Cybersecurity Threat Radar 2025

Cyber resilience despite geopolitical challenges

swisscom

Contents

Cybersecurity Threat Radar

Cyber resilience despite geopolitical challenges

In the fast-changing world of cybersecurity, it is essential for companies to continually review and adapt their defence strategies. Cybercriminals are becoming more and more sophisticated and are constantly changing their attack methods. This calls for innovative and flexible approaches to defence. In this Cybersecurity Threat Radar, we give you an insight into the current focal points and challenges in the area of cyber resilience, which we at Swisscom are addressing actively.

To combat specific cyberthreats, we are prioritising the targeted advancement of our detection and response capabilities. This is based on practical findings from red-team exercises, incident response experiences and current threat intelligence information.

The importance of basic security practices, often referred to as 'cyber hygiene', cannot be emphasised enough. These basics form the foundation of a robust cybersecurity strategy and are crucial for successfully defending against a wide range of threats. We attach great importance to the implementation and continuous improvement of these basic security measures. This includes regular security updates, strong authentication methods and regular training of our employees to foster overall security awareness.

The changing geopolitical situation presents companies with new challenges in the area of cybersecurity. The growing influence of tech billionaires, political shifts in Europe and stricter regulations require a flexible and forward-looking security strategy.

In order to meet these challenges, we at Swisscom also rely on close cooperation with national and international partners. Our Computer Security Incident Response Team (CSIRT) regularly exchanges information with other operators of critical infrastructures and security service providers in order to obtain a comprehensive picture of the current threat status.

Looking to the future, we are confronted with new technological developments that present both opportunities and risks. For example, the use of generative AI in cybersecurity requires a balanced approach: on the one hand, we use this technology to improve our threat detection; on the other hand, we need to guard against its misuse by cybercriminals.

Additionally, the concept of 'zero trust' architecture is gaining in importance. It systematically calls into question the inherent trust within the IT infrastructure and verifies every access request. In doing so, companies not only increase their security but also drive digital transformation forward.

In summary, it can be said that strengthening cyber resilience is an ongoing process that requires vigilance, adaptability and also innovative strength. At Swisscom, we try to take a holistic approach that takes into account real threats, fundamental security practices and cutting-edge technologies in equal measure. This is the only way we can effectively counter the wide range of cyberthreats and shape a secure digital future for our customers and partners.

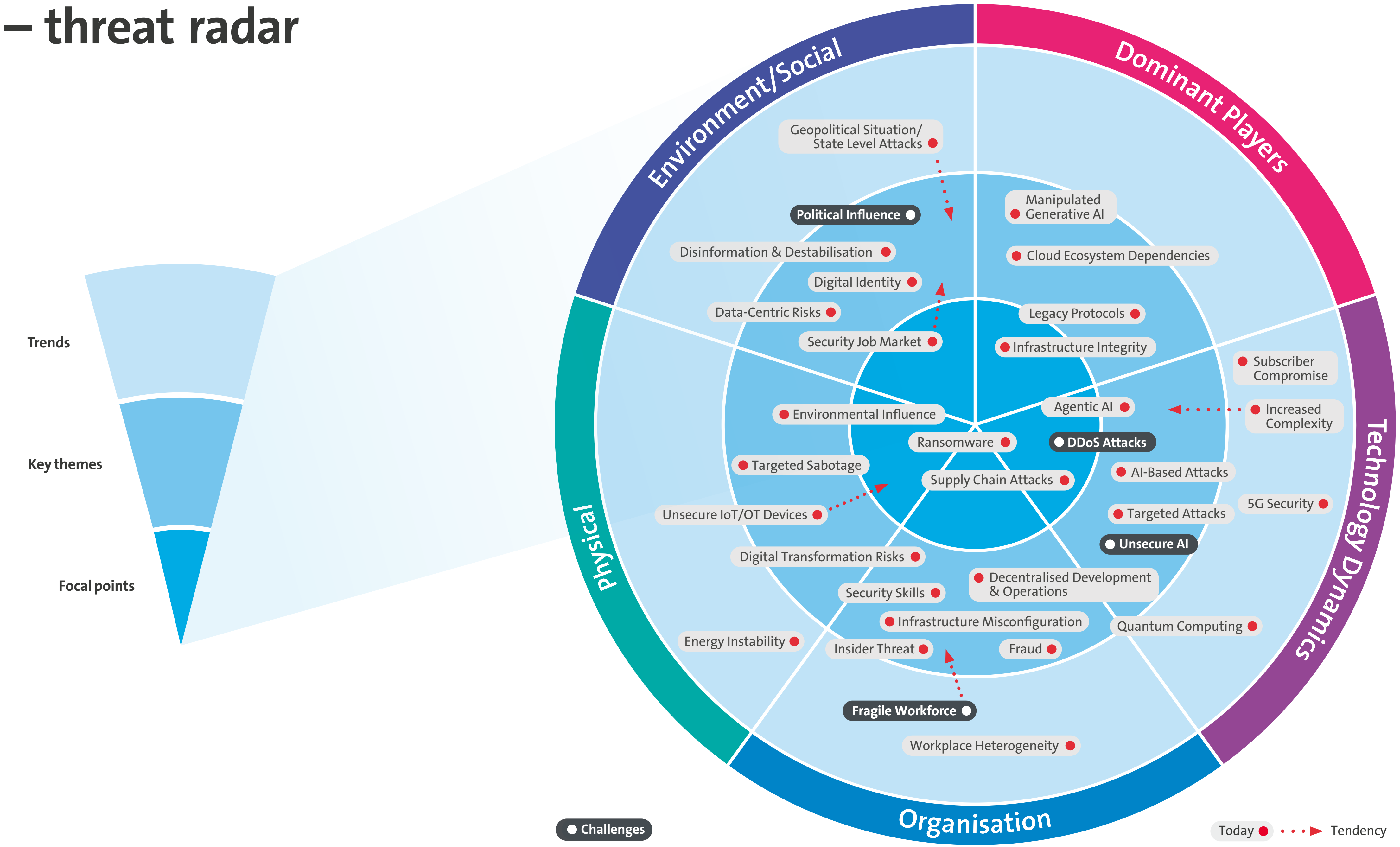
> *'The changing geopolitical situation presents companies with new challenges in the area of cybersecurity. The growing influence of tech billionaires, political shifts in Europe and stricter regulations require a flexible and forward-looking security strategy.'*

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.



