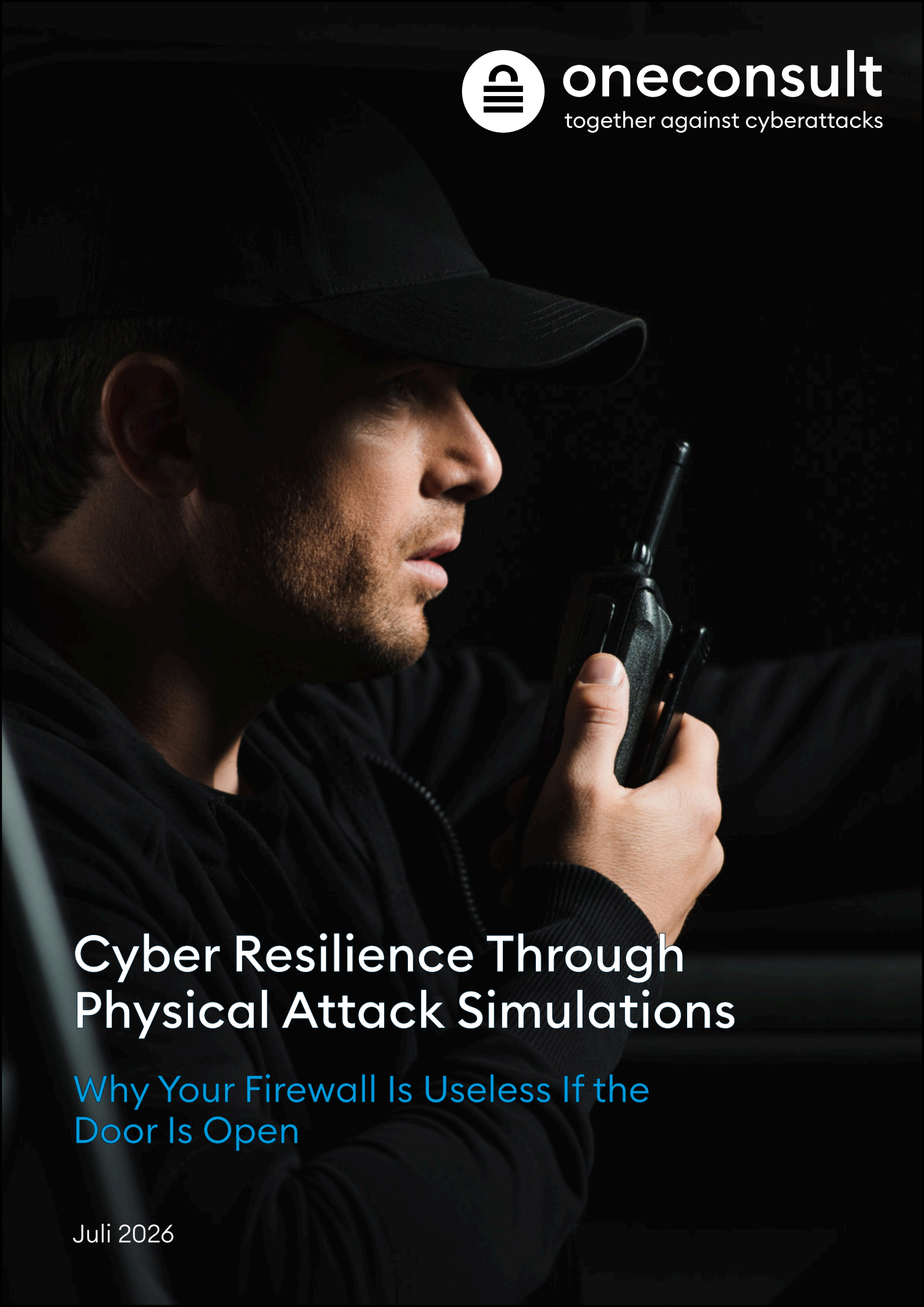
oneconsult
together against cyberattacks



Cyber Resilience Through Physical Attack Simulations

Why Your Firewall Is Useless If the Door Is Open

Juli 2026

Abstract

Physical security vulnerabilities play a significant role in today's threat landscape: According to the IBM Cost of a Data Breach Report 2025, they account for approximately 9 % of all successful attacks. German companies alone suffered losses of around 87 billion euros due to physical attacks, as reported in the Bitkom study "Wirtschaftsschutz 2025". Industrial espionage and sabotage are thus no longer a marginal phenomenon, and the number of unreported cases is likely to be significantly higher.

