swisscom

Cyber Security Threat Radar 2021/2022

Always reassess risks and environment

Contents

> *“Only security that is precisely adapted to the needs of the user will be able to fulfil its task in the medium and long term and create the necessary resilience.”*

Cyber Security Threat Radar

What was unthinkable until recently has been a sad reality since 24 February. **Right now, the war in Europe is changing our world.**

With the outbreak of the war in Ukraine, I once again became acutely aware of the role and importance of media, especially social media. Stirring reports, blatant falsehoods and virtuoso performances constantly alternate with subtle disinformation.

The fact is that, since the start of the Russian invasion of Ukraine, many threats and risks have become even more of a focus for governments, organisations and companies than was already the case during the pandemic situation of the last two years. The tense situation is making itself felt throughout society.

Now for the good news: despite the difficult situation, no increase in attacks has been observed in the Swiss network infrastructure so far.

Of course, cyber criminals are trying to exploit the war in Ukraine for their illegal activities, for example via suitably adapted phishing attempts or manipulated appeals for donations. Unfortunately, this is common practice during major events. The number of illegal cyber activities remains at a consistently high level — it's just the story behind them that has changed.

I hope that this Cyber Security Threat Radar 2021/2022 gives you valuable insights into the issue of cyber security and helps you to develop your activities around the topic of security in your company or organisation.

Philippe Vuilleumier
Head of Group Security
Swisscom (Switzerland) Ltd

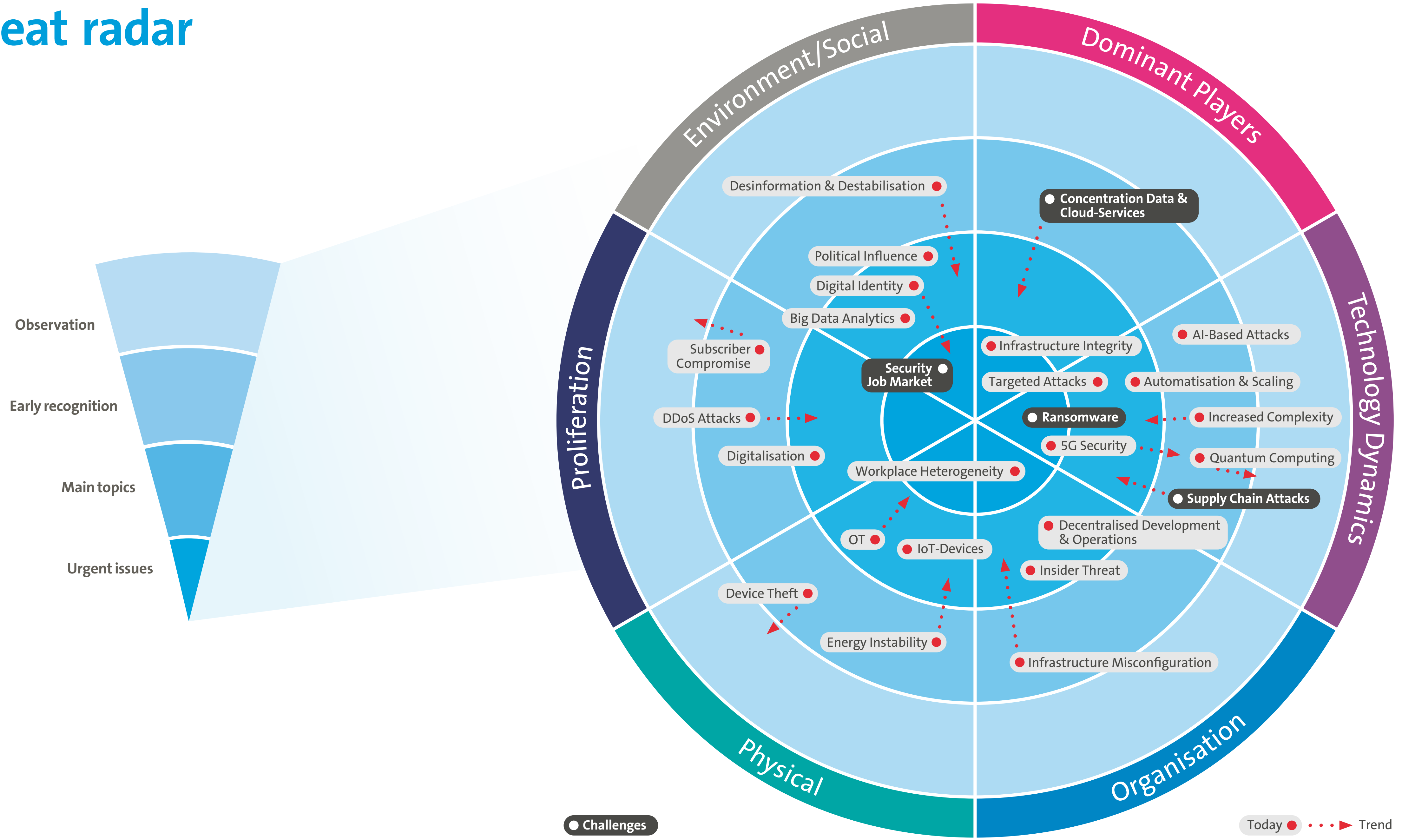
My statement from last year's Cyber Security Threat Radar, "Special situations call for special measures in terms of security, protection and risk awareness", has lost none of its relevance — on the contrary. Especially in this disruptive situation, it is important to maintain an overview in order to be able to take the right measures in a timely manner.

And, at the heart of these measures, are people. Of course, technology is an indispensable building block of the security system. But technology alone does not guarantee protection. That's why I urgently recommend putting people at the centre of all security considerations, solutions and measures. Only security that is precisely adapted to the needs of the user will be able to fulfil its task in the medium and long term and create the necessary resilience.

Current situation — threat radar

Being able to fall back on tried and tested security strategies and procedures at the right moment helps us to deal with unpredictable events — so-called “black swans”. Combined with a consistent security culture, error transparency and properly trained staff, they create the basis for organisational resilience.

This requires potential threats to be recognised at an early stage and systematically recorded. To map the threat situation and its evolution, we use the well-known Cyber Security Threat Radar.