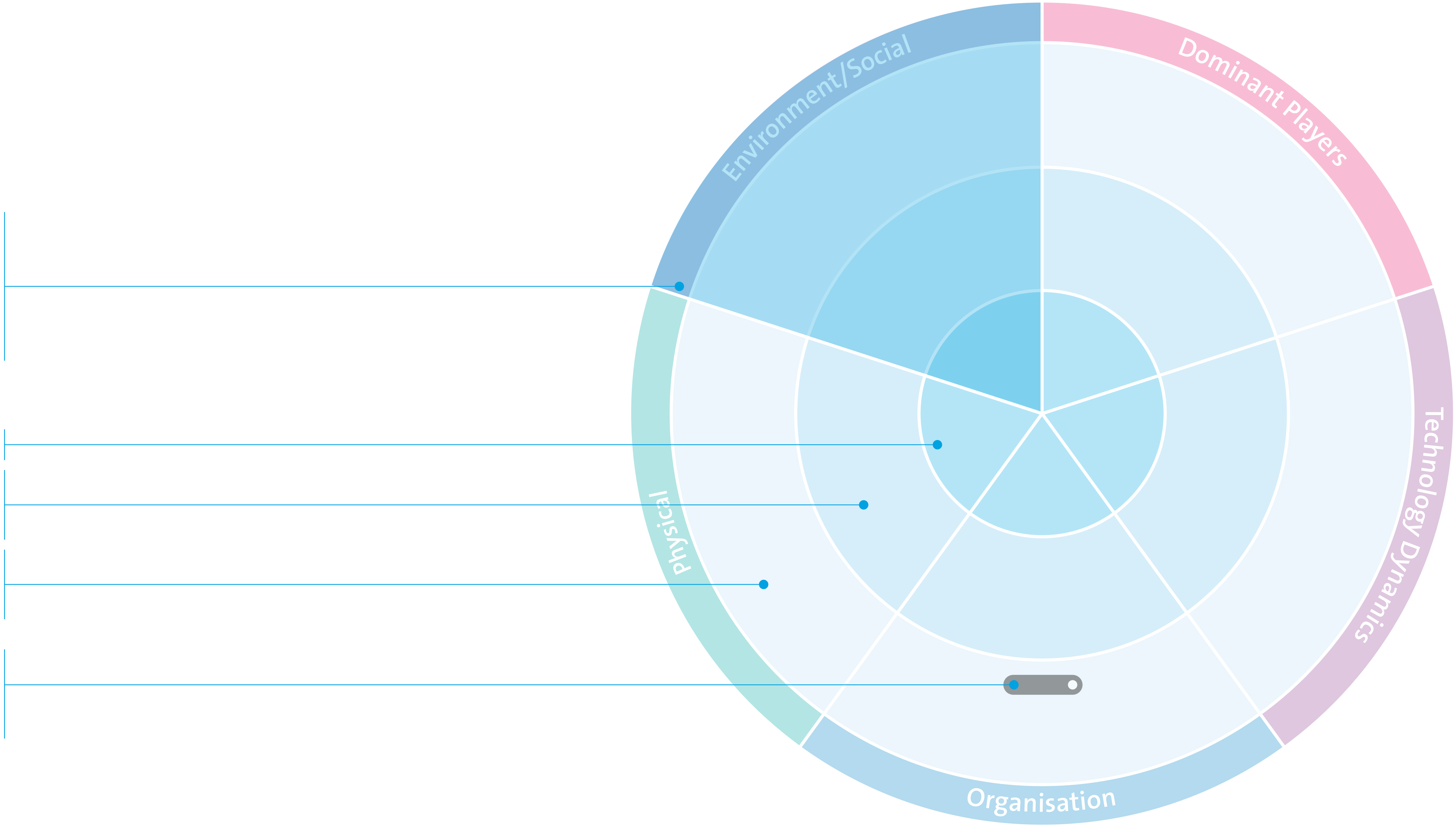
Method

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:

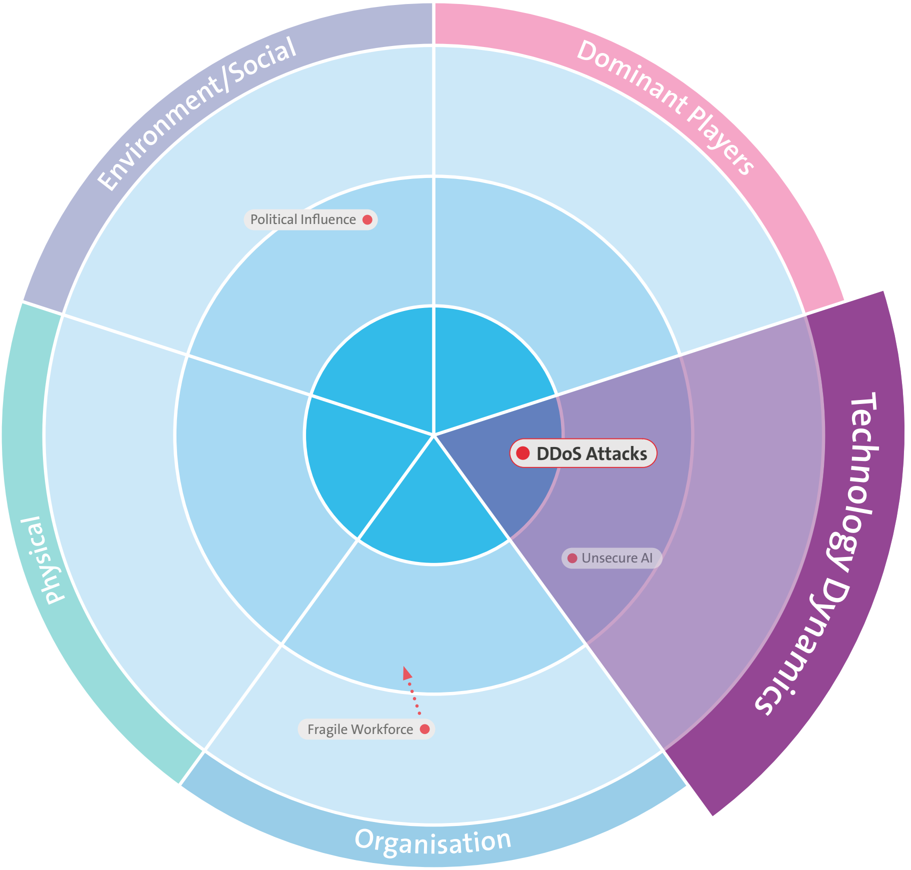
- **Focal points** for threats that are already real and can be managed with a relatively large input of resources.
- **Key themes** for threats that have already occurred sporadically and can be managed with the normal use of resources. Regulated processes often exist to efficiently counter such threats.
- **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.



