Cyber Security Threat Radar

2023/2024

Strengthening cyber resilience

swisscom

Contents

Cyber Security Threat Radar

Strengthening cyber resilience

It is crucial that companies and organisations remain resilient, particularly during these turbulent and challenging times. This should not just encompass physical health and stable, redundant IT systems, but also clear guidelines to serve as guard rails to offer better orientation.

The Cyber Security Threat Radar highlights the fact that protection against cyber risks and risk mitigation are multifaceted processes that should not be the sole responsibility of IT departments. Cybersecurity needs the attention of executives and the active participation of every member of the company's management team.

In this year's Cyber Security Threat Radar, we will not focus on managing the fourth sector of cyberthreats, namely monitoring. This theme is already an integral part of Swisscom's cybersecurity DNA and is a key consideration in our daily business operations.

Instead, the spotlight is directed towards 'Disinformation and destabilisation', which has been identified as one of the most significant challenges of our times. The dissemination of false information, manipulated content and targeted propaganda campaigns can influence entire societies, disrupt political processes and undermine trust in institutions. Even the experts behind the Global Risks Report 2024 from the World Economic Forum (WEF) have categorised this threat as the greatest short-term risk. The themes discussed in this edition of the Radar are by no means exhaustive.

The revision of the Swiss Data Protection Act and the new Federal Information Security Act (ISA) mean that governance aspects are once again taking centre stage. We are curious to see what the future holds. I hope that this edition of the Cyber Security Threat Radar will provide valuable insights and will help you to further advance cybersecurity in your company or organisation.

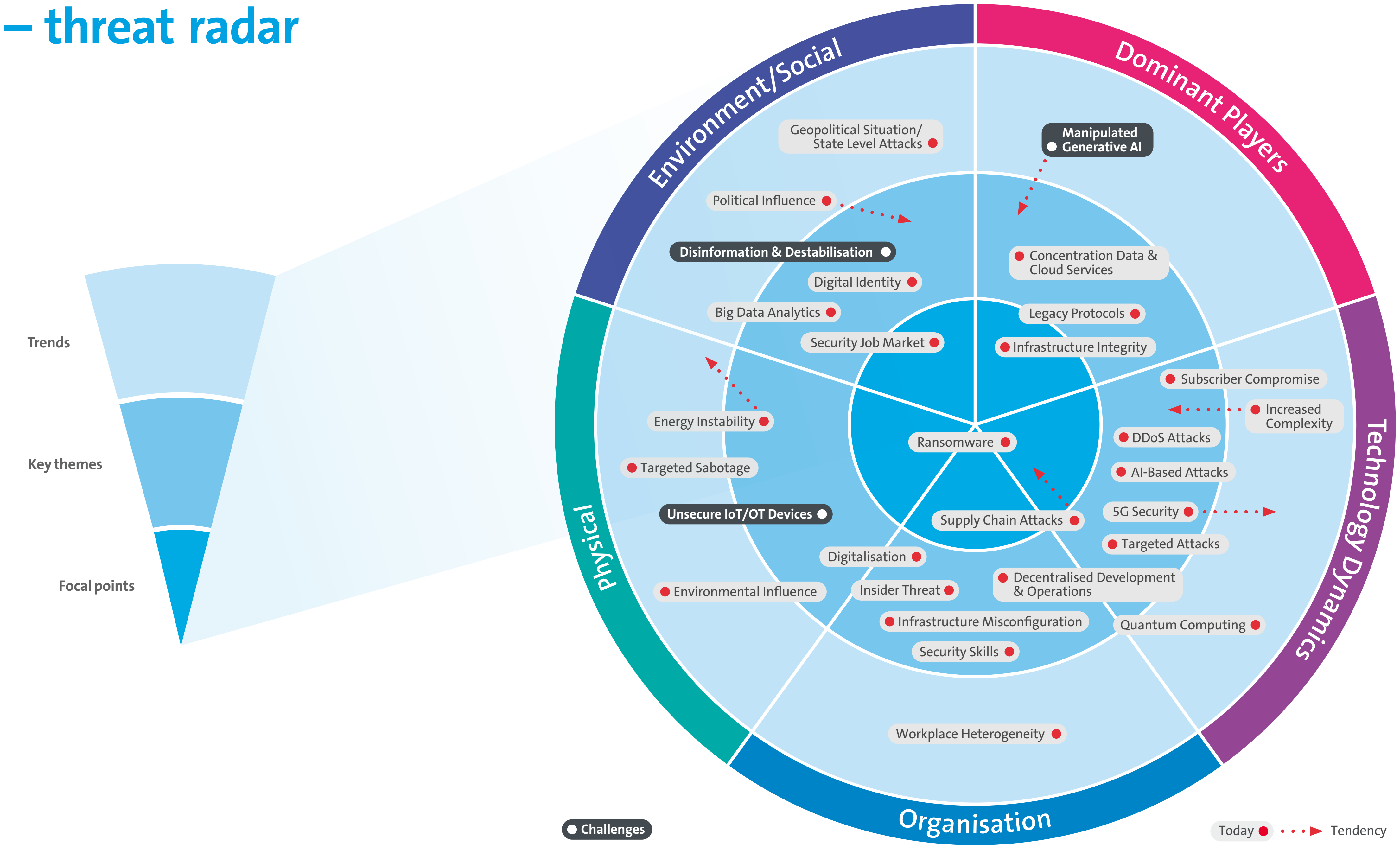
Marco Wyrsch
Head of Group Security
Swisscom (Schweiz) AG

> *'Monitoring and observing our network enable us to continually make Switzerland a whole lot safer. Because cyber risks will remain one of the top risks for organisations, companies and society in general in the coming years.'*

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 Cyber Security Threat Radar to map the current threat status and its evolution.