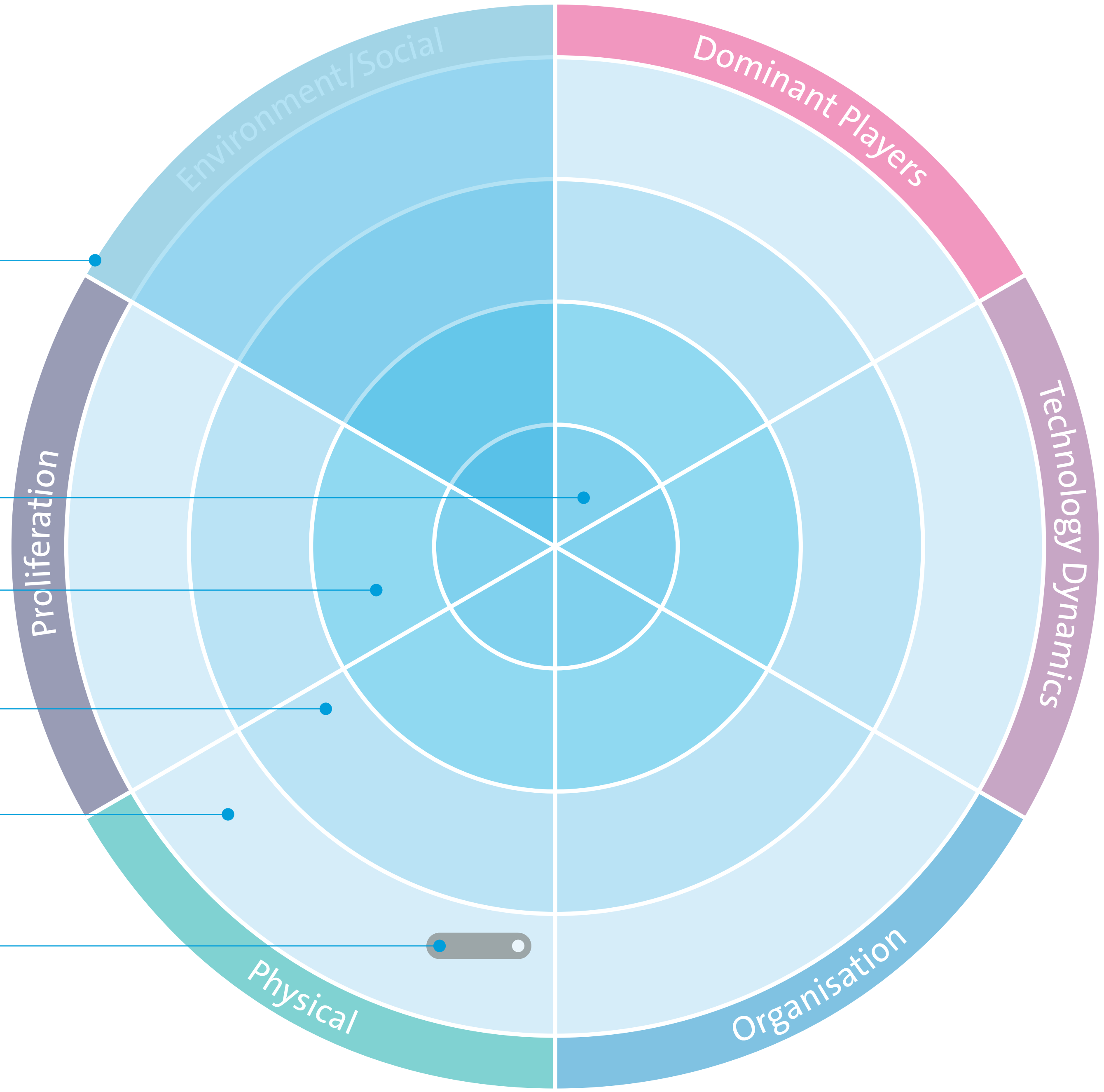
Methodology

The threat radar is broken down into six **segments**, which demarcate the different threat domains. The threats belonging to each of these **segments** can be assigned to one of four concentric circles. The circles indicate each threat's urgency and thus also the vagueness inherent in assessing such threats. The closer the threat is to the centre of the circle, the more concrete it is and the more important it is to take appropriate countermeasures.

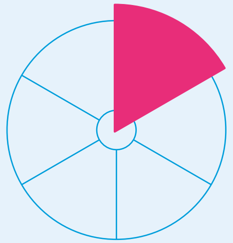
We refer to the circles as follows:

- **Urgent issues** in the case of threats that are already a reality and are being managed with a relatively large deployment of resources.
- **Main topics** in the case of threats that have already materialised on occasion and are managed with a normal deployment of resources. Defined processes often exist to efficiently counter threats of this nature.
- **Early recognition** for threats that have not yet materialised or are currently at a very low level. Projects have been launched with the goal of addressing imminent growth in importance of these threats at an early stage.
- **Observation** for threats that are only expected to arise in a few years' time. No specific measures have been defined for handling these threats.

Moreover, the individual **threats** indicated by the points mentioned display a **trend,** which may be increasing, decreasing or stable in terms of its criticality. The length of the trend beam indicates the speed with which criticality of the threat is expected to change.

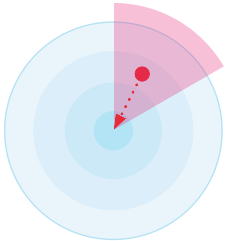


Details incl. trend and comparison with the previous year



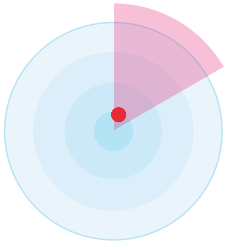
Dominant Players

This section summarises threats arising through dependencies on dominant manufacturers, services or protocols.



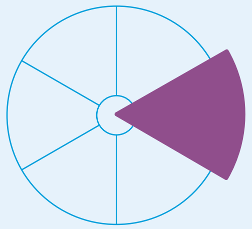
Concentration Data & Cloud Services
The strong centralisation of data in the cloud leads to cluster risks. The failure of a service or central service can have global implications.