Challenges and trends

DDoS attacks: ‘Destroy what destroys you’



In an increasingly digitalised business world, Distributed Denial of Service (DDoS) attacks represent a serious and growing threat to companies. These attacks aim to make online services, websites or networks inaccessible through a flood of data traffic, which can have far-reaching consequences for affected companies. The DDoS attack on Swisscom in August 2024 even made it into the media.

The number of targeted DDoS[1] attacks on financial services providers, the public sector, hosting providers, energy providers, telecommunications providers, online shops, etc. doubled in Switzerland between 2023 and 2024. According to the NETSCOUT Cyber Threat Horizon Report, around 56,200 DDoS attacks of all kinds were registered in 2023, followed by 107,000 in 2024. There were 293 attacks per day last year. The Swiss telecommunications industry was also targeted by the attackers.

Threat scenario

Performing DDoS attacks is becoming easier and easier. For years now, criminal marketplaces have offered DDoS attacks on the Internet as a service for a small fee (starting at USD 15 per month) – cybercrime as a service as it were – or as a stress test. These offerings are growing. It is therefore to be expected that the number of DDoS attacks will continue to increase.

In addition, thanks to the rise of artificial intelligence (AI), cybercriminals have an easier time making their DDoS attacks more dangerous and more effective.

As a result, the protection of intangible assets such as data, networks or intellectual property is becoming a priority for risk management. Inadequate IT security must be classified as a corporate risk if entire businesses can be paralysed by cyberattacks.

[1] DDoS (Distributed Denial of Service) is a type of cyberattack in which publicly accessible IP addresses from the Internet are flooded with a very large number of requests from infected PCs, TVs, webcams and many other IP devices. The aim of the attackers is to keep the e-services that can be accessed via the attacked IP addresses offline for as long as possible.

Why are DDoS attacks dangerous for companies?

1. **Operational disruption:** DDoS attacks can significantly disrupt normal business operations by crippling websites, online services or internal networks.
2. **Financial losses:** companies, especially those with a high dependence on online traffic, can suffer significant losses in revenue if their services are unavailable.
3. **Damage to reputation:** repeated or long-lasting downtime can undermine customers' trust in the reliability and security of the company.
4. **High recovery costs:** the cost of restoring services and strengthening the security infrastructure after an attack can be considerable.
5. **Distraction manoeuvres:** DDoS attacks can serve as a distraction to divert attention from other malicious activities, such as data theft.

Potential damage

Companies can already suffer financial damage before a DDoS attack occurs. The National Cyber Security Centre (NCSC) reports on blackmail attempts on the Internet threatening companies with DDoS attacks if they are unwilling to pay the amount demanded. The blackmailers do not always actually have the ability to carry out a DDoS attack. But they are gambling, hoping that the threat alone will be enough for a ransom.

Protective measures

DDoS attacks pose a serious and growing threat to companies of all sizes. With the rise of digitalisation and the increasing reliance on online services, the importance of robust protective measures will continue to grow. Companies need to be proactive in protecting their digital infrastructure to ensure business continuity. As the saying goes: 'It is better to be safe than sorry.'

'Opportunities and risks are a constant companion on the Internet. You can consciously influence both parameters. Waiting and hoping never to fall victim to a DDoS attack is definitely not recommended. Take targeted measures and implement them as quickly as possible.'

Beat Hunziker
Senior Product Manager Business Internet &
Security Services

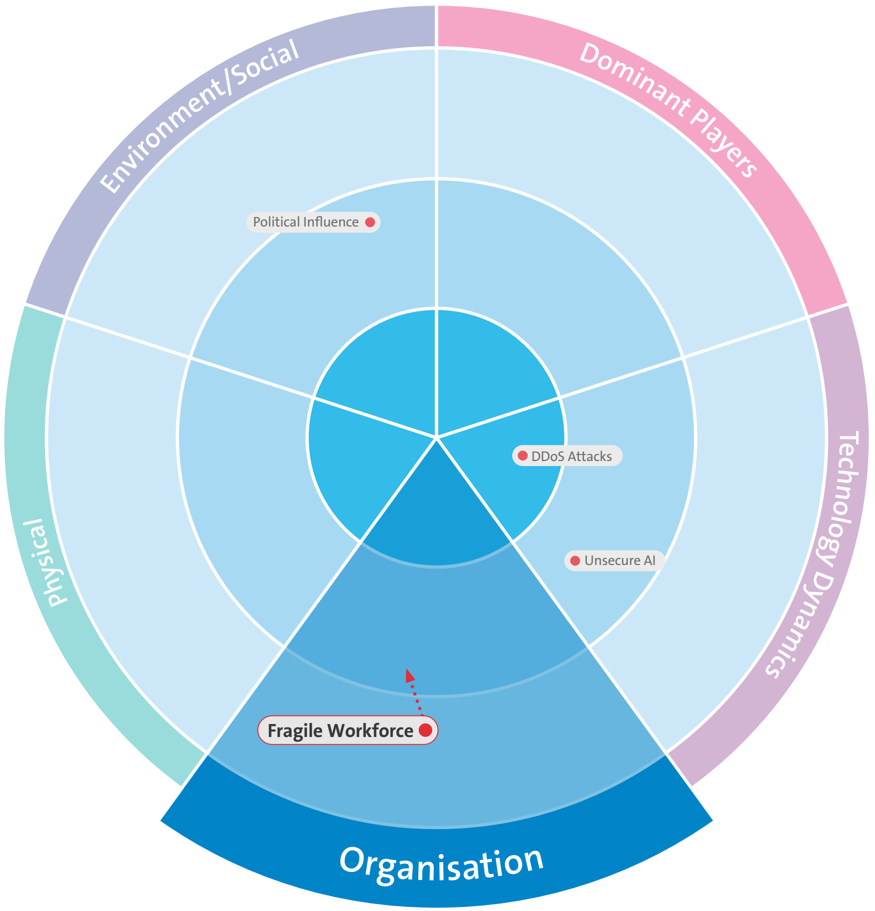
Investing in comprehensive DDoS protection solutions, ongoing training and developing flexible response plans are key to meeting the challenges of the ever-evolving cyber landscape. Only by taking a holistic and forward-thinking approach can companies strengthen their resilience to DDoS attacks and minimise potential damage.

Ultimately, protecting against DDoS attacks is not just a technical challenge, but a strategic necessity for any modern company. The ability to effectively ward off such attacks is increasingly becoming a decisive competitive advantage in the digital economy.

'The threat of DDoS attacks is omnipresent. They not only cause financial damage but can also severely impact a company's reputation.'

Reto Friedl
Product Manager Managed Security Services

Fragile workforce: ‘When the going gets tough’



Cybersecurity teams are under enormous pressure. The threat landscape is constantly changing – from sophisticated phishing attacks to targeted ransomware attacks and deep-fake manipulations. At the same time, the complexity of IT infrastructures is growing, while areas of attack are increasing due to hybrid working models and networked devices.