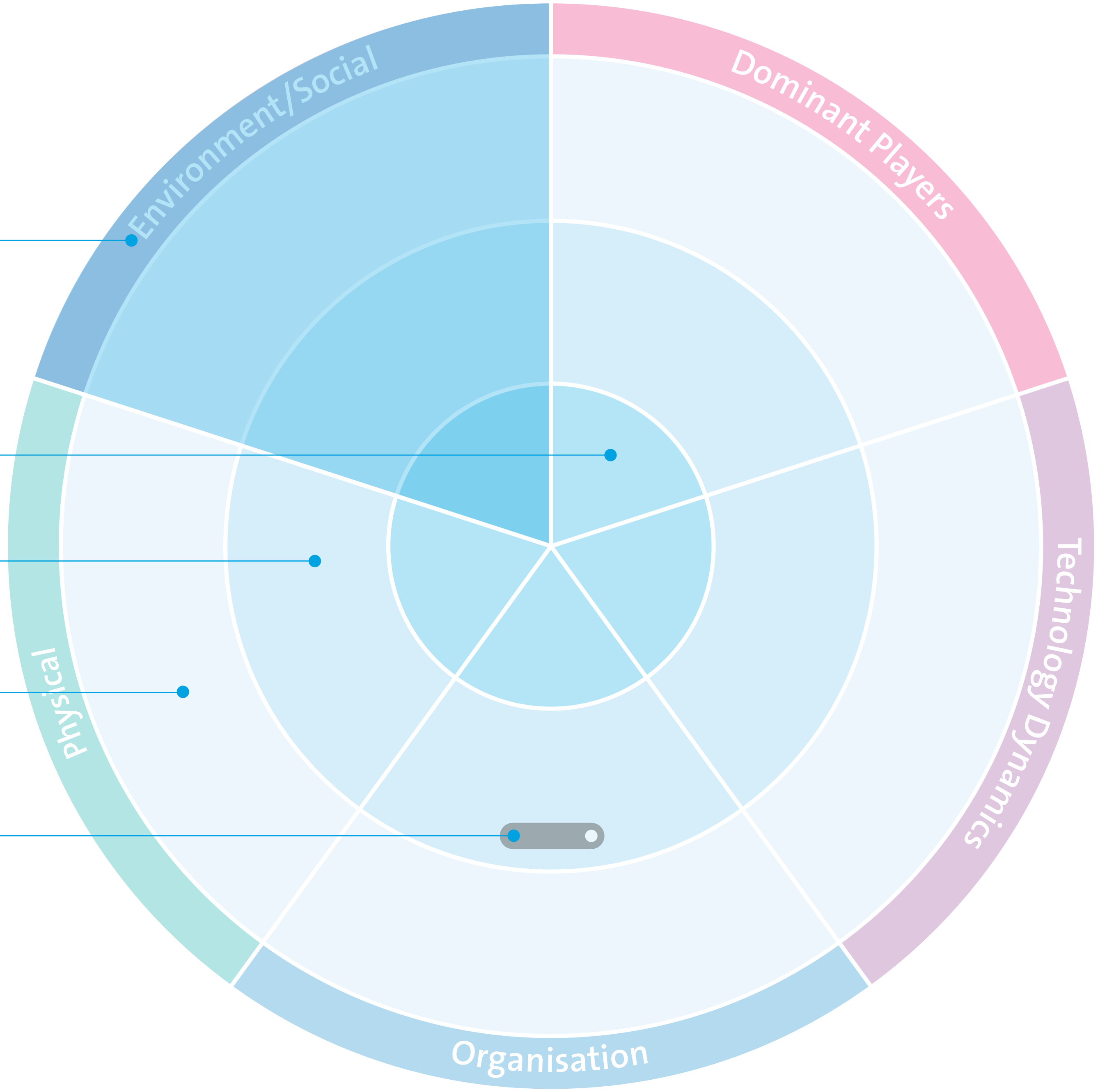
Method

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:

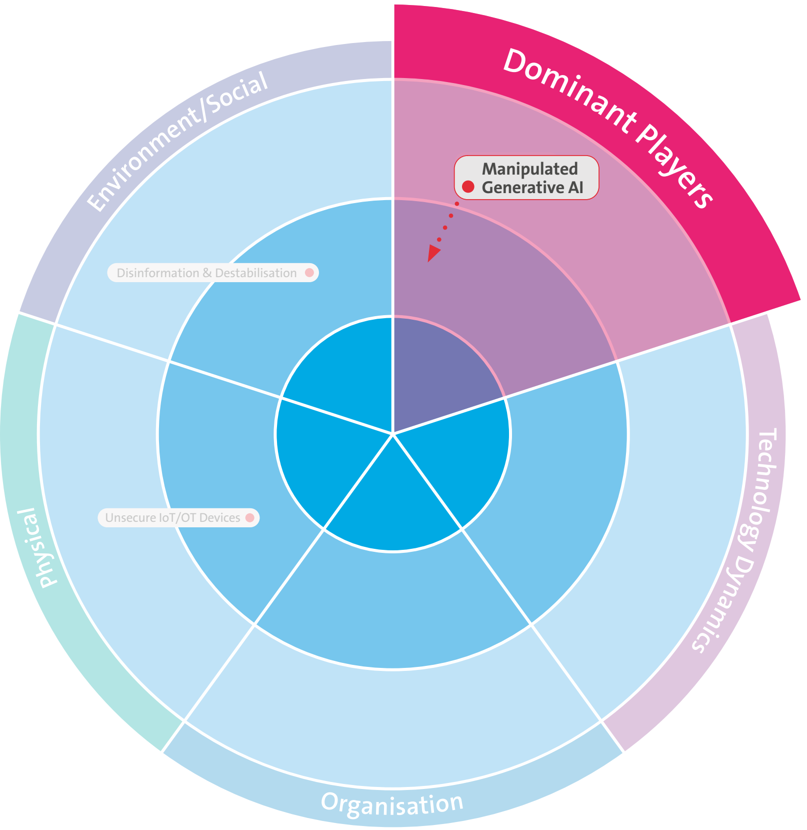
- **Focal points** for threats that are already real and can be managed with a relatively large input of resources.
- **Key themes** for threats that have already occurred sporadically and can be managed with the normal use of resources. Regulated processes often exist to efficiently counter such threats.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

Manipulated Generative AI or: How much can artificial intelligence be manipulated?



Over the past 15 years, digitalisation, virtualisation and the emergence of cloud computing have significantly shaped the IT landscape, playing a crucial role in the rapid expansion of Generative AI. The launch of ChatGPT in November 2022 garnered significant media attention. Generative AI has been rapidly adopted by society. Many innovative companies have been inspired by this wave of enthusiasm, leading them to launch numerous new applications onto the market.

The global interest in AI has also meant that the theme has been more closely scrutinised within the field of security. Questions about security risks were quickly raised and needed to be answered because – as always – there are also some downsides to innovation. Despite the significant advances that AI and machine learning have made, these technologies are still vulnerable to attack. In many sub-areas, new standards are still being developed, including regulations such as the AI Act. There are also a number of unknown factors to consider, which are only possible to prepare for to a limited extent.

Three aspects of AI systems can be identified in the context of cybersecurity:

1. Use of AI systems to launch attacks: Notable examples include the refinement of well-known types of attacks such as CEO fraud and business email compromise (BEC) attacks using AI-generated videos instead of simple emails; more realistic phishing emails → AI-based attacks

2. Use of AI to detect and defend against attacks (e.g. in spam and phishing filters), in anomaly detection in network traffic, workflow support in cyber defence (e.g. as a co-pilot), in the automation of analysis steps, the creation of incident timelines or communication with users. Overall, we can anticipate the development of additional intelligent and automated security solutions in this area.

3. Security loopholes in deployed AI systems – and here we are talking about manipulable artificial intelligence – can specifically be found in:
   the Top 10 for LLM (owaspai.org) and/or the
   MITRE ATLAS (atlas.mitre.org).
   Therefore, this concerns AI security risks and is not about risks from the use of AI systems.

In our view, the following topics are particularly relevant in the third aspect – in addition to numerous other possible opportunities for attack:

- **Manipulation of inputs (e.g. prompt injections)**
  These attacks aim to bypass existing security mechanisms by manipulating inputs, and consequently unintended results are produced by the operator of the AI system. For example, this may involve the disclosure of confidential information or the generation of unwanted content or unwanted behaviour.

- **Poisoning attacks**
  Even during the training phase of AI systems, the system can be manipulated by infiltrating malicious, false or corrupted data. One example would be inserting inappropriate language into audio recordings so that a chatbot interprets these instances as general enough to use in customer interactions.

- **Supply chain attacks**
  These are attacks directed at external components of AI systems. One example would be the infiltration of malicious code into open-source libraries that are utilised within an AI model.

There also continues to be a risk of DoS (denial of service). For instance, a user could intentionally or unintentionally use up all resources with one input and paralyse the system.

Other AI risks should also be mentioned briefly, such as 'Shadow AI', where employees use AI systems in an uncontrolled manner, thereby jeopardising the confidentiality of the company, customers or other sensitive data. This jeopardises data security. Safeguarding sensitive company data and establishing trustworthiness in the AI system are absolutely imperative.

'Due to the unpredictable nature of GenAI and LLMs, we are facing new security challenges and risks. An in-depth understanding of how LLMs work is essential for defining and implementing appropriate security measures.'

Beni Eugster
Swisscom Outpost

What should companies and organisations focus on when dealing with the risks of artificial intelligence?