Foreign intelligence services are increasingly suspected of specifically recruiting organizations and individuals that are becoming increasingly criminal in order to expand their operational reach. At the same time, digital protection measures alone often fall short: The hybridization of threat actors is leading to increasingly professional attacks that unilateral protection strategies can no longer counter.

True security is achieved only through the coordinated interplay of human, constructional-technical, digital, and organizational measures.

This white paper analyzes the current threat landscape in the context of physical risks in the field of information and communication technology (ICT) and highlights the limitations of isolated protection approaches. It explains how physical attack simulations enable a realistic assessment of the security situation, describes their procedure, and defines the prerequisites for a successful implementation.

The white paper is intended for corporate executives responsible for information security. Practical examples and insights from numerous projects carried out by Oneconsult help readers critically assess their own security posture. Specific recommendations outline how physical attack simulations can be successfully integrated into a security strategy.

03 **Directly Accessing the Network by Physical Means**

04 - 07 **Industrial Espionage and Sabotage – A Real Threat**
Risk Situation in Numbers, State Actors and Organized Crime

08 - 13 **Technologically Strong – Systemically Vulnerable**
Human, Constructional-technical, Digital, Organizational

14 - 16 **Attack Simulations as a Solution Strategy**
Procedure and Requirements of a Physical Attack Simulation

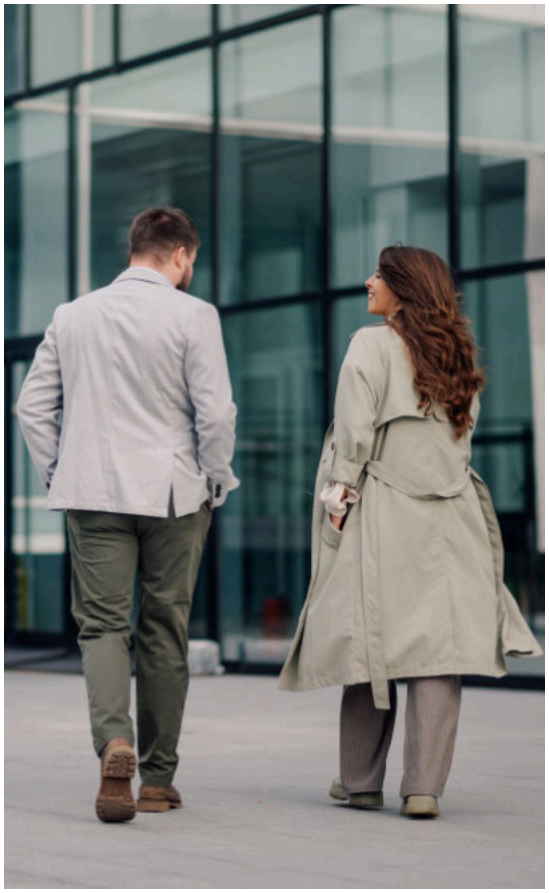
17 - 18 **Findings and Recommendations**

Directly Accessing the Network by Physical Means

It's a typical Tuesday morning. Two people dressed in business suites are standing outside the back entrance of a large company, a cup of coffee in hand, engaged in a lively conversation. Both are clearly wearing employee badges – chip-less imitations created based on a YouTube video. When the building supervisor leaves the building, he is greeted warmly, holds the door open, and lets the supposed employees in..

Through unsecured interior doors, the attackers reach an unoccupied workstation. They connect a prepared rogue device – a manipulated gadget, barely larger than a USB flash drive – between the network and the computer. The device bypasses security measures using a NAC bypass and establishes an encrypted tunnel to the outside. From that moment on, remote access to the internal network is established – without bypassing the firewall, without an exploit, without triggering an alarm. After 13 minutes, the attackers exit the building without leaving a single trace.