More than 10,000 alerts per day: why is this problematic?

Alerts, incident analyses and rapidly changing threat scenarios lead to ‘alert fatigue’ – a state in which warning signals are no longer followed up with the attention necessary because the system is overloaded. A study by Devo Technology shows that 42 % of IT security teams regularly ignore alarms because there are simply too many, making them difficult to manage. The result is inattention and poor decisions, which presents a significant security risk.

Challenge: managing the cognitive and emotional load

These challenges have serious consequences for employees: chronic stress not only affects health but also work performance. A recent industry study by SoSafe shows that up to 57% of security professionals in the DACH countries suffer from burnout. The main reasons are:

- **High pressure to perform:** constant threat detection and defence as a core task.
- **Overload and contractual overtime:** employees are regularly putting in extra hours.
- **Insufficient training:** lack of further training leads to uncertainty.
- **Staff shortages:** a shortage of skilled workers increases the load even further.

In addition, cognitive overload occurs when the brain struggles to process excessive information, tasks and decisions at the same time. Distractions, multitasking and constant stress exacerbate the problem – making it increasingly difficult to take reliable decisions. Typical consequences are:

- Delayed threat response
- Misconfigurations and security loopholes
- Limited communication under stress
- Burnout and high fluctuation

The result: anyone who ignores the mental load risks not only the security of the company but also the health of the people who protect it.

Strategies for safe, effective and healthy working

A sustainable approach addresses these core areas: leadership, team dynamics and key competencies.

Managers as a firewall against overload

Managers play a key role in setting an example of mindful work, having regular conversations and prioritising mental health. They help to create structures for focused work and minimise unnecessary interruptions. At the same time, they can foster psychological safety and prevent overload with preventive measures.

HR managers should also take action, for example by promoting occupational health management. This creates a corporate culture in which psychological stability is considered a success factor.

Psychological safety as the foundation for effective teamwork
A resilient cybersecurity team needs psychological safety. Sharing knowledge, talking openly about mistakes and providing collegial support in stressful situations strengthens the resilience of the team. Success factors include:

- **Promoting emotional intelligence** – conscious awareness and support within the team.
- **Establishing mentoring programs** – experience sharing and individual development.
- **Using peer groups** – reflecting on best practices and psychological challenges.

Key competencies for resilient cybersecurity teams
Mental agility can be trained – and mastering it not only reduces mistakes but also stress. The ability to respond quickly to threats while making well-thought-out decisions is essential:

- Mental agility enables flexible switching between analytical thinking and quick action.
- Mental clarity ensures that relevant information is evaluated under pressure rather than reacting impulsively.

Why does it help with stress?

Cybersecurity professionals need to train their minds to consciously switch between systems of thought and avoid making wrong decisions. Under high pressure or when experiencing cognitive overload, intuitive, fast but error-prone thinking often takes over – a concept that psychologist Daniel Kahneman describes as 'system 1'. The reflective, analytical 'system 2', on the other hand, helps to make more precise decisions, but requires more cognitive resources.

- Those able to consciously switch between systems 1 and 2 can make better-informed decisions and reduce stress.
- Targeted control of systems of thought prevents impulsive reactions and increases control in critical situations.
- Less cognitive overload eases mental pressure and improves long-term resilience to stress.

‘Slight destroyers: ignoring them jeopardises security.’

Anja Peter
CEO & Co-Founder Human Empowerment Center AG

Focus and regeneration

Working in crisis mode at all times is mentally and physically unsustainable. Those who constantly jump between tasks and work without breaks are exhausting their cognitive resources. Studies show that permanent sensory overload due to multitasking and constant interruptions drastically reduces the ability to focus and problem-solve. Targeted regeneration increases long-term resilience. These measures include:

- **Deep work and time blocking** – targeted phases of uninterrupted work in order to make efficient use of cognitive resources.
- **Focus sprints** – intensive work phases with clearly defined breaks to avoid mental fatigue.
- **Micro time-outs and breathing techniques** – targeted relief of the nervous system to improve concentration and stress management.

Consciously switching between focus and recovery protects your mental performance. Mindful work means not letting yourself be guided by distractions, but making specific decisions about what to focus your attention on. Without this conscious control, the brain remains in constant alarm mode, which in the long run leads to exhaustion and poor decisions.

Conclusion: sustainable cybersecurity starts with resilient teams

A resilient security team is crucial to success in cybersecurity. Sustained excellence requires resilience and support for the people behind the monitors.

The aim must be to create an environment in which mindfulness, psychological safety and active stress management are a matter of course. This is the only way to mitigate cognitive overload, alert fatigue and the much-quoted 'slight destroyers of strong cybersecurity'. Companies or organisations not only gain motivated and healthy employees but also increase their overall resilience to cyberattacks in the long term. This is the only way to build a strong and resilient workforce that is up to the challenges of the future.

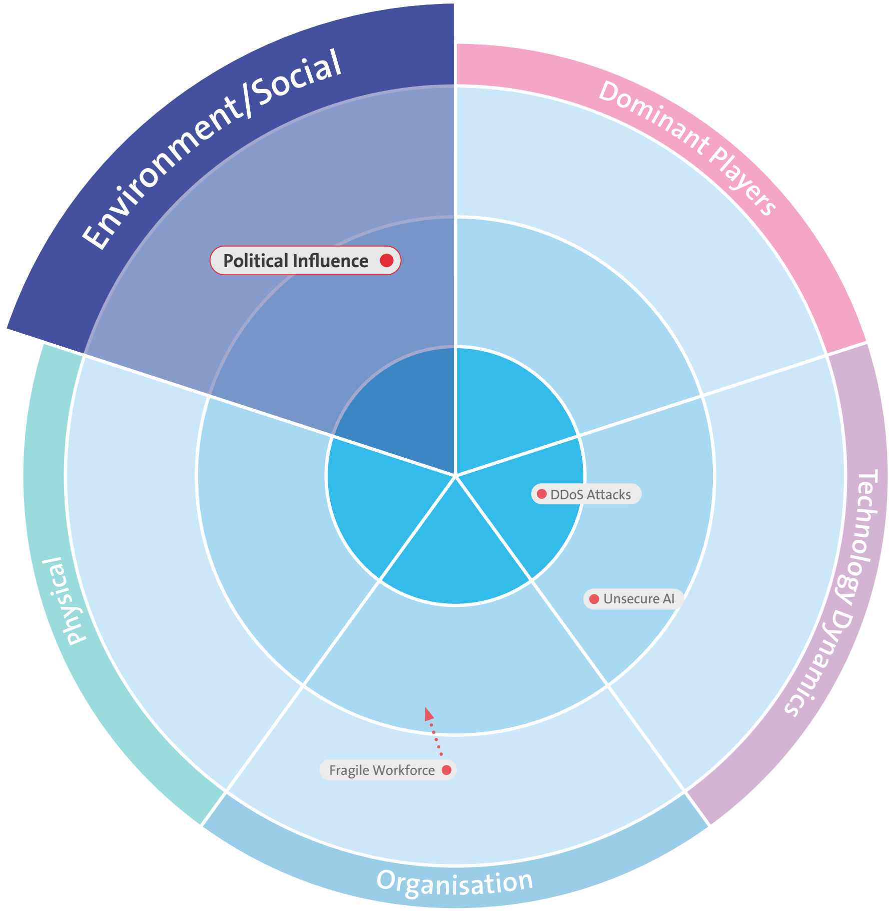
Ultimately, every security strategy depends on the people who implement it. A resilient workforce is the key to resilient cybersecurity – for businesses and the health of those who protect them.