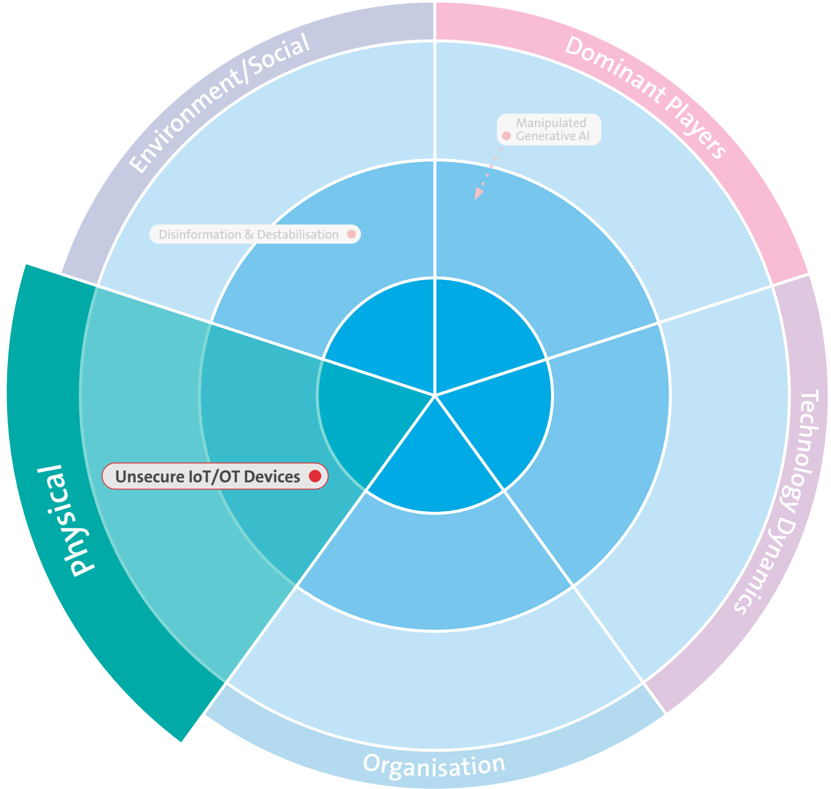
- Monitor current developments and react quickly to changes
- Implement employee training
- Carry out careful risk analyses before using AI systems (including from third parties) for possible impacts
- Check and implement security measures at all levels of the AI life cycle. Consider security controls from NIST AI RMF, MITRE ATLAS and OWASP for AI security.
- Maintain good relationships between AI and security teams. Regularly update regulations and guidelines in response to new developments.
- Develop instructions for dealing with AI in your organisation.
- Observe legal frameworks: The AI Act already mandates special security measures for risky AI systems or restricts their use. The EU's AI Regulation carries extraterritorial implications and, therefore, also applies to Swiss companies under specific conditions. Copyright and liability when using third-party AI systems as SaaS solutions are also risks that should not be ignored.

'The rapid advancements in the AI landscape will exacerbate the challenges of managing AI security risks. And at a fast rate, too. To effectively respond to changes, it's vital to continuously monitor ongoing developments.'

Raiko Zwilling
Security Officer Group Companies

Challenges and trends

Security risks from increasing digitalisation in areas ranging from production facilities to operating theatres



In today's complex and interconnected world, IoT (Internet of Things) and OT (Operational Technology) devices are a key part of daily activities across various areas of life. The technology fulfils a variety of tasks, both simple and complex – from home entertainment and smart home applications to the control of production systems in industrial plants and the monitoring of critical infrastructures.

However, the growing interconnectedness of these devices also presents considerable security risks. Insecure or inadequately protected IoT/OT devices can be compromised and sabotaged, potentially serving as gateways for cyberattacks. Such devices not only face limitations in their functionality, such as availability or data integrity, but also pose risks to the physical safety and well-being of people. The security of IoT/OT systems is, therefore, of crucial importance, as attacks on these systems can cause considerable damage.

The risks associated with insecure IoT/OT devices are diverse and can vary depending on the specific area of application. The main risks include:

- **Operational disruption**
  A security breach can render critical systems temporarily or permanently non-operational, resulting in substantial production downtime and financial losses.

- **Intellectual property theft, data loss or data theft**
  Unauthorised access to IoT/OT devices can result in the theft of sensitive data, including intellectual property and trade secrets. This can undermine a company's competitiveness and expose it to data breaches, as well as financial losses.

- **Manipulation of device data and sabotage**
  Attackers can manipulate data from IoT/OT devices to produce false information that can lead to incorrect decisions or faulty products. In industrial settings, attackers can disrupt or manipulate critical infrastructure, leading to outages and even endangering human safety.

- **Network infiltrations**
  Once compromised, IoT/OT devices can serve as a gateway to infiltrate deeper into networks, exacerbating the potential for further damage. IoT/OT devices can be infected with ransomware that locks important functions or encrypts data until a ransom is paid. They can also be integrated into botnets and thus pose a threat to other systems.

- **Compliance violations**
  Companies operating in regulated sectors could violate data protection laws or industry standards through security loopholes in their IoT/OT systems, which could lead to fines and sanctions. The European Cyber Resilience Act will play an important role in the future, particularly in the area of product liability. The potential damage and financial repercussions of insecure IoT/OT devices are extensive and can lead to economic losses, the impairment of public security, interruptions to critical services and the erosion of public trust. In extreme cases, attacks on OT systems in critical infrastructure can even result in environmental disasters or pose threats to human life.

In addition to the direct costs of remedying security breaches and restoring affected systems, companies also have to deal with indirect costs such as loss of sales due to business interruptions, compensation payments to affected customers or business partners, and higher insurance premiums.