The attackers' cost: a few hundred Swiss francs. The potential damage: access to all internal systems, customer data, research and development documents, confidential email communications – and millions in damages.



This scenario is not fictional. It is based on real-world experiences from physical penetration tests and highlights a reality that many organizations underestimate: While investments in technical cybersecurity are on the rise, physical and human attack vectors are often neglected.

Attackers do not think in silos. They seek the path of least resistance – and that path leads not only through a firewall, but also through the door. According to the IBM Cost of a Data Breach Report 2025, physical security deficiencies are already responsible for a good 9 % of all successful attacks.[1] As ICT systems become increasingly hardened, social engineering attacks – particularly those involving physical access – are likely to increase even further in the future.

This white paper analyzes why physical attacks pose a real and increasingly professional threat, which vulnerabilities make organizations particularly susceptible, and how physical attack simulations, so-called physical penetration tests, can help strengthen cyber resilience.

Industrial Espionage and Sabotage – A Real Threat

Industrial espionage and sabotage are no abstract risks, but a real and cross-industry problem – even though many organizations still do not treat them as a priority business risk. Particular focus is placed on companies in the DACH region with valuable intellectual property, advanced manufacturing processes, and strategically relevant research. As home to leading companies in sectors such as pharmaceuticals and chemicals, mechanical and plant engineering, finance and insurance, and semiconductor technology, companies in the DACH region are an attractive target.

This chapter highlights the current risk landscape, explains why the dangers are systematically underestimated, and discusses why companies would be well advised to protect themselves against physical attack vectors as well.

Risk Situation in Numbers

The annual Bitkom study "Wirtschaftsschutz" provides the most comprehensive overview of the threat landscape facing the German economy. Even though physical attack vectors lagged behind digital ones in 2025, the survey results are striking:

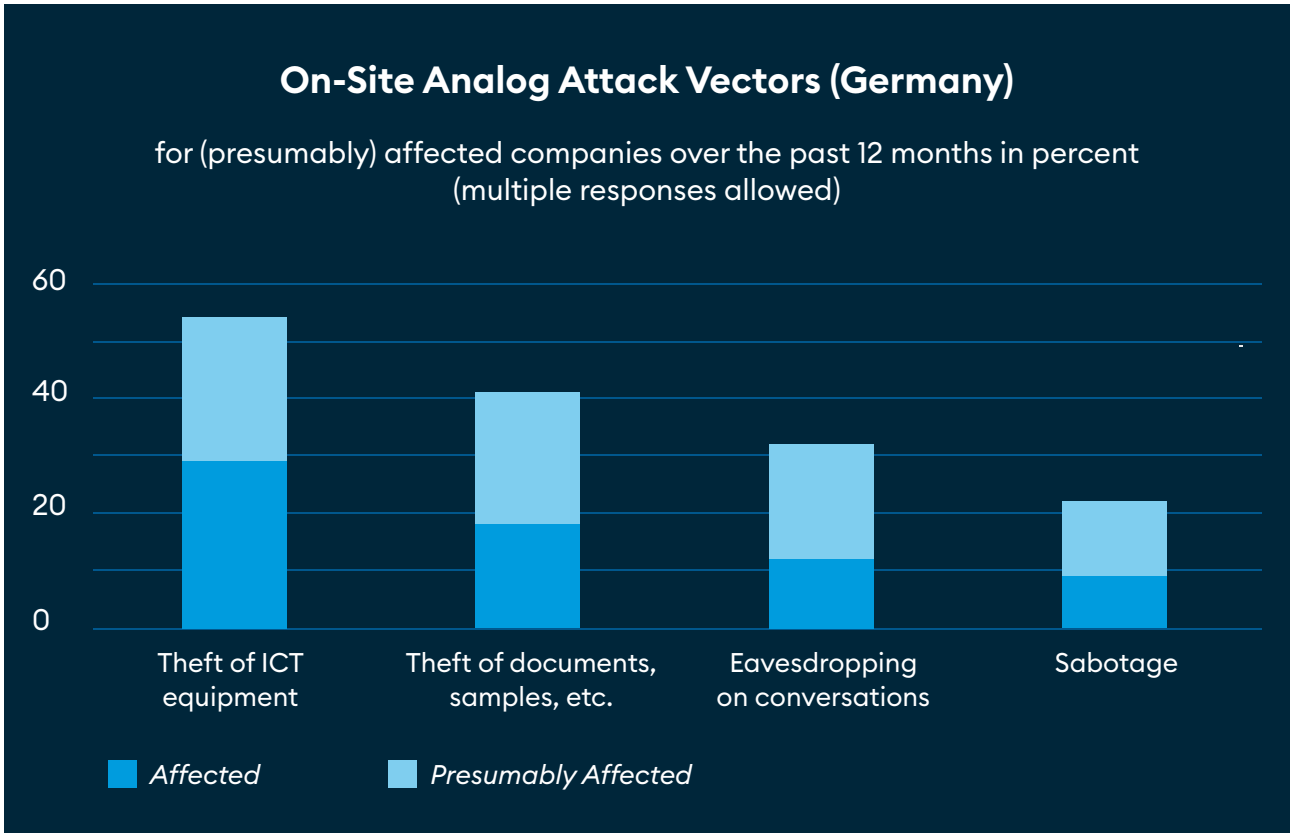


Table 1: On-Site Analog Attack Vectors (Source: Bitkom Study "Wirtschaftsschutz 2025", p. 11)



The motive for the theft of information and communication technology (ICT) equipment is not entirely clear. It is reasonable to assume that resale is the primary motive in many cases. The impact on information security can usually be limited – provided the thefts are detected in time.

The other three categories, however, are driven by industrial espionage or sabotage, which can no longer be considered a marginal phenomenon.

In addition, nearly one in two companies reported having been affected in the past twelve months by social engineering attacks (some of which were carried out remotely) as a prelude to data theft, industrial espionage, or sabotage.[2]

The total cost of all attacks rose to 289.2 billion euros – another all-time high. While 202.4 billion euros of this amount is attributable to cyberattacks, around 87 billion euros result from analog attacks, including physical theft and on-site sabotage.[3] This also covers damage that is difficult to quantify, such as reputational damage, lost revenue due to lost competitive advantages, and lost orders, etc.

Lack of Statistics Does Not Mean Lack of Risk

A key challenge in assessing the scale of physical attacks is the lack of available data, as few countries maintain relevant public statistics. The Bitkom study is an exception in this regard. Switzerland serves as a prime example: Since April 1, 2025, there has been a mandatory reporting requirement for cyberattacks on critical infrastructure. Physical on-site attacks, however, are not recorded.

Organizations are reluctant to voluntarily disclose analog security incidents – without anonymizing them – for reasons such as reputational concerns. The data used in studies and statistics therefore comes primarily from surveys, however, caution is advised when interpreting the results, as they are based on self-reported information and the subjective perceptions of the respondents.

Furthermore, an attack must first be detected in order to be statistically recorded. This is particularly difficult when there is a significant geographical, temporal, or thematic distance between the attack and its impact. For example, if an identical product is launched in China, it is often difficult to clearly trace or unequivocally attribute the underlying leak of design plans.

This is further complicated by the difficulty of distinguishing between cyber incidents and physical incidents, especially when multiple attack vectors are used in combination. A typical example is a password written on a sticky note under the keyboard: This can be spied on during physical access at an unobserved moment, while the actual system access occurs remotely. In practice, the incident is often classified as a cyber incident, even though the underlying vulnerability was of a physical nature.

Consequently, it can be assumed that the number of physical attacks is significantly underestimated in studies. Decision-makers would therefore be well advised not to allow this statistical underrepresentation to mislead them into underestimating the risk of physical attacks.

State Actors and Organized Crime

Even though civil society activists act creatively, they generally lack both the resources and the expertise required to carry out complex attacks on ICT infrastructures that combine on-site and cyber operations. Furthermore, they usually aim for isolated disruptions rather than long-term espionage campaigns. While this group of attackers is not irrelevant, the focus of this white paper is on actors capable of persisting undetected in ICT systems over extended periods and exfiltrating sensitive information.

