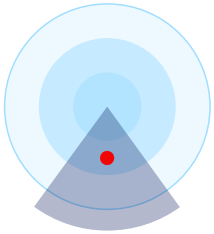
Workplace Heterogeneity
In addition to the many opportunities that new working models bring, the uncontrolled use of models such as Bring Your Own Device (BYOD) or the increased use of remote workplaces leads to greater risk exposure.

- Unchanged



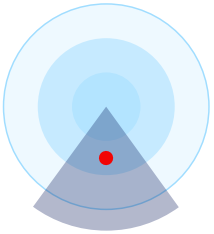
Decentralised Development & Operations
Traditional development departments are 'dying out' and application development is gradually being undertaken by business units themselves while release cycles are becoming shorter. This makes it more difficult to control/manage security.

- Unchanged



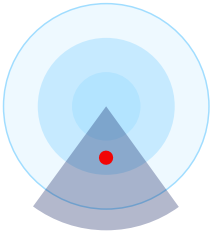
Insider Threat
Partners or employees manipulate, misuse or sell information negligently or intentionally.

- Unchanged



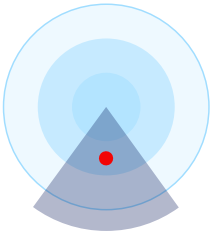
Digital Transformation Risks
The way the real world is increasingly connected to the virtual world in both private and business domains is creating more avenues of attack. The ‘New Work’ concept and the shift to remote working also increase cyberrisk and the vulnerability of the IT infrastructure via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

► Unchanged



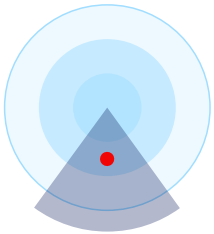
Security Skills
Due to the complexity of cyberattacks and advancing digitalisation, security skills and the deployment of cyberprofessionals within organisations are becoming indispensable. The threat of ‘downskilling’ – the unlearning of knowledge – through automation in IT can lead to new attack vectors.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

► Unchanged



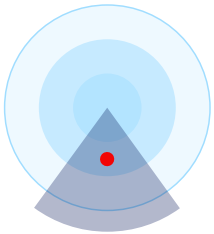
Fragile Workforce
A fragile workforce describes the vulnerability of cybersecurity and cyberdefence teams to psychological stress and a lack of stress and burnout prevention. If someone is mentally unstable and unable to perform under pressure, the likelihood of human error increases. This creates an increased risk of security loopholes and attack points that can jeopardise the stability of the entire company.

► Unchanged



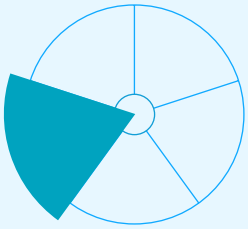
Infrastructure Misconfiguration
Exploitation of misconfigured infrastructure components and/or vulnerabilities that are identified and fixed late. The fact that technical operating processes are automated more than ever before will have a greater impact if there are successful attacks or misconfigurations.

- Unchanged



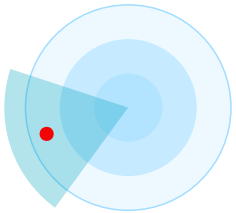
Fraud
Fraud refers to illicit activities based on deception and unlawful enrichment. It manifests itself in fraudulent transactions, identity theft or manipulated documents. Fraud poses a significant risk to companies and private individuals as it can lead to financial losses and damage to reputation.

- Unchanged



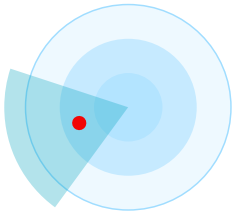
Physical

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.