The challenge of managing OT systems are due to the fact that:

- some of them have remote service access via the Internet.
- these systems comprise both very old and new and complex technologies, but legacy protocols and devices also exist; security mechanisms (encryption, authentication, etc.) are not in place and networks that were once separate are being integrated due to increased digitalisation.
- there are still not many sources of expertise and technology support available (e.g. outdated Windows versions or laptops with RS232 connections, etc.).
- there is still a discrepancy between security and safety. Consequently, there are conflicting objectives, such as prioritising access protection with passwords versus the ability to intervene quickly in the event of risks.
- the baby boomer generation, which is familiar with the systems, is retiring.
- there is increasing regulatory pressure for operators (NIS2, DORA, etc.) and manufacturers (RED2, CRA, etc.).
- the importance of security in organisations is underestimated or there may be an unclear delineation of responsibilities regarding security measures.

Faced with these challenges, companies need to take proactive measures to secure their IoT and OT devices. These measures include:

- **Risk assessment**
  Regular security assessments and audits to identify and eliminate potential vulnerabilities.

- **Security guidelines**
  It is important to develop and implement security guidelines based on proven standards such as the IEC 62443 series of standards. These guidelines facilitate the secure configuration and management of IoT/OT devices. Furthermore, integrating security-by-design principles can enhance security during the development of the devices.

- **Ensure technology is up to date**
  Update and patch outdated systems, maintain control over vulnerability management and segment the network, if necessary.

- **Employee training**
  Enhance awareness and provide training to all employees and service technicians on how to work with IoT/OT devices to mitigate human error.

- **Active monitoring and controls**
  Carry out regular safety checks and continuously monitor systems.

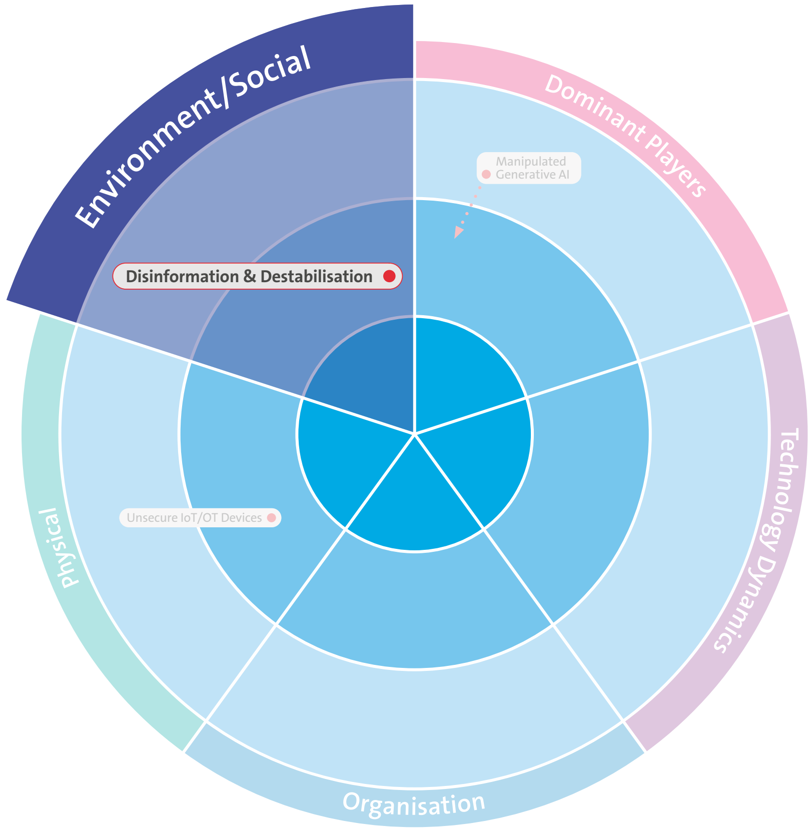
- **Collaborations**
  Collaborate with trustworthy providers. Choose devices and software from providers who demonstrably prioritise security and consistently provide updates.

‘Securing IoT and OT infrastructures is a task that companies should not underestimate and is crucial for maintaining operational security and long-term commercial success. The security of OT systems is not optional and must be given the same priority as the security of IT systems.’

Thomas Dummermuth
Head Physical Security & Safety, BCM

Challenges and trends

Disinformation and destabilisation – reality checks



Disinformation is currently a significant concern for companies and organisations. With the exponential growth of digital platforms and the speed at which information can be disseminated, organisations face the challenge of safeguarding the integrity of their information. They must also combat disinformation, which can compromise their brand, business and security credentials.

The Global Risks Report 2024 published by the World Economic Forum (WEF) highlights how disinformation has become a significant social challenge and consequently also a threat to companies and organisations. AI-generated fake news and cyberattacks are identified as pressing global risks, particularly as major elections approach in countries like the USA, the UK and India.

Companies are increasingly becoming targets of disinformation campaigns aimed at damaging their reputation, deceiving consumers or even influencing their stock market value. In an era where information can be disseminated globally in seconds, an organisation's ability to respond effectively to disinformation is critical to maintaining corporate integrity and stakeholder trust.

The risks posed by disinformation include not only external threats, such as damage to public perception, but also internal risks, such as the dissemination of false information within the organisation, which can lead to wrong decisions and security loopholes. Security experts stress that the safeguarding of company data and infrastructures is closely linked to the ability to detect and combat disinformation. As AI technology rapidly evolves, particularly in image and video generation, the proliferation of deepfake attacks and disinformation campaigns are possible that are difficult to detect by conventional means.