▲ Increasing (note: read more on page 28)



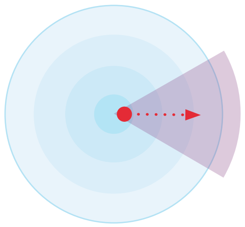
Infrastructure Integrity
Key components of critical infrastructures may have built-in vulnerabilities, either through negligence or deliberately, that endanger the security of the system.

► Unchanged



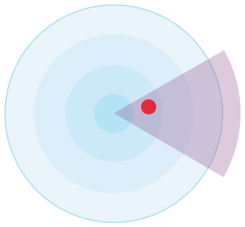
Technology Dynamics

This is the term used to describe threats arising from the swift pace of technological innovation, which not only offers attackers new opportunities to launch attacks but also enables them to develop new threats themselves.



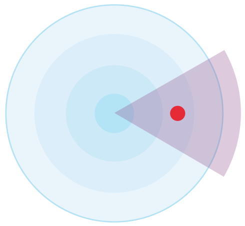
5G Security
5G is still a recent mobile telecommunications technology. Its launch will not only offer up a large number of opportunities, but also open the door to unknown threats.

▼ Decreasing



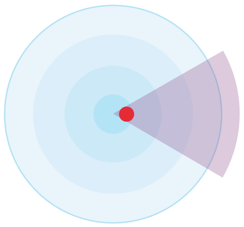
Automatisation & Scaling
The greater automation of technical operating processes will have a bigger impact in the event of successful attacks or misconfigurations.

► Unchanged



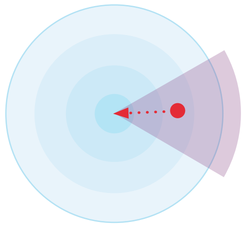
Quantum Computing
Quantum computers can make existing cryptographic processes unusable, since they are able to bypass them in next to no time.

▼ Decreasing



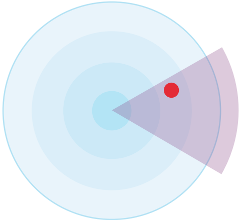
Ransomware
Large amounts of critical data are encrypted and only (possibly) decrypted in exchange for the payment of a ransom.

▲ Increasing (note: read more on page 32)



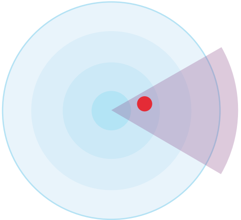
Increased Complexity
The complexity of systems is constantly increasing, particularly beyond technological and corporate boundaries. Especially in the hybrid / multi-cloud environment with many cloud providers, IT landscapes are becoming more complex. This increases exposure to risk and makes locating errors more difficult.

▲ Increasing



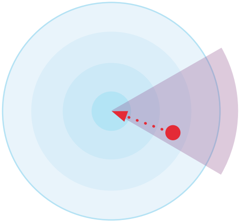
AI-Based Attacks
Attacks using artificial intelligence (AI) are more targeted and thus more difficult to detect. AI enables attacks to be executed more efficiently over classic attack vectors such as ransomware, phishing and spear-phishing, and also occasionally via new scenarios such as deepfakes, disinformation, etc.

► Unchanged



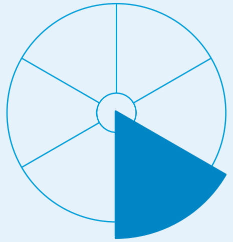
Targeted Attacks (APTs)
Targeted and complex attacks intended to achieve a specific objective. Key individuals are identified and attacked in a targeted manner directly or indirectly (lateral movement) in order to obtain relevant information or maximise the amount of damage inflicted. A key aspect is persistence, i.e. the attacker operating undetected for as long as possible.

► Unchanged



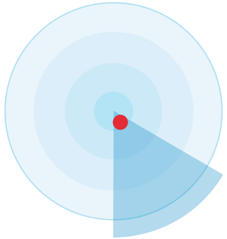
Supply Chain Attacks
Attacks on supply chains aim to exploit trust and business relationships between a company and external parties. These relationships may include partnerships, supplier relationships or the use of third-party software.

▲ Increasing (note: read more on page 36)



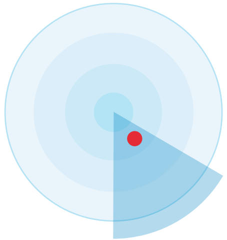
Organisation

Organisation refers to threats that arise through changes in an organisation or which exploit weaknesses in the organisation.



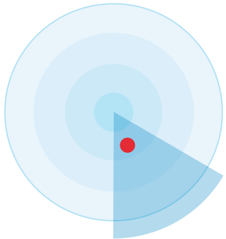
Workplace Heterogeneity
Alongside the many opportunities associated with new working models, the uncontrolled use of such models, such as “Bring Your Own Device” (BYOD), or the increased use of remote workplaces, exposes companies to greater risks.

► Unchanged



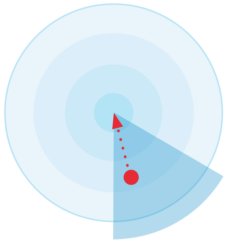
Decentralised Development & Operations
Traditional development departments are dying out and application development is moving more closely towards the business units, while at the same time release cycles are getting shorter. This makes it more difficult to control and/or manage security.

► Unchanged



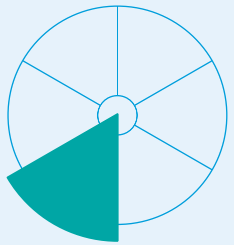
Insider Threat
Partners or employees manipulate, misuse or sell information, whether through negligence or intent.

► Unchanged



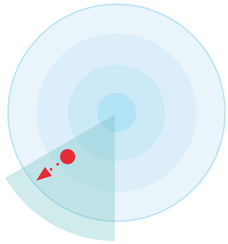
Infrastructure Misconfiguration
Exploitation of misconfigured infrastructure components and/or vulnerabilities, which are identified and rectified at a late stage.

▲ Increasing



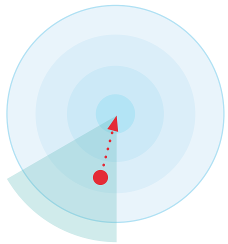
Physical

This heading includes attacks on the cyberspace infrastructure, which will increasingly cause damage in the physical world. However, it also includes threats that arise from the physical environment and are generally more focused on physical targets.