‘A fragile workforce reacts, a resilient workforce takes action.’

Martina Novo
Tribe Chief Security

Challenges and trends

Political influence: 'More security through more regulations?'



We are living in an era of profound change, in which geopolitical, economic and technological developments can cause general uncertainty. This 'Age of Disorder' calls for reliability, stability and leadership. Companies and governments are under considerable pressure as hybrid threats, such as targeted disinformation, cyberattacks and acts of sabotage, aim to undermine trust in political institutions, fuel social fears and weaken social cohesion.

Companies and governments must therefore focus on a sustainable and digital transformation in order to be able to ensure economic stability. Resilience strategies, such as diversification and cybersecurity, are essential to mitigate future crises. The 'Age of Disorder' requires proactivity in order to anticipate and actively shape disruptive changes. Only those who drive innovation with agility and shape change with courage will be able to hold their own in the face of global competition.

The digital transformation presents not only challenges but also numerous opportunities. Companies that are able to adapt quickly to new circumstances and develop innovative solutions will succeed in global competition. However, this requires a culture of openness and continuous learning, where mistakes are seen as learning opportunities and new ideas are encouraged.

In this rapidly evolving environment, companies face the challenge of ensuring cybersecurity while remaining innovative. Regulations such as NIS2, DORA, the Cyber Resilience Act (CRA), standards such as ISO 27001 and national requirements such as the Information Security Act (ISA) in Switzerland are designed to help.

However, the increasing density of regulation also entails risks of what is known as a 'regulatory paradox': companies and organisations have a false sense of security, focussing on ticking off regulatory requirements instead of thinking holistically about security.

To counter this trend, companies need to strike a balance between compliance and proactive security management and adopt a risk-based approach that focuses on real threats rather than just regulatory compliance. Regular reviews of the security situation beyond regulatory requirements are necessary in order to be able to respond flexibly to new threats. It is crucial that organisations take personal responsibility for their security rather than relying solely on external requirements. Only by combining regulatory compliance, strong and self-directed security management and a sustainable and effective security culture can companies build resilience to cyberthreats.

In an ever-changing world, it is imperative that companies and governments not only respond to current threats but also take proactive measures to address future challenges. Continuous adaptation and improvement of security strategies as well as close collaboration between different stakeholders and an understanding of the situation are essential. It is only through joint efforts that we can shape a secure and stable digital future.

The resilience and availability of services and infrastructures are also crucial. Companies need to ensure that their systems remain functional even in times of crisis and can be recovered quickly. This requires close collaboration between different departments and clear communication about responsibilities and measures in the event of an incident.

Control over key digital processes and the infrastructures that enable them is vital to ensure digital sovereignty. Companies must ensure that they retain control over their data and systems and are not dependent on external providers. This requires careful planning and implementation of security measures as well as continuous monitoring and adaptation to new threats. Companies must ensure that their systems and data are protected from unauthorised access and that they are capable of responding quickly and effectively to security incidents.

Digital Sovereignty

Access to trustworthy information is another important aspect of digital sovereignty. Companies and governments must ensure that they have reliable and up-to-date information in order to make informed decisions. This requires close collaboration with different information sources and the ability to process and analyse information quickly and efficiently.

‘Social policy and innovation are changing our world more rapidly than ever. But the future does not simply happen – it is shaped by those who lead the way with resilience, agility and foresight.’

Florian Kässberger
Experience Innovation Expert

Overall, it is vital that companies and governments take a holistic approach to overcome the challenges of digital transformation. This requires close collaboration between different stakeholders, continuous adaptation and improvement of security strategies and a culture of openness and continuous learning. It is only through joint efforts that we can shape a secure and stable digital future.

Cybersecurity is and will remain a central component of the digital sovereignty of companies and organisations, i.e.

- Resilience and availability of services and infrastructures.
- Control over data and data flows.
- Control over key digital processes and the infrastructures and organisations that enable them.
- Access to trustworthy information.
- Cybersecurity.
- Digital skills.
- Diversified supply chains.

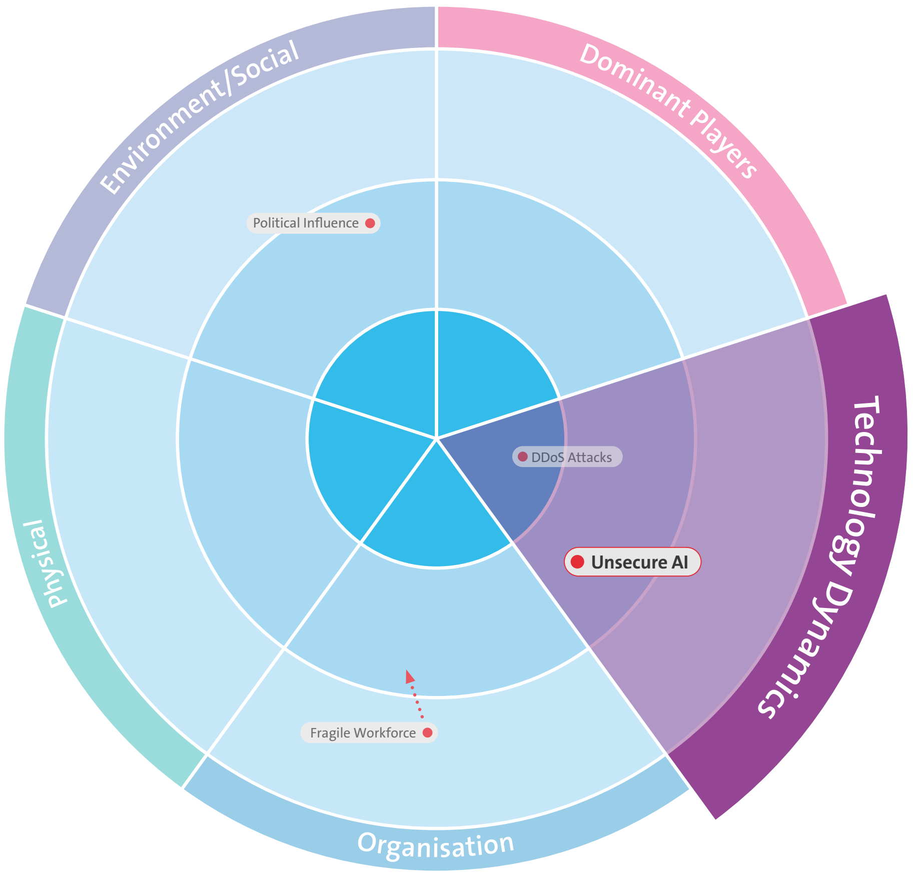
And it is up to all of us to contribute to digital sovereignty. The business community is ready to engage in dialogue and to contribute. The voice of the industry is particularly important when it comes to the feasibility and implementation of digital sovereignty.