In the context of cybersecurity, disinformation campaigns have the potential to affect both public opinion and the internal security protocols within companies and organisations. Attackers can use disinformation to orchestrate targeted phishing attacks, instil uncertainty and deceive employees into disclosing confidential information or carrying out malicious actions. The subject of 'disinformation and destabilisation' is also present in the attack vectors 'attacks based on AI' and 'big data analytics'. Identifying and defending against disinformation should therefore be a key part of a company's security policy.

Strategies companies can employ to combat disinformation

1. **Strengthen internal communication channels:** A clear and transparent internal communication strategy is imperative to ensure that employees receive and disseminate the right information.

2. **Training and sensitisation:** Employees must be regularly trained to recognise and respond correctly to disinformation. This includes understanding the risks associated with the dissemination of false information.

3. **Use of technologies:** Harnessing artificial intelligence and machine learning can help companies to detect disinformation campaigns at an early stage. AI can play a key role in analysing the dissemination of false information, identifying its origins and implementing appropriate countermeasures.

4. **Proactive public relations and crisis management:** Swift and decisive action is essential when confronting a disinformation attack. Organisations should develop preparedness plans to address disinformation, which includes working with the media and using their channels to disseminate accurate information.

5. **Partnerships and collaborations:** Collaboration with external experts, other companies and organisations can provide valuable insights into best practices when dealing with disinformation and promotes the development of common standards and responses.

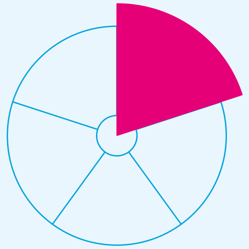
It is imperative for companies to acknowledge that disinformation poses a significant threat to both their business activity and reputation. It was for good reason that the German Association for Security in Industry and Commerce introduced disinformation protection as the fourth quadrant in its security focus back in 2019 as part of its 'Security study on disinformation attacks on companies'.

The WEF Global Risks Report 2024 emphasises once again that combating disinformation is a crucial component of corporate security and strategy. Organisations can effectively protect themselves and their shareholders by adopting a comprehensive strategy that encompasses education, technology and proactive engagement. At a time when the lines between true and false information are becoming increasingly blurred, it is critical that organisations are at the forefront of maintaining the integrity and trustworthiness of their information.

> *'The deliberate dissemination of false information, commonly referred to as fake news, can cause economic and social instability. Cyberspace is also being deliberately misused for this purpose. Companies need to be aware of this danger so that they can adequately prepare for and respond to this type of threat.'*

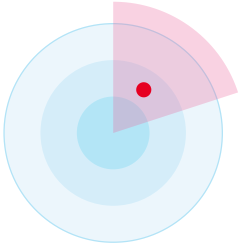
Marcus Beyer
Security Professional and
Security Awareness Officer

Details including tendencies and comparison with the previous year



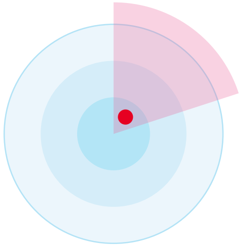
Dominant Players

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



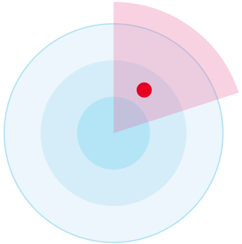
Concentration Data & Cloud Services
Intensively centralising data in the cloud leads to cluster risks. The failure of a service or central service can have a global impact.

► Unchanged



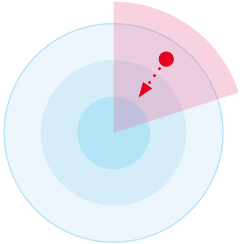
Infrastructure Integrity
Vulnerabilities may have been negligently or deliberately built into essential components of critical infrastructures, jeopardising system security.

► Unchanged



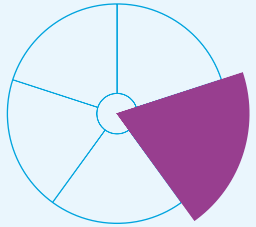
Legacy Protocols
Due to software dependencies, completely outdated and vulnerable protocols are still used (e.g. NTLMv1, SMBv1, RC4), resulting in a few applications endangering the security of entire infrastructures.

► Unchanged



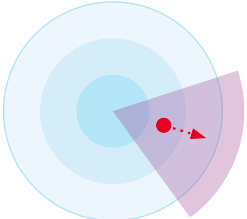
Manipulated Generative AI
Targeted manipulations can alter the output of an AI system. This may involve the infiltration of malicious, false or corrupted data during the training phase, the theft of LLMs, as well as prompt manipulation, which may result in adverse and legally binding ramifications.

▲ Increased



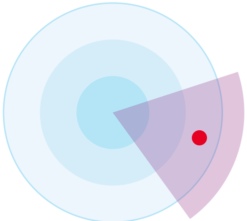
Technology Dynamics

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.



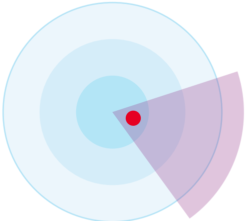
5G Security
5G is still a new mobile telecommunications technology. Its introduction will bring many opportunities as well as still unknown threats.

▼ Decreasing



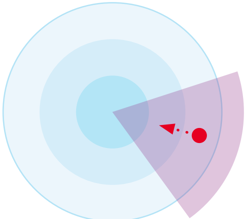
Quantum Computing
Quantum computers can render existing cryptographic methods useless because they can bypass them in a very short time.