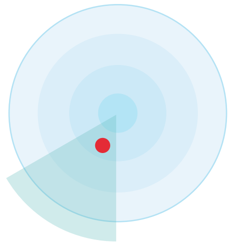
Device Theft
The theft or other loss of end devices such as smartphones and laptops, as well as relevant IT components, can lead to data loss or impair the availability of IT services.

▼ Decreasing



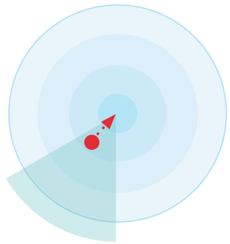
Energy Instability
Attacks on critical infrastructures such as electricity grid operators. Protection against outages is crucial and business continuity is also increasingly part of the cyber resilience debate. Power shortages, blackouts (widespread power failure) and even “blueouts” (widespread failure of water supply) are among the key issues. Media reports indicate that the vulnerability of critical infrastructures has increased significantly due to cyber attacks.

▲ Increasing



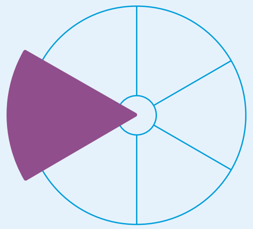
IoT-Devices
Poorly protected devices may be compromised and sabotaged. Such acts could limit the devices’ integral functions, such as availability or data integrity.

► Unchanged



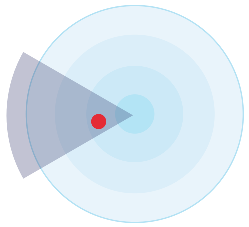
Operational technology OT
Operational technology (OT) is the use of hardware and software to monitor and control physical processes, equipment and infrastructure. OT is found in a variety of asset-intensive sectors and performs a wide range of tasks, from monitoring critical infrastructure (CI) to controlling robots on a factory floor. There are still many control systems for critical infrastructure installations that are either poorly protected or not protected at all.

▲ Increasing



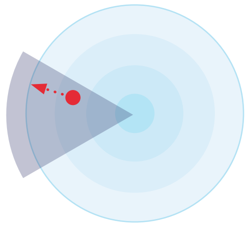
Proliferation

Threats that take advantage of the increasingly easier and cheaper availability of IT media and expertise come under the heading of “proliferation”. This prevalence leads to more attack surfaces and increases the availability of attack targets.



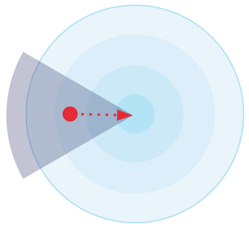
Digitalisation
Increasing levels of interconnection between the real and virtual world of people’s private and work lives open up more avenues of attack. “New Work” and the shifting of work to home office environments also increase the cyber risk and the vulnerability of the IT infrastructure due to unsecured end devices.

► Unchanged



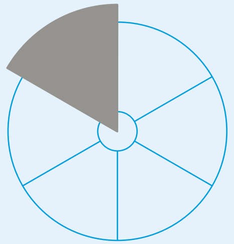
Subscriber Compromise
Malware gains access to mobile users’ personal data or is used to attack telecommunication and IT infrastructures.

▼ Decreasing



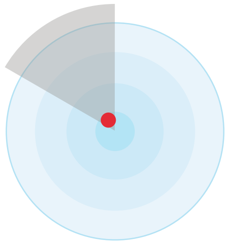
DDoS Attacks
A denial of service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a target server, service or network by overwhelming the target or surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve their effectiveness by using multiple compromised computer systems as sources for attack traffic. Exploited machines may include computers and other networked resources such as IoT devices. Rapid growth in the number of IoT devices coupled with low-level protection produces more “takeover candidates” for botnets.

▲ Increasing



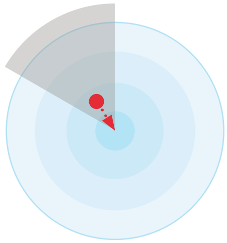
Environment / social

This refers to threats that emanate from socio-political changes or that become easier to abuse as a result of such changes and thus more valuable to attackers.



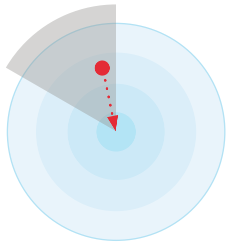
Security Job Market
The demand for security professionals is huge and extremely difficult to meet. This leads to decreasing expertise in the fight against increasingly complex and intelligent attacks.

► Unchanged (note: read more on page 24)



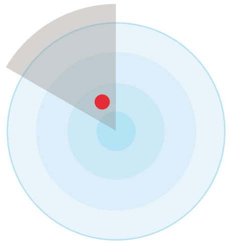
Digital Identity
Authenticated, personal digital identities may be misused or stolen, e. g. to conclude a contract under another person's name.

▲ Increasing



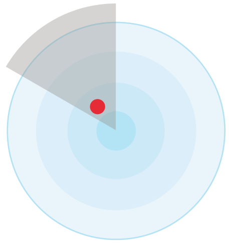
Desinformation & Destabilisation
The deliberate dissemination of false information can lead to economic and social destabilisation and is increasingly being deployed in a targeted manner via cyberspace, especially in crisis scenarios.

▲ Increasing



Political Influence
The political climate may influence technological or economic decisions, e. g. the selection of technology suppliers. This may give rise to new risks.