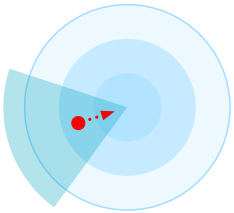
Energy Instability
Attacks on critical infrastructure such as power grid operators. Safeguarding against failure is essential and business continuity is increasingly being discussed in the cyberresilience debate. Power shortages, blackouts (widespread power failures) or even blueouts (widespread failure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

► Unchanged



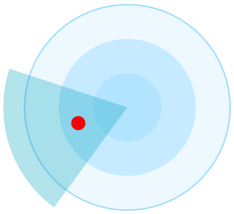
Targeted Sabotage
This concerns targeted attacks on important critical infrastructure, utilities and connections, which can significantly restrict the functioning of the internet. The targeted sabotage of critical fibre optic cables is increasing and is a danger that needs to be monitored. Counter measures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

► Unchanged



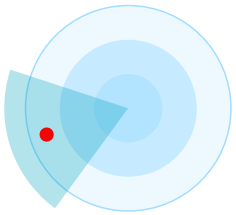
Unsecure IoT/OT
Whether operational technology (OT) for monitoring and controlling physical processes, devices and infrastructures, or IoT devices – the Internet of Things is forever present. A wide variety of tasks – from the simple to the complex – are performed here, ranging from home entertainment applications and 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.

▲ Increased



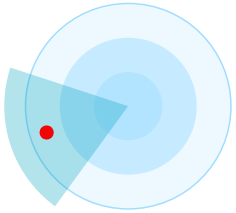
Environmental Influence
Due to the effects of climate change and urbanisation, unpredictable weather phenomena and weather influences such as heat, heavy rain, tornadoes, hail or lightning intensities are increasingly occurring, which have an impact on infrastructure resilience and thus have a high potential for damage to the external and internal environment of an information system or network.

► Unchanged



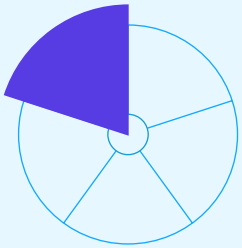
UAS Threats
UAS threats (Unmanned Aerial System Threats) refer to the risks arising from the use of unmanned aerial vehicles, i.e. drones. These range from espionage, surveillance and data theft, smuggling and sabotage to physical attacks on infrastructure or personnel. Particularly relevant scenarios in the corporate context are industrial espionage, aerial surveillance of factory premises and disrupting sensitive installations. With the increasing proliferation and autonomy of drone technologies, the security-relevant importance of this threat increases significantly.

- Unchanged



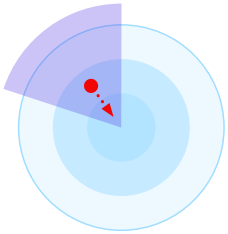
Hybrid Warfare
The combination of traditional military means with non-military tactics such as cyberattacks, disinformation, economic pressure or political influence is referred to as hybrid warfare. Because attacks are often carried out covertly, below the ‘war threshold', they are difficult to recognise and defend against. The aim is to destabilise states, undermine trust and promote social division. Their effectiveness is enhanced by digitisation, social media and global networking.

- Unchanged



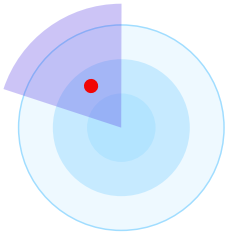
Environment/Social

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



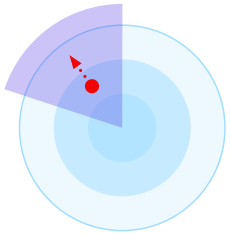
Identity Theft & Impersonation
Authenticated personal digital identities can be stolen or misused to impersonate another person or organisation. This enables attackers to gain unauthorised access to systems and information or to carry out actions such as signing contracts, making payments or communicating on behalf of others.

▲ Increased



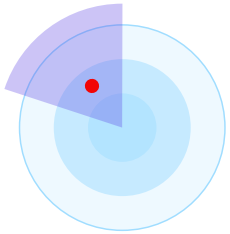
Geopolitical Situation / State Level Attacks
During times of war, terrorist activity and political instability across countries and societies, the negative effects in cyberspace are becoming increasingly apparent. Hacks are commissioned by a variety of actors, including nations, politically motivated hacktivist groups, state actors and organised crime syndicates. All these entities are placing growing pressure on companies and organisations through commissioned work. Increased attention is also being paid to collateral damage caused by hack-back strategies carried out by individual nations.