These include, in particular, state actors that have substantial financial and human resources, are highly organized, and can also employ technical means that are not available to the private sector. Citizens, and in particular diplomatic personnel, of states known for their extensive espionage and sabotage activities[4] are now screened for security risks.[5/6] The shrinking of the network of agents in Western countries is making it increasingly difficult for intelligence agencies to operate on the ground. In order to compensate, they are relying more heavily – and on an entirely new scale – on existing organized crime networks.[7] In addition, there is an increasing use of so-called "disposable agents" – private individuals who are often recruited via social media and deployed for specific operations on the ground, but who are difficult to definitively link to state actors.[8]

The growing convergence is striking: State actors are using criminal groups and private individuals as tools, while these groups are thereby achieving a level of professionalism that was once the exclusive domain of state actors. This hybridization of attacker groups significantly increases the complexity of the threat landscape.

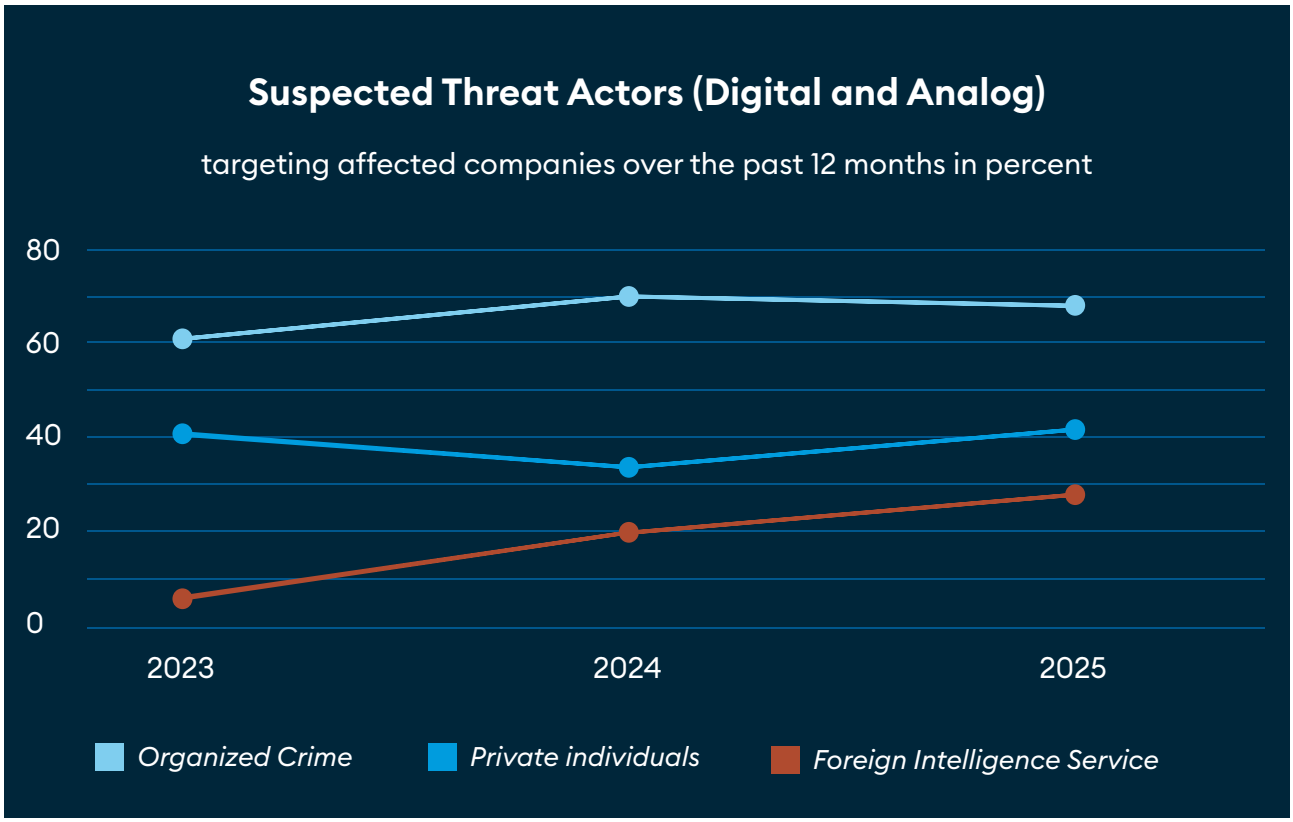


Table 2: Threat Actors (Source: Bitkom Study "Wirtschaftsschutz 2025", p. 13)