► Unchanged

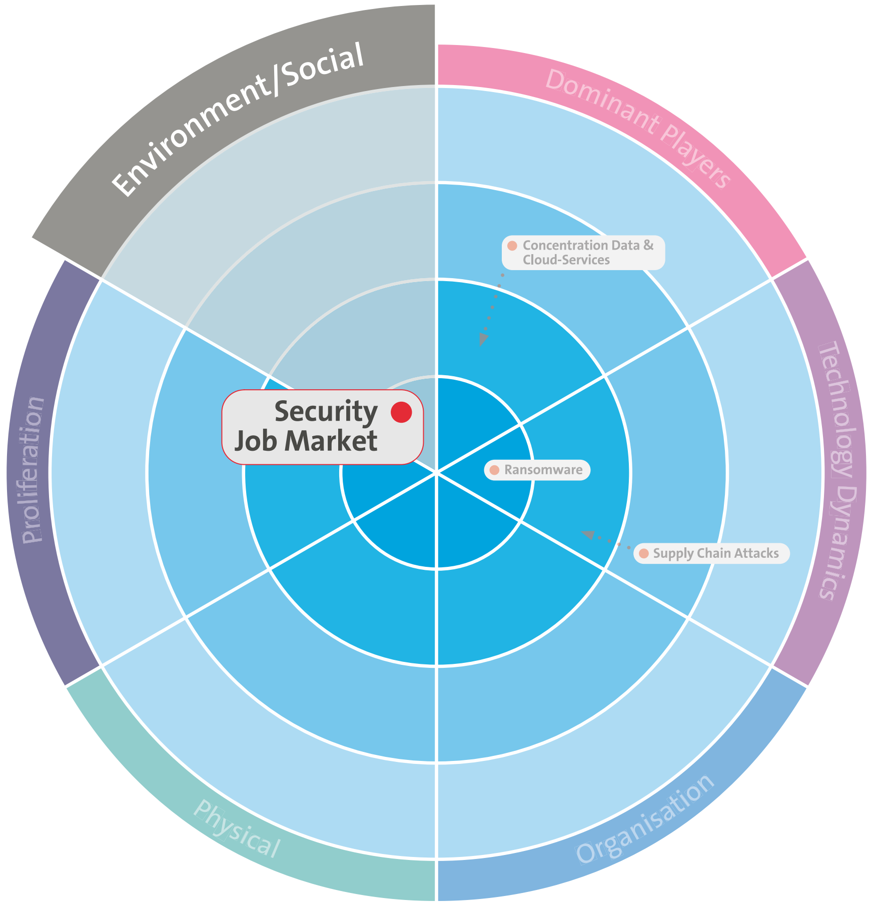


Big Data Analytics
More data and better analysis models may be misused in order to influence human behaviour. Decisions are increasingly left to autonomous systems. Data from "big data lakes" are being used specifically for the purposes of disinformation, fake news and for social and psychosocial analyses, as well as to establish movement patterns. The latter is accompanied by invasion of privacy.

► Unchanged

Challenges and trends

Shortage of skilled workers in the security job market



What's it all about?

Hybrid, increasingly decentralised IT infrastructures, IoT environments and remote working: the demands on IT security systems are growing and threats are increasing, but skilled professionals are scarce. Companies need to bundle a number of measures to protect networks and data and build up expertise. Automation as well as education and training also play a role.

The current challenges in IT security are exacerbated by a lack of qualified specialists. The WEF's Global Risk Report 2022 also points to the global shortage of cyber security experts. It is estimated that there is a shortage of around three million skilled professionals on the labour market.

The International Information System Security Certification Consortium (ISC)² ran a survey on the potential consequences of staff shortages in cyber security. 32 % of respondents cite misconfigured systems as a possible consequence. Almost as many fear that there is not enough time for proper risk management or that something important will be overlooked. 27 % report that it is impossible to identify all threats to the network. Likewise, 27 % consider hasty installation and configuration of software due to staff shortages to be a real danger.

The study "ICT Skilled Workers Situation: Demand Forecast 2028" by the Swiss ICT training organisation ICT-Berufsbildung Schweiz predicts that around 118,000 additional ICT specialists will be needed in Switzerland by 2028. If this additional demand is to be met, around 36,000 more people would have to be trained than is currently the case. This is a challenge for education policy and the economy as a whole, and it calls for extraordinary measures. Companies in all sectors as well as public authorities are called upon to create new apprenticeships and university places in IT and mediamatics.

In view of such numbers, it is no surprise that companies are finding it difficult to find and retain suitable candidates. On average, it takes six months and requires several advertisements and interviews to fill a vacant position in IT. Moreover, small and medium-sized companies in particular not only find it difficult to hire specialists, but also to challenge them sufficiently over a longer period of time and thus also to retain them.

How will the challenge evolve?

Recruiting IT specialists is a challenge when there are not enough qualified and suitable professionals available. Many companies therefore try to keep the staff they have already hired. However, this alone will not solve the problem: the solution to these challenges will be to retain qualified staff and automate the day-to-day tasks.

The challenge faced by a company in finding the right professionals with IT security skills will continue to grow, as more companies (even smaller ones) need experts. The situation is further exacerbated by demographic changes in the labour market. Companies have less and less access to new and young skilled workers. The "war for talent" will intensify and security needs will increase in general. Crisis scenarios such as the war in Ukraine will further increase and strengthen the awareness of security in companies and organisations.

The shortage of specialists in the field of cyber security will make itself felt in two ways. Firstly, there is a lack of digital experts in the development of IT security solutions, while cyber-crime attacks are becoming increasingly sophisticated and targeted. Secondly, companies lack the qualified IT security officers capable of countering the increasing threat of cyber crime with appropriate measures.

The shortage of IT specialists affects small and medium-sized enterprises (SMEs) in particular, as qualified staff often prefer large corporations, with more attractive salary models and/or social benefits, to smaller companies.

To alleviate the lack of personnel, more and more universities are offering special courses in cyber security. Whether this will rapidly solve the structural problems, however, remains questionable. It takes a lot of time to build up the necessary expertise and, in addition to purely theoretical training, a certain amount of practical experience is also needed. A more promising approach could be one in which companies become practically involved in research and teaching, along with their technical departments and specialists. Companies should also capitalise on interested employees by focusing more on their further training in the area of cyber security. However, this will probably not be enough to close the gaping personnel and associated security gap, at least in the medium to long term. In understaffed security departments, not only is there a shortage of specialised knowledge, but the experts are usually also working hard at the limits of their capacity, which is of course not a healthy basis for their own cyber security.