‘Digital sovereignty is not an end goal, but an ongoing process and requires a holistic view.’

Karin Stöckli
Public Affairs Delegate of
Federal Administration and NGO

Challenges and trends

Shadow AI: ‘Here to stay – AI at any cost?’



In today’s fast-moving economy, companies are increasingly turning to artificial intelligence (AI) to remain competitive. However, in addition to the officially implemented AI systems, there is a lesser-known phenomenon: **shadow AI.**

Shadow AI affects companies of all sizes and industries. Similar to shadow IT, the phenomenon of shadow AI refers to the use of AI tools and applications within a company without the approval of the IT or security team. This may seem harmless, but it entails significant risks. According to a Gartner study, more than 50% of employees use AI or machine learning applications for their work that the IT department is unaware of. This may lead to serious incidents such as:

- Data breaches and security risks.
- Compliance violations, in particular in the area of data protection and confidentiality, or also in relation to the EU AI Act (if applicable to companies in Switzerland).
- Inefficiencies due to duplicate expenses and inconsistent processes.
- Potential reputational damage if misuse becomes known.

The EU AI Act is an EU law, but may also be relevant for companies in Switzerland under certain conditions. The EU AI Act will impose additional requirements on companies:

- Risk-based categorisation of AI systems. The higher the risk, the stricter the requirements.
- Controls for high-risk AI applications.
- Transparency obligations for certain AI systems.
- High penalties for non-compliance (up to 30 million euro or 6% of global annual turnover, depending on the violation).

Manifestations of shadow AI

- **AI-powered chatbots:** these are often used without permission to process customer enquiries, which can lead to inaccurate answers.
- **Machine learning models:** employees use external platforms for data analysis, which can put confidential data at risk.
- **Marketing automation tools:** although these increase productivity, they can violate compliance policy and erode customer trust.
- **AI functionality in customer software:** additional AI functionality is activated after updating an existing application without additional testing, disclosing sensitive data to unauthorised persons.

Opportunities and challenges

The integration of AI into corporate processes offers enormous potential for innovation. AI can help optimise business processes, develop new products and services and increase customer satisfaction. By analysing large volumes of data, companies can gain valuable insights and make informed decisions. AI-powered automation can increase efficiency and relieve employees of repetitive tasks, allowing them to focus on strategic activities.

Artificial intelligence has become an integral part of today's working world. It serves as a driver of innovation and, if applied correctly, can boost productivity. However, companies need to minimise risks through clear policies and monitoring.

To overcome the challenges of shadow AI, it is critical that companies foster a culture of transparency and collaboration between IT and departments. Through regular audits and training, potential risks can be identified and resolved at an early stage. This is the only way to integrate shadow AI into a controlled and secure AI ecosystem.

> *‘Every company that uses AI tools should establish company-wide AI governance in future – not only to prevent reputational risks, but also to comply with existing and future regulations. AI technology is evolving rapidly, which makes it all the more important to keep up and ensure responsible use.’*

Anne-Sophie Morand
Data Governance Counsel

Measures for integrating shadow AI and innovation through AI

To address shadow AI and prepare for the EU AI Act, companies should take the following measures:

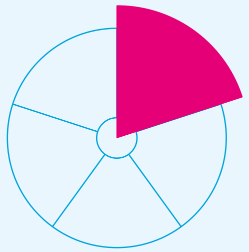
- **Inventory and risk assessment:** identify all AI systems in the company and assess their risks with regard to the relevant legal provisions (e.g. Data Protection Act or the EU AI Act, if applicable).
- **Governance and policies:** develop clear AI usage guidelines and establish an approval process for new AI tools.
- **Technical controls:** implement network monitoring and DLP systems.
- **Training and sensitisation:** conduct regular AI-specific employee trainings and foster an open communication culture on AI topics.
- **Provide approved AI solutions:** evaluate and provide official AI tools.
- **Compliance management:** establish an AI ethics committee and implement processes for ongoing monitoring and documentation.
- **Collaboration and expertise:** establish an AI competence centre and work closely with legal and compliance experts.

These measures enable companies to effectively manage shadow AI while also complying with legal requirements. It is important to take a proactive approach in order to benefit from the opportunities presented by AI and minimise the risks associated with it.

> *‘Users and companies still pay far too little attention to data breaches and security risks when using AI tools. In addition to the opportunities offered by AI in combination with the processing of large volumes of data, this has the potential to pose significant risks.’*

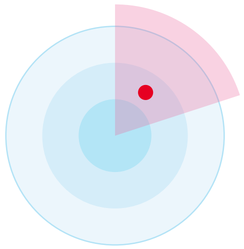
Marc Scheidegger
Solution Security Architect for Data, Analytics & AI

Details including tendencies and comparison with the previous year



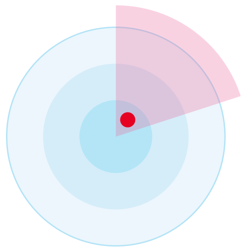
Dominant Players

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



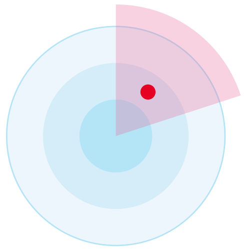
Cloud Ecosystem Dependencies
Intensively centralising data in the cloud leads to cluster risks. The failure of a service or central service can have a global impact.

► Unchanged



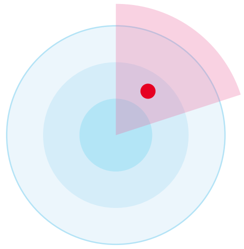
Infrastructure Integrity
Vulnerabilities may have been negligently or deliberately built into essential components of critical infrastructures, jeopardising system security.