The Bitkom study identifies these three groups as the most frequently suspected perpetrators of attacks (both digital and analog). Of particular interest is the increase in suspected attacks by foreign intelligence services. For the sake of transparency, it should be noted that this reflects the perceptions of the companies involved.

The motives behind the attacks are also intriguing. According to the Verizon 2025 Data Breach Investigations Report – which, however, focuses solely on remote social engineering – espionage was the objective in roughly half of the cases.

Conclusion on the Threat Situation

The risks of industrial espionage and sabotage for companies in the DACH region are very real. Practical difficulties in assessing security incidents mean that the actual threat situation is likely to be significantly underestimated. This is particularly true for analog attacks carried out on-site, which are much more difficult to detect and trace than pure cyberattacks. Due to increasing hybridization, the potential for various threat actors to carry out highly professional attacks is growing. Because many companies have now significantly expanded their cyber defenses, it is likely that attackers will increasingly rely on on-site physical vectors and social engineering in the future – as part of a complex attack chain.

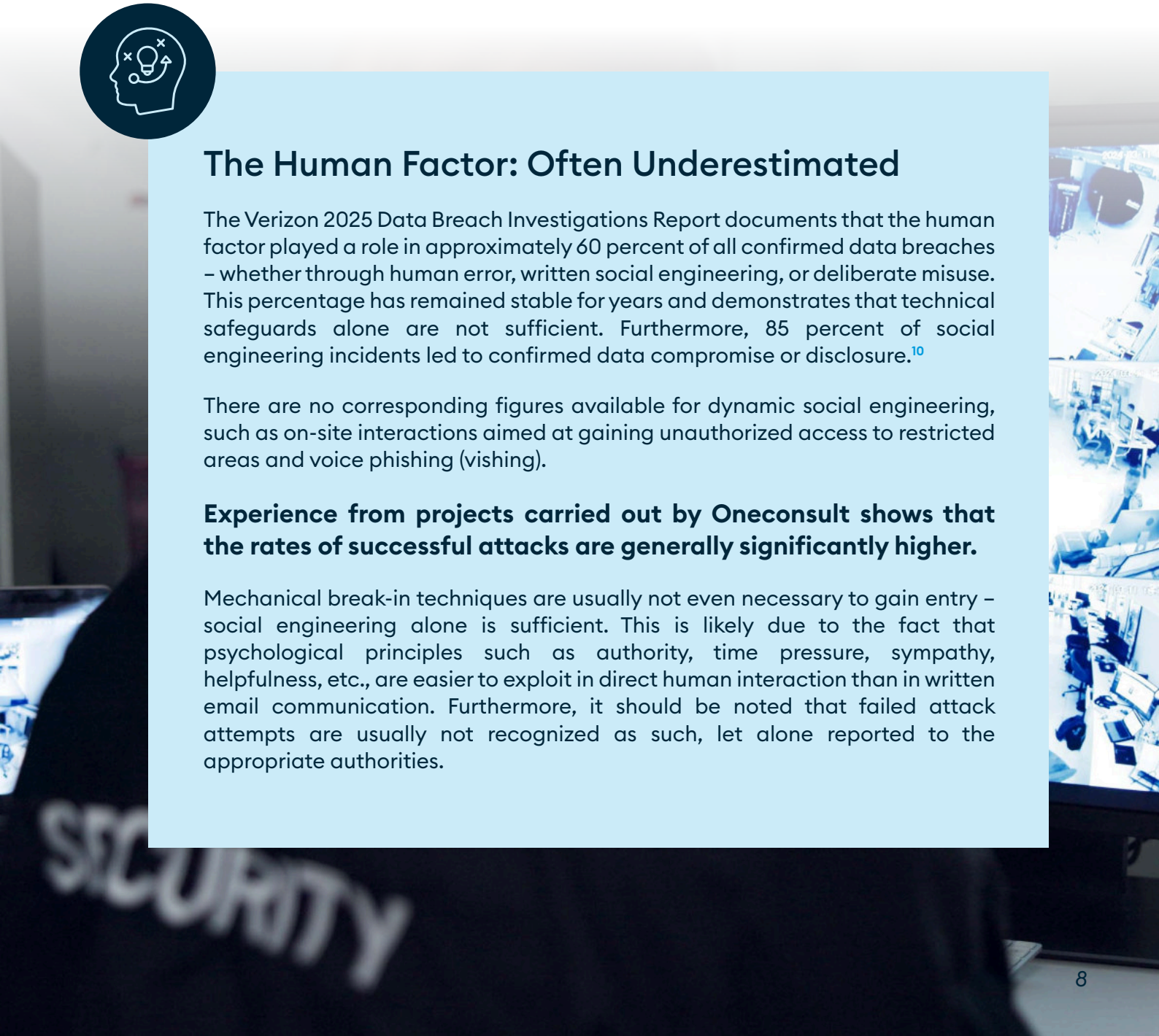
"State actors are increasingly leveraging criminal groups to conduct attacks, significantly escalating the threat landscape."