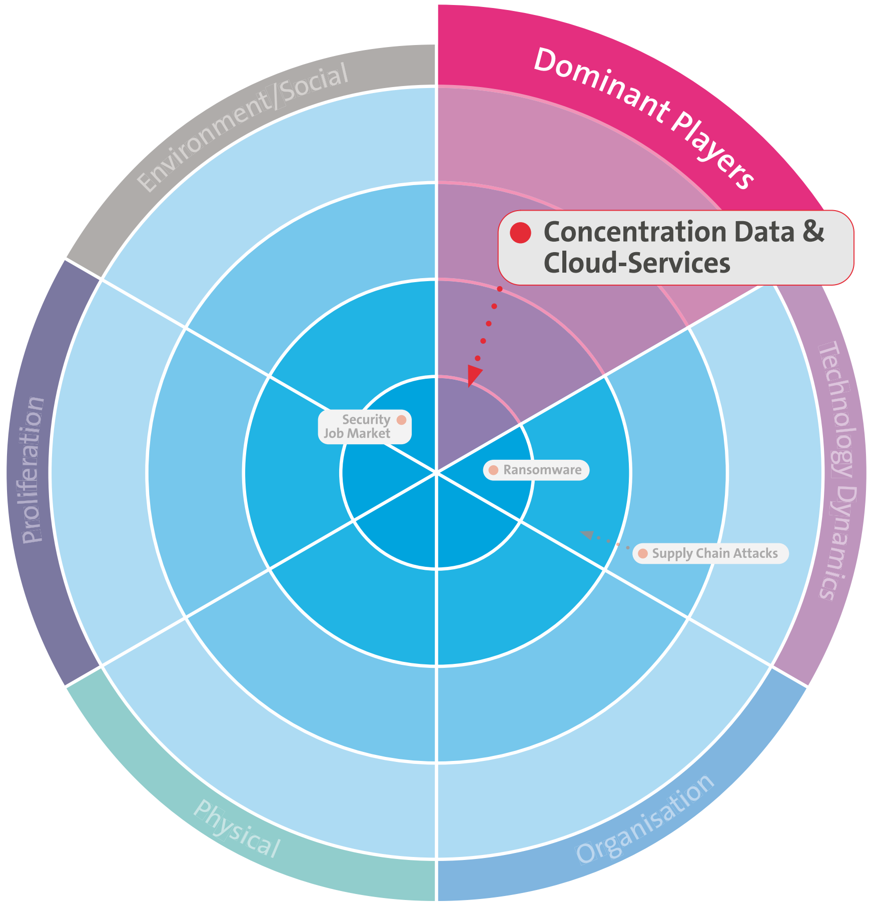
How can we deal with the challenge effectively?

- Maintaining the attractiveness of the employer and retaining employees in the company
- Talent needs practical support
- Investing in specialist in-house training and establishing attractive training programmes
- Offering development opportunities within the company and a high level of employability
- Making greater use of social media for recruitment and being visible at specialist events
- Using employer brand marketing and the employee network
- Establishing junior programmes and/or promoting opportunities for juniors (making future employees fit for the task)
- Internal bug bounty programmes can also unearth talent
- Automating standard processes and software support even for complex tasks
- Integration of an external MSSP (Managed Security Service Provider)

> *"You don't always need fully trained experts. We have good experience with professionals from adjacent fields of expertise (developers, network admins, etc.) and young people who have completed their education and wish to pursue the subject further."*
>
> **Dimosthenis Georgokitsos**
> Program Manager Cyber Security,
> Recruiting & Education, Swisscom (Switzerland) Ltd

Challenges and trends

Hybrid/multi-cloud in concentration data and cloud services



What's it all about?

In a multi-cloud solution, a company uses several different cloud services, often from several providers. The multi-cloud offers flexibility and choice, but also leads to complexity. However, the "right" cloud solution for most companies is neither public nor private, but a combination of the two.

Multi-cloud is part of the journey to the cloud. After a successful migration and/or onboarding of cloud services, the realisation that another cloud is needed becomes a necessity. There are several reasons for this, e. g. risk; lock-in; services; projects; decentralised DevOps teams using different cloud platforms. Most often, this is a multi-Azure, GCP or AWS cloud environment. The underlying services need to be managed multiple times, leading to inefficiencies. An umbrella solution for multiple clouds can provide some solutions, but the overall complexity becomes a new challenge.

A multi-cloud strategy involves two or more cloud computing platforms or providers. Some experts would only talk about multi-cloud when an organisation uses functionally identical services from different providers — as opposed to a strategy in which an organisation cherry-picks from each provider.

Most studies/experts point to the following challenges:

- Centralised identity and access management across the lifecycle
- Compliance
- Lack of visibility and control (E2E)
- Privacy
- Increased complexity
- Knowledge and skills gap
- Inconsistent logging and monitoring capabilities
- Security in the supply chain
- Shift in responsibility for security

How will the challenge evolve?

Centralised Identity and Access Lifecycle Management will become even more important as the need for data security and compliance continues to steadily increase. The issue of "end-to-end visibility" must be clarified for the preparation of Incident Detection & Response.

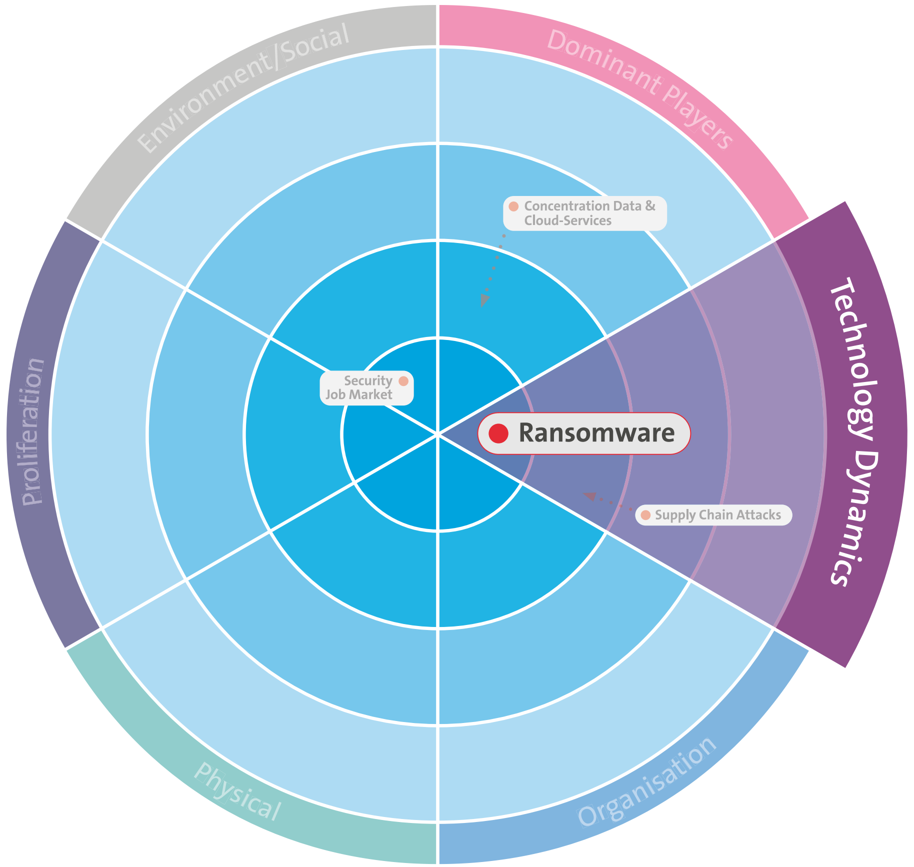
How can we deal with the challenge effectively?