► Unchanged



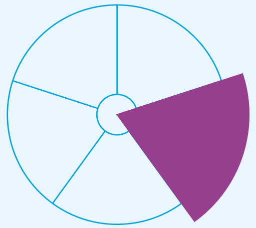
Legacy Protocols
Due to software dependencies, completely outdated and vulnerable protocols are still used (e.g. NTLMv1, SMBv1, RC4), resulting in a few applications endangering the security of entire infrastructures.

► Unchanged



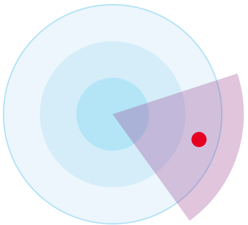
Manipulated Generative AI
Targeted manipulations can alter the output of an AI system. This may involve the infiltration of malicious, false or corrupted data during the training phase, the theft of LL models, as well as prompt manipulation, which may result in adverse and legally binding ramifications.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

► Unchanged



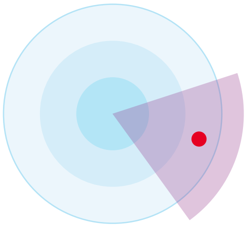
Technology Dynamics

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.



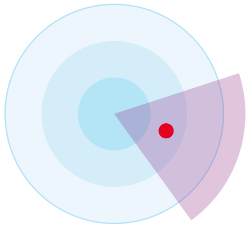
5G Security
5G is still a new mobile telecommunications technology. Its introduction will bring many opportunities as well as still unknown threats.

► Unchanged



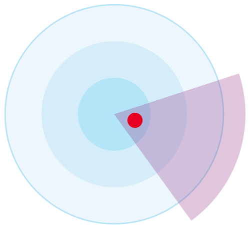
Quantum Computing
Quantum computers can render existing cryptographic methods useless because they can bypass them in a very short time.

► Unchanged



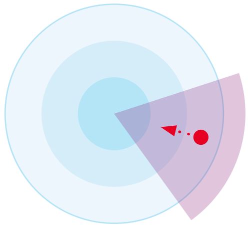
Unsecure AI
Unsecure AI systems endanger supply chains and data protection, as generative models can disclose confidential data in an uncontrolled manner. This can not only affect business continuity, but also significantly damage a company's reputation. In addition, there is a risk of regulatory consequences,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

► Unchanged



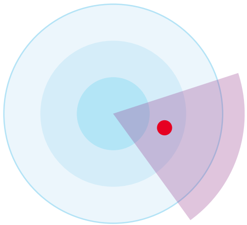
Ransomware
Critical data is encrypted on a large scale and (possibly) decrypted again in return for a ransom payment.

► Unchanged



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.

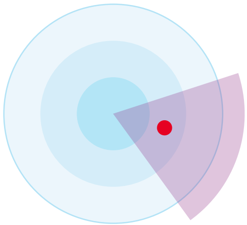
▲ Increased



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.

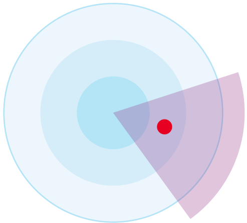
► Unchanged



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 Copilot can cause considerable damage through incorrect instructions or manipulation on the part of the attackers.

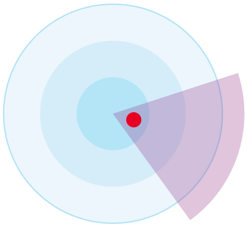
► Unchanged



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).

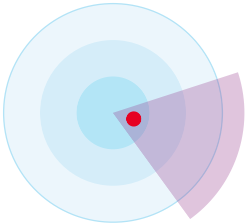
► Unchanged



DDoS Attacks

A 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.

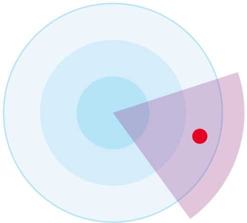
► Unchanged



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.

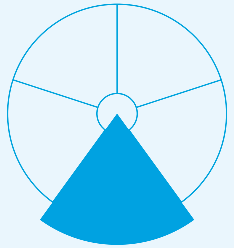
► Unchanged



Subscriber Compromise

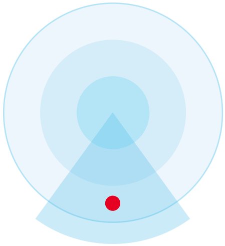
Malware gains access to the private data of mobile users or is used to attack the telecommunications or IT infrastructure. Phishing, smishing, vishing and MFA bypass attacks target subscriber credentials. Entire digital identities are consequently stolen and taken over during the follow-up attacks.

► Unchanged



Organisation

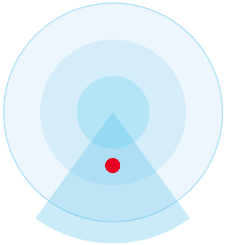
Organisation means threats that emanate from changes in organisations or that exploit weaknesses in organisations.



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.

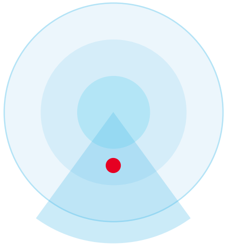
► Unchanged



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.

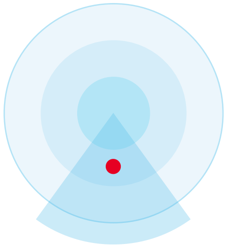
► Unchanged



Insider Threat

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

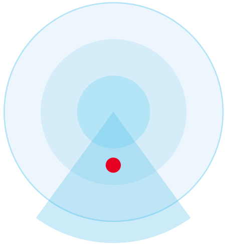
► Unchanged



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 cyber risk and the vulnerability of the IT infrastructure via unsecured end devices.

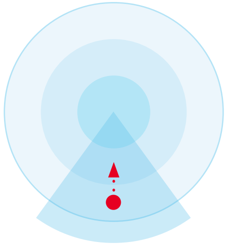
► Unchanged



Security Skills

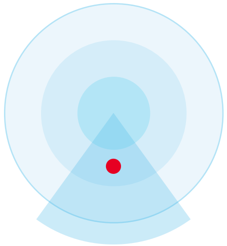
Due to the complexity of cyberattacks and advancing digitalisation, security skills and the deployment of cyber professionals within organisations are becoming indispensable. The threat of 'downskilling' – the unlearning of knowledge – through automation in IT can lead to new attack vectors. For example,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

► Unchanged



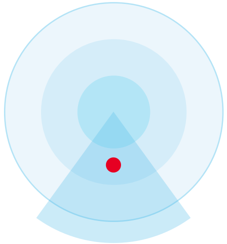
Fragile Workforce
A fragile workforce describes the vulnerability of cybersecurity and cyber defence teams to psychological stress and a lack of stress and burnout prevention. If someone is mentally unstable and unable to perform under pressure, the likelihood of human error increases. This creates an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

▲ Increased



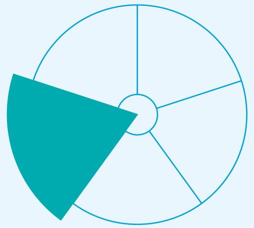
Infrastructure Misconfiguration
Exploitation of misconfigured infrastructure components and/or vulnerabilities that are identified and fixed late. The fact that technical operating processes are automated more than ever before will have a greater impact if there are successful attacks or misconfigurations.