Technologically Strong – Systemically Vulnerable

Investment in cybersecurity has reached a significant level in recent years. Many organizations use sophisticated perimeter protection, powerful SIEM systems, multi-factor authentication, and regular vulnerability scans. These measures are essential – but they primarily address remote technical attack vectors.

The following section highlights key protective and risk factors related to on-site (ICT) security. It also outlines typical vulnerabilities that Oneconsult has frequently encountered in the course of projects. This information should not be considered exhaustive.



The Human Factor: Often Underestimated

The Verizon 2025 Data Breach Investigations Report documents that the human factor played a role in approximately 60 percent of all confirmed data breaches – whether through human error, written social engineering, or deliberate misuse. This percentage has remained stable for years and demonstrates that technical safeguards alone are not sufficient. Furthermore, 85 percent of social engineering incidents led to confirmed data compromise or disclosure.[10]

There are no corresponding figures available for dynamic social engineering, such as on-site interactions aimed at gaining unauthorized access to restricted areas and voice phishing (vishing).

Experience from projects carried out by Oneconsult shows that the rates of successful attacks are generally significantly higher.

Mechanical break-in techniques are usually not even necessary to gain entry – social engineering alone is sufficient. This is likely due to the fact that psychological principles such as authority, time pressure, sympathy, helpfulness, etc., are easier to exploit in direct human interaction than in written email communication. Furthermore, it should be noted that failed attack attempts are usually not recognized as such, let alone reported to the appropriate authorities.

The Constructional-Technical Factor: Often Overestimated

While organizations invest significant resources in digital security solutions, physical security systems often remain at a level that was outdated a decade or more ago. Although access control systems are implemented, they are not reviewed until the end of their lifecycle. In the meantime, attack techniques continue to evolve, meaning that such systems can potentially be bypassed – for example, by cloning outdated access credentials.