► Unchanged



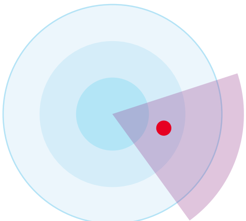
Ransomware
Critical data is encrypted on a large scale and (possibly) decrypted again in return for a ransom payment.

► Unchanged



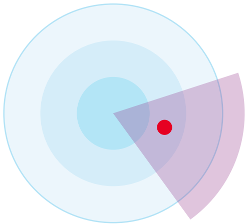
Increased Complexity
The complexity of systems, especially across technology and company boundaries, is constantly increasing. IT landscapes are becoming more complex, especially in the hybrid/multi-cloud environment with its many cloud providers. This increases risk exposure and makes troubleshooting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

▲ Increased



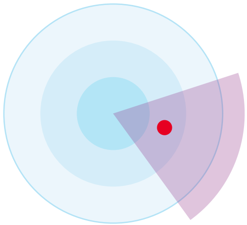
AI-Based Attacks
AI-based attacks are more targeted and therefore more difficult to detect. They can be carried out more efficiently on classic attack vectors such as ransomware, phishing, spear phishing and occasionally also in new scenarios such as deep fakes, disinformation and similar.

► Unchanged



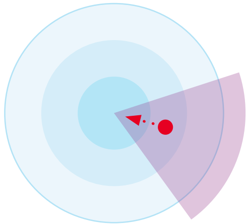
Targeted Attacks
Targeted and complex attacks to achieve a specific goal. Key people are identified and targeted directly or indirectly (lateral movement, social engineering methods) in order to obtain relevant information or cause maximum damage. One essential aspect is persistence, which means the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



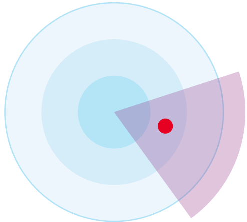
DDoS Attacks
A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal data traffic of a target server, service or network by flooding the target or surrounding infrastructure with a deluge of internet traffic. DDoS attacks achieve their effectiveness by using multiple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



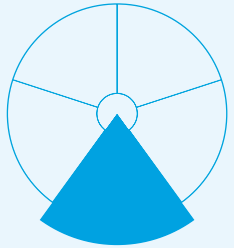
Supply Chain Attacks
Supply chain attacks aim to exploit trust and commercial relationships between a company and external parties. These relationships may include partnerships, supplier relationships or the use of third-party software.

▲ Increased



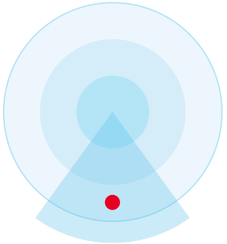
Subscriber Compromise
Malware gains access to the private data of mobile users or is used to attack the telecommunications or IT infrastructure. Phishing, smishing, vishing and MFA bypass attacks target subscriber credentials. Entire digital identities are consequently stolen and taken over during the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

► Unchanged



Organisation

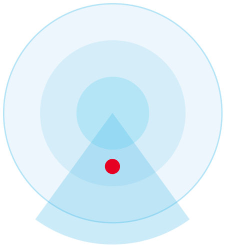
Organisation means threats that emanate from changes in organisations or that exploit weaknesses in organisations.



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.

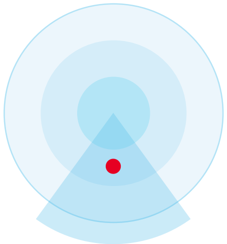
► Unchanged



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.

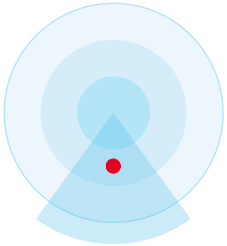
► Unchanged



Insider Threat

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

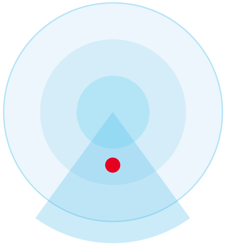
► Unchanged



Digitalisation

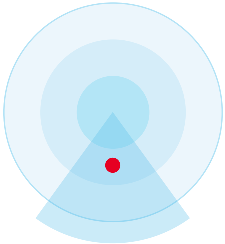
The way the real world is increasingly connected to the virtual world in both private and business domains is creating more avenues of attack. The 'New Work' concept and the shift to remote working also increase cyber risk and the vulnerability of the IT infrastructure via unsecured end devices.

► Unchanged



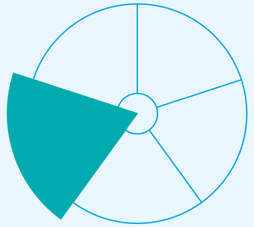
Security Skills
Due to the complexity of cyberattacks and advancing digitalisation, security skills and the deployment of cyber professionals within organisations are becoming indispensable. The threat of 'downskilling' – the unlearning of knowledge – through automation in IT can lead to new attack vectors.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

► Unchanged



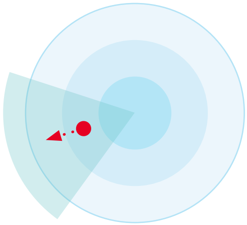
Infrastructure Misconfiguration
Exploitation of misconfigured infrastructure components and/or vulnerabilities that are identified and fixed late. The fact that technical operating processes are automated more than ever before will have a greater impact if there are successful attacks or misconfigurations.