- Early-stage thinking towards multi-cloud
- An overall architecture that facilitates the move from cloud to multi-cloud
- Deploying a system to check security posture and compliance across all clouds
- Monitoring cloud infrastructures globally and creating a central overview of all security-related events

> *"A multi-cloud environment offers undeniable benefits. However, the resulting complexity must be properly managed in order to control the risks associated with the increase in attack surface."*

Duilio Hochstrasser
Security Specialist, Swisscom (Switzerland) Ltd

Challenges and trends
Ransomware



What's it all about?

Ransomware is malware designed to prevent a user or organisation from accessing their own files. By encrypting these files with ransomware and demanding a ransom payment for the decryption key, cyber attackers put companies in a position where paying the ransom seems like the easiest and cheapest way to regain access to their files. Sometimes, data theft is added to the mix, putting additional pressure on ransomware victims to pay the ransom.

Ransomware has quickly become the most well-known and visible type of malware, costing over $1 billion annually worldwide (Gartner). As ransomware has become a lucrative business option for cyber criminals and attack methods continue to grow in sophistication, the costs caused by the attacks will continue to rise. Until recently, it was mainly large corporations that trembled before attacks with ransomware, but in recent years the problem has also increasingly affected SMEs.

It is not only the direct costs — i.e. if a company actually pays the ransom, averaging around CHF 710,000 for an attack on a small company — that are involved, but also the indirect costs for business losses during the hours/days when the systems are locked. In addition, there are the costs for repairing or restoring the systems plus the damage to the company's image. A poor reputation can put companies in an existential emergency within a very short time. Rebuilding a reputation costs a lot of energy, time and money.

How will the challenge evolve?

The trend will continue unabated. As long as unpatched systems or RAS/VPN connections without multi-factor authentication (MFA) can be reached on the internet and employees keep installing malware such as Quakbot, the risk of a ransomware attack is present. Due to easily executed and often successful phishing/malspam manoeuvres, the evolution of successful ransomware attacks by cyber criminals is not even necessary. In the future, attacks may be increasingly automated or further organised on an "as-a-service" basis. Deepfake technologies and the use of artificial intelligence (AI) will make these attacks even more difficult to identify. In addition, it is becoming apparent that more and more attackers are not only encrypting the data, but also threatening to publish it ("double extortion").

From mid-2023, companies in the EU will have to report ransomware attacks. Therefore, it must be assumed that the number of attacks becoming public will increase massively and that this will create a feeling among the population that the number of attacks has increased. Whether this will have an influence on the actual number of attacks cannot be deduced from this. One thing is clear: ransomware is not "force majeure" and we must certainly expect that cloud services will also be taken into "captivity" by cyber criminals in the future.

We and comparable industries are working flat out to improve the way we deal with ransomware.

How can we deal with the challenge effectively?

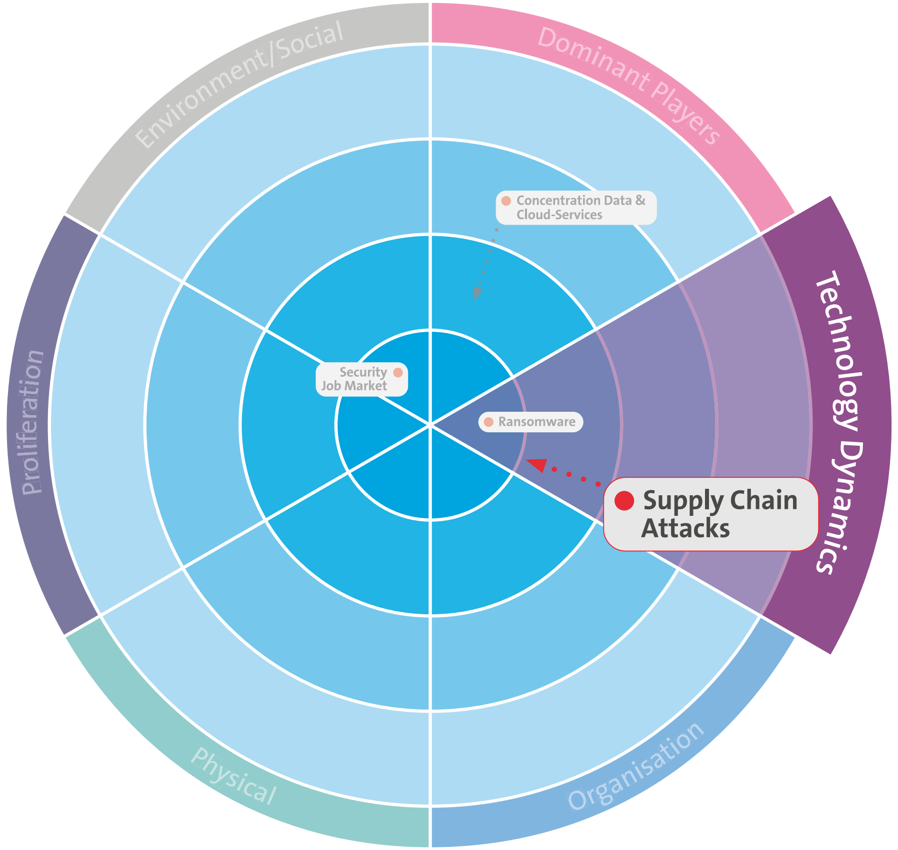
- Ensuring that the management of IT systems and software applications is properly handled throughout the organisation.
- Patching all Internet-facing services in a timely manner (especially if vulnerabilities are already being exploited)
- Making regular (offline) back-ups of systems and data (and testing the recovery of these back-ups)
- Developing a crisis communication plan that takes into account third-party vendors, suppliers, partners, employees and other key stakeholders
- Assessing the organisation's (and IT department's) ability to respond to an attack and to manage potential system outages using response plans
- Ensuring that employees are adequately educated about cyber security and the risk of a ransomware attack
- Protecting RAS/VPN services with multi-factor authentication (MFA)/conditional access
- Investing in EDR and monitoring (e. g. of the Active Directory infrastructure) that is rolled out across the board. In this way, you may still have the chance to recognise and stop an attack in time
- Reducing the attack surface