► Unchanged



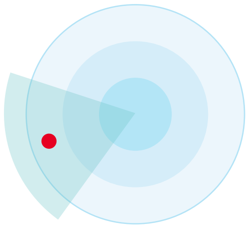
Fraud
Fraud refers to illicit activities based on deception and unlawful enrichment. It manifests itself in fraudulent transactions, identity theft or manipulated documents. Fraud poses a significant risk to companies and private individuals as it can lead to financial losses and damage to reputation.

► Unchanged



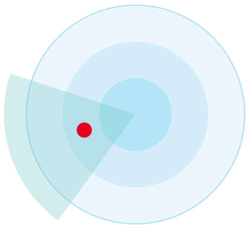
Physical

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.



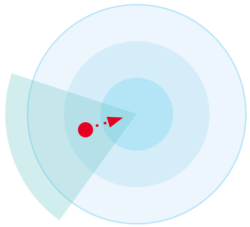
Energy Instability
Attacks on critical infrastructure such as power grid operators. Safeguarding against failure is essential and business continuity is increasingly being discussed in the cyber resilience debate. Power shortages, blackouts (widespread power failures) or even blueouts (widespread failure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

► Unchanged



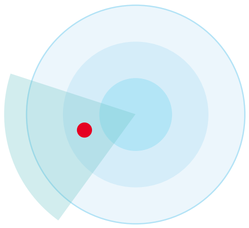
Targeted Sabotage
This concerns targeted attacks on important critical infrastructure, utilities and connections, which can significantly restrict the functioning of the internet. The targeted sabotage of critical fibre optic cables is increasing and is a danger that needs to be monitored. Counter measures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

► Unchanged



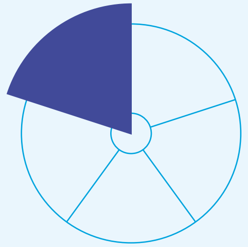
Unsecure IoT/OT Devices
Whether operational technology (OT) for monitoring and controlling physical processes, devices and infrastructures, or IoT devices – the Internet of Things is forever present. A wide variety of tasks – from the simple to the complex – are performed here, ranging from home entertainment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



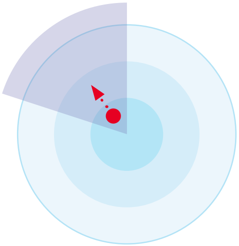
Environmental Influence
The climate crisis is leading to a rise in unpredictable weather patterns and extreme weather events, including heatwaves, heavy rainfall, tornadoes, hailstorms and lightning strikes. This can cause damage to the infrastructure of organisations and companies and significantly affect the external and internal environment of an information system or network.

► Unchanged



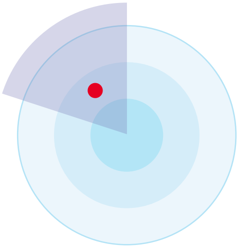
Environment/Social

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.



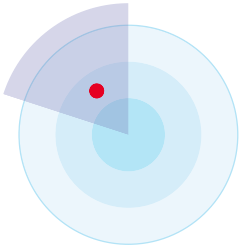
Security Job Market
The demand for security professionals is enormous and can only be met with great difficulty. This leads to decreasing levels of expertise that are needed to combat increasingly complex and intelligent attacks.

▼ Decreasing



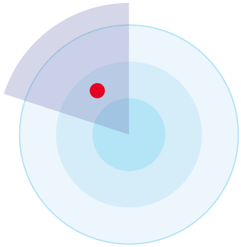
Digital Identity
Authenticated, personal digital identities can be misused or stolen. For example, this information can be used to sign off contracts under someone else's name.

► Unchanged



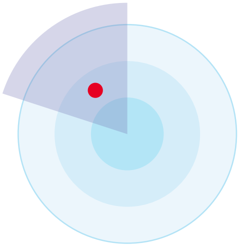
Disinformation & Destabilisation
The deliberate dissemination of false information can lead to economic and social instability and is increasingly being used in a targeted way via cyberspace, especially in crisis scenarios.

► Unchanged



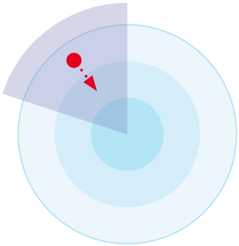
Political Influence
Political trends as well as regulations and specifications can influence technological or economic decisions, such as in the selection of technology suppliers. This can lead to new risks.

► Unchanged



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



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.

▲ Increased

Summary

The digital transformation presents companies and institutions with numerous challenges.

The digital transformation presents companies and institutions with numerous challenges. The geopolitical situation that we face on a daily basis also has a direct impact on technological and economic decisions. This includes dealing with uncontrolled AI applications, ensuring general cybersecurity and protecting cybersecurity teams from burnout. Companies are therefore well advised to develop resilience strategies in order to anticipate disruptive changes and successfully assert themselves in the face of global competition. Finding a healthy balance between compliance and proactive security management is crucial. A sustainable way of working requires a culture of transparency, psychological safety and continuous training. Managers play a key role in preventing mental overload and creating a resilient workplace environment.

This is why companies and institutions should take proactive measures in this rapidly evolving digital world in order to seize the opportunities of digital transformation while actively minimising the associated risks. This requires close collaboration between different stakeholders, continuous review and improvement of security strategies and a culture of openness and continuous learning.

Companies and organisations that rely on innovative solutions foster a transparent and security-conscious corporate culture and invest in the continuous training of their teams. This creates a secure digital future where companies, organisations and governments are resilient to security threats. We can all do our part and set a good example. Let's seize the opportunities of the digital future together.

#BeTheStrongestLink

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

As 'Innovator of Trust', Swisscom facilitates and shapes the digital future. By offering innovative products and services and earning the trust of our customers, we create a unique customer experience that has a sustainable impact on both the environment and society – in Switzerland and across the entire world.

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? Take a look at our current vacancies and apply today: swisscom.com/securityjobs

#BeTheStrongestLink