► Unchanged



Physical

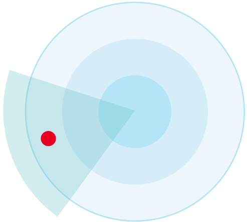
This term covers attacks on infrastructure in cyberspace that will cause increased damage in the physical world. But it also includes threats that emanate from the physical environment, which are usually aimed more at physical targets.



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.

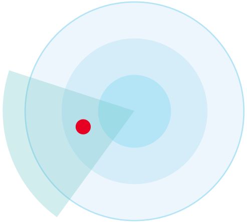
▼ Decreasing



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.

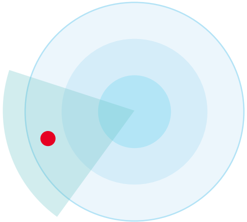
► Unchanged



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.

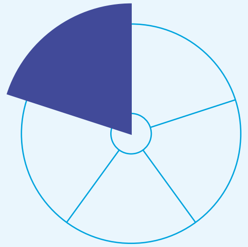
► Unchanged



Environmental Influence

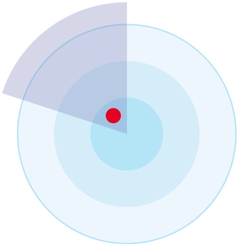
The climate crisis is leading to a rise in unpredictable weather patterns and extreme weather events, including heatwaves, heavy rainfall, tornadoes, hailstorms and lightning strikes. This can cause damage to the infrastructure of organisations and companies and significantly affect the external and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

► Unchanged



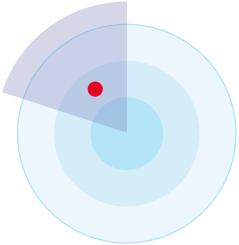
Environment/Social

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.



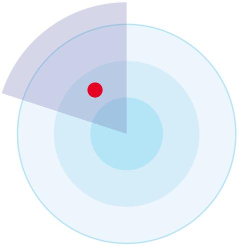
Security Job Market
The demand for security professionals is enormous and can only be met with great difficulty. This leads to decreasing levels of expertise that are needed to combat increasingly complex and intelligent attacks.

► Unchanged



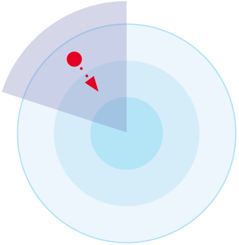
Digital Identity
Authenticated, personal digital identities can be misused or stolen. For example, this information can be used to sign off contracts under someone else's name.

► Unchanged



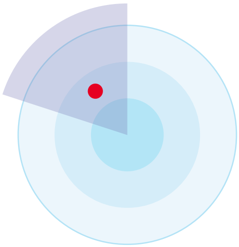
Disinformation & Destabilisation
The deliberate dissemination of false information can lead to economic and social instability and is increasingly being used in a targeted way via cyberspace, especially in crisis scenarios.

► Unchanged



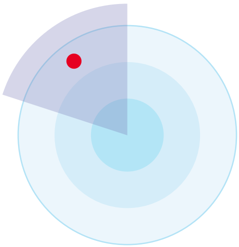
Political Influence
Political trends can influence technological or economic decisions, such as in the selection of technology suppliers. This can lead to new risks.

▲ Increased



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

► Unchanged



Geopolitical Situation / State Level Attacks
During times of wars, 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 hactivist groups, state-sponsored entities 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

Summary

Achieving strong cyber resilience requires interdisciplinary and cross-departmental effort. The following 5-step model can be helpful:

1. **Identify**
   Identification entails analysing available data, determining its relevance to protection and managing both the storage and processing of this data. It is also important to be aware of potential risks and threats and to ensure security measures are in place across the supply chain.

2. **Protect**
   All employees across hierarchical levels must undergo training and awareness programmes on cybersecurity. Bug Bounty programmes and red teaming attacks also help to strengthen resilience. It is also advisable to integrate new security philosophies such as zero trust.

3. **Detect**
   Continuous monitoring of your company's infrastructure and internal network is essential. Increased automation of the Security Operations Center is also a logical step to take.

4. **Respond**
   It is extremely important to respond quickly to security incidents. 'Near misses' should also be recognised and documented so that valuable lessons can be extracted from them. In addition, an operational crisis management system should be set up and trained.

5. **Recover**
   A well-prepared communication strategy in the event of a crisis helps to maintain trust. In addition, service and business continuity plans are recommended to ensure smooth operations.

Physical security should not be overlooked, despite often being neglected in cybersecurity. Physical attacks can compromise a company's resilience against cyberthreats.

For example, extreme weather conditions such as drought, heatwaves, floods and cold periods can cause damage to infrastructure, which can affect the resilience of cyber services, both nationally and internationally. Conversely, cyber incidents can also have a serious impact on physical areas. It is therefore crucial to consider both physical security and cybersecurity and implement appropriate measures to bolster the resilience of organisations.

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
Copyright	© April 2024 by Swisscom (Switzerland) Ltd, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Print	OK DIGITALDRUCK AG, Zurich
Edition	200 copies

As ‘Innovators 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.ch/securityjobs

#BeTheStrongestLink