"Ransomware attackers behave opportunistically. They attack where an opportunity presents itself, i. e. where access is available."

Thomas Röthlisberger
Senior Security Analyst & Tech Lead Red
Team im Swisscom CSIRT

Challenges and trends

Supplier ecosystem and dependencies/supply chain security



What’s it all about?

All organisations need to have a certain level of trust in other companies when they install each other’s software on their networks and collaborate with them. A supply chain attack exploits precisely these trust-based relationships — as well as the loss of control due to dependencies between different organisations.

The attack targets the weakest link in a chain of trust. If an organisation has strong cyber security but works with an insecure provider, the attackers will target that provider. With a foothold in the supplier’s network, the attackers can then move to the more secure network through this trusted relationship. Disruptions at suppliers jeopardise our own service provision, e. g. due to missing advance payments (SLA breach on our side) or by directly endangering us (e. g. by compromising third-party devices in our networks or software).

This is because Managed Service Providers (MSPs) are a common target of attack in the supply chain. MSPs have extensive access to their customers’ networks, which is invaluable to attackers. Once the MSP has been exploited, attackers can easily extend their activities to customer networks. By exploiting vulnerabilities in the supply chain, these attackers have greater leverage and can gain access to networks that would otherwise be much harder to attack. This is how the Kaseya attackers managed to infect so many organisations with ransomware.

Other supply chain attacks are carried out using software that delivers malware to a company’s customers. For example, the Solarwinds attackers gained access to the company’s build servers and inserted a backdoor into updates to the network monitoring product Solarwinds Orion. After this update code was passed on to customers, the attackers also gained access to their networks. Log4J also showed that many companies have an inadequate understanding of the use of libraries and frameworks in solutions. This goes beyond the direct suppliers and includes subsuppliers and sub-subsuppliers.

How will the challenge evolve?

We expect this challenge to increase as a result of greater connectivity with suppliers (remote support; software libraries; SaaS) and targeted attacks to disrupt supply chains. In addition, attackers are now much quicker to exploit the gaps that they discover.

How can we deal with the challenge effectively?

- Focusing on the most important/critical suppliers
- Integration of DevSecOps techniques into the development life cycle
- Data minimisation in exchanges with partners
- Inventorising supplier relationships and assessing their impact
- Continuous monitoring of key suppliers and creation of continuity plans
- Developing alternatives and fallback solutions for key suppliers

> *“Using verifiable ‘Software Bills of Materials’ (SBOMs), the composition of supply items can be checked and verified down to functional levels — even across multiple levels. The same can be done at the hardware level for both custom and standard hardware. It is already available to some extent in certain technologies today.”*
>
> **Oliver Jäschke**
> Security Governance Manager, Swisscom (Switzerland) Ltd

Conclusion

If we thought that a gradual decline in the special pandemic circumstances would bring a little calm, the war in Ukraine has once again revealed the vulnerability of our world. Many things now seem even more fragile and uncontrollable.

Added to this is the increasingly noticeable lack of resources in many IT and security departments. The world is confronted with “wicked problems”, i. e. problems which, due to incomplete, contradictory and changing requirements, are difficult to identify and cannot always be predicted, planned for or mitigated; such problems are therefore usually difficult or impossible to solve.

This all sounds complicated and comes with slightly depressing overtones — but we need not let this discourage us. Digitisation in companies and organisations is making bold advances. The shifting of IT components and IT services to the cloud is on the IT agenda for 2022 in almost all organisations and companies — or it already has been for the last few years. Issues such as Metaverse, Web 3.0, NFTs and Blockchain are shaping current developments in the cyberspace and give cause for hope. This is where we need to stay on the ball, weigh things up and practise active risk management.

We need to put more focus on our own risk management in an increasingly volatile, uncertain, complex and ambiguous world. What do we consider to be worth protecting? Who or what threatens our values and assets in the organisation? What is the role of critical services and components from third parties — suppliers, SaaS providers, cloud services, etc.?

We need to turn employees into allies, demand the much-vaunted role model function from managers, consistently monitor compliance with guidelines and rules, and create alliances across departmental boundaries. In order to be able to counter the constantly changing risks and dangers with the appropriate “defence”, security must be more agile.

> *“The central role in the security system is played by people.”*

Notes

Imprint

Publisher	Swisscom (Switzerland) Ltd, Group Security
Concept / Realisation	Agentur Nordjungs, Zurich
Editorial	Swisscom (Switzerland) Ltd Marcus Beyer (Group Security) Manuel Bühlmann (Group Communications) Claudia Lehmann (B2B Communications)
Translation	Textraplus AG
Copyright	© May 2022 by Swisscom (Switzerland) Ltd, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Print	OK DIGITALDRUCK AG, Zurich
Edition	200 copies

Facing the networked world with confidence

We put the needs of our employees, customers and partners at the heart of all our security considerations. We develop secure solutions, products and services based on state-of-the-art IT and networks.

Are you looking for a job in security at Swisscom? Then take a look here and apply:

swisscom.com/securityjobs

#talkingaboutsecurity

swisscom.ch/security