► Unchanged



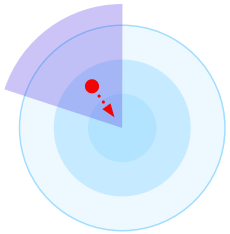
Security Job Market
The demand for security professionals is enormous and can only be met with great difficulty. This leads to decreasing levels of expertise that are needed to combat increasingly complex and intelligent attacks.

▼ Decreasing



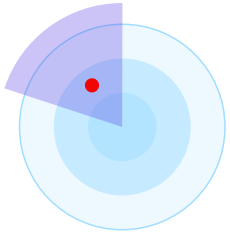
Disinformation & Destabilisation
The deliberate dissemination of false information can lead to economic and social instability and is increasingly being used in a targeted way via cyberspace, especially in crisis scenarios.

► Unchanged



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

▲ Increased



Data-Centric Risks
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

Summary

The digital transformation is leading to an ever-increasing dependence on external ecosystems.

Cloud platforms, software supply chains, AI models and industrial control systems are highly networked and often beyond the direct control of companies. As a result, traditional safety boundaries are shifted. Trust alone is no longer enough – security must be comprehensible, verifiable and controllable. The origin, integrity and dependencies of software, data and systems must be made transparent and actively managed.

This is particularly evident in supply chain attacks and digital sovereignty. Anyone who does not know how software is created, where data is processed or what legal framework conditions providers are subject to risks losing control with potentially serious consequences for the entire company. Regulatory developments such as NIS2 and CRA or data protection laws are further intensifying this pressure and making verifiable security the standard.

Artificial intelligence acts as an accelerator. It can increase productivity, innovation and resilience, but in the absence of governance it exacerbates existing risks along the entire value chain. Non-transparent models, shadow AI, loss of competence and new areas of attack make it clear: The decisive factor is not the use of AI per se, but the way in which it is introduced, controlled and accounted for.

OT and IoT security remains an often underestimated but critical area. The increasing convergence of IT and OT makes production facilities and critical infrastructure attractive targets. OT security should no longer be treated as a peripheral technical discipline; the topic is on the agenda of the Executive Board.

The 2026 threat scenario shows that risks are increasingly arising from the interplay of technology, organisation and geopolitics. Resilience is becoming a key skill – technically, organisationally and culturally.

The greatest risks arise where complexity meets a lack of transparency, automation meets a lack of responsibility and speed meets a lack of skills. The answer to this is not a single tool, but an holistic approach. Clear strategies, verifiable security, conscious choice of partner, continuous training and a safety culture that managers actively and credibly exemplify.

The developments identified in the current Cybersecurity Threat Radar make it clear that cybersecurity has long since ceased to be just a technical discipline, but a strategic success factor. Cybersecurity is not a state of affairs, but an ongoing strategic process. Actively shaping it strengthens resilience, trust and digital sovereignty.

#EngageYourSecuritySkills

Imprint

Publisher
Swisscom (Switzerland) Ltd, Group Security

Concept / Realisation
Agency Nordjungs, Zurich

Editors
Swisscom (Switzerland) Ltd
Marcus Beyer (Group Security)
Manuel Bühlmann (Group Communications)
Claudia Lehmann (B2B Communications)

Translation
Apostroph Bern AG

Print
OK DIGITALDRUCK AG, Zurich

Edition
140 copies

Today, cybersecurity determines trust and the ability to act, because digital transformation, AI and geopolitical dependencies are breaking down security boundaries and making transparent, verifiable security and holistic resilience a strategic obligation.

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

Are you looking for a cybersecurity role at Swisscom? Then apply here: swisscom.ch/securityjobs

#EngageYourSecuritySkills