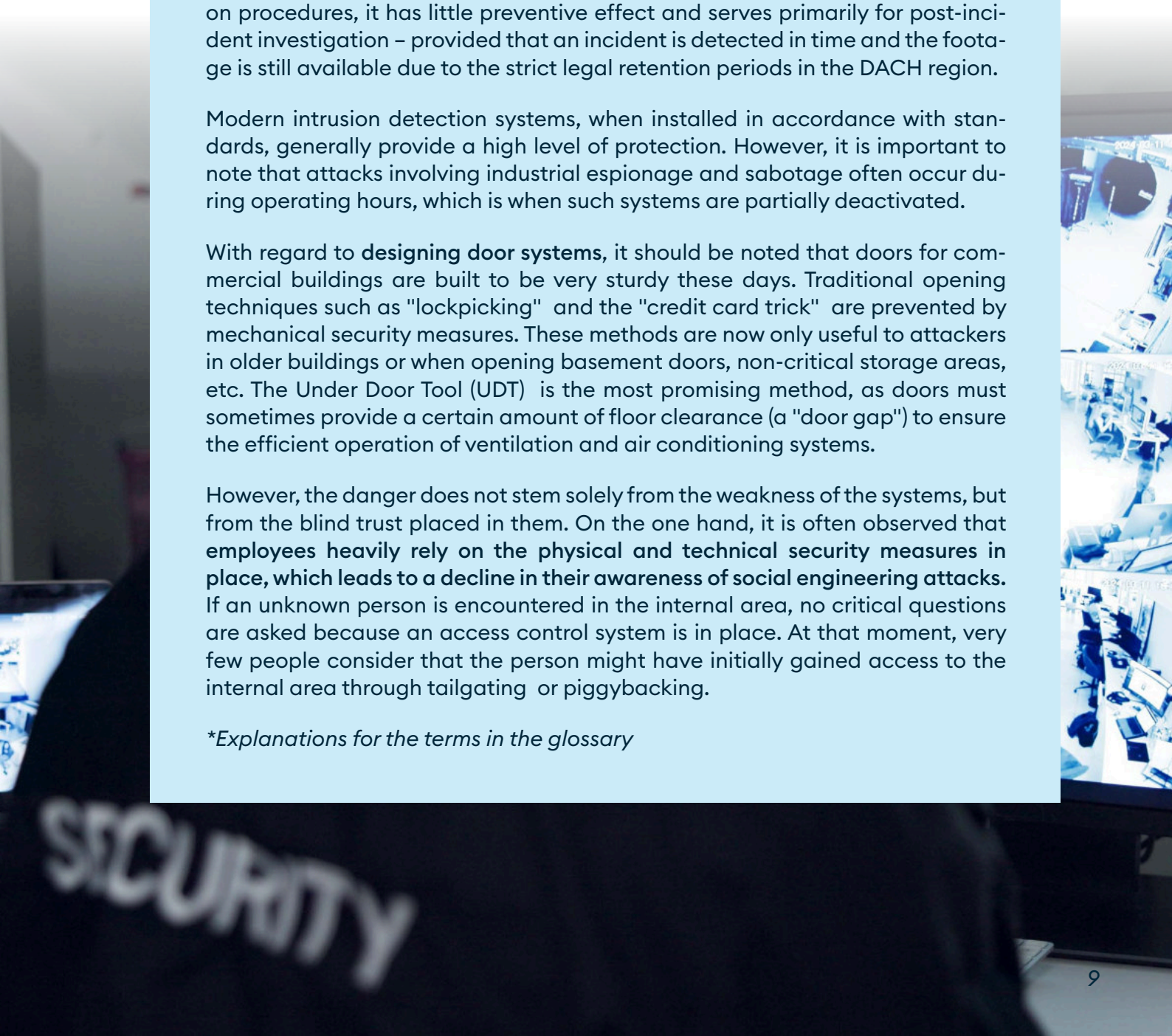
The benefits of video surveillance are often overestimated. While it can act as a warning to opportunistic offenders, this effect is very limited when it comes to professional criminal groups. Without active monitoring and defined intervention procedures, it has little preventive effect and serves primarily for post-incident investigation – provided that an incident is detected in time and the footage is still available due to the strict legal retention periods in the DACH region.

Modern intrusion detection systems, when installed in accordance with standards, generally provide a high level of protection. However, it is important to note that attacks involving industrial espionage and sabotage often occur during operating hours, which is when such systems are partially deactivated.

With regard to **designing door systems**, it should be noted that doors for commercial buildings are built to be very sturdy these days. Traditional opening techniques such as "lockpicking" and the "credit card trick" are prevented by mechanical security measures. These methods are now only useful to attackers in older buildings or when opening basement doors, non-critical storage areas, etc. The Under Door Tool (UDT) is the most promising method, as doors must sometimes provide a certain amount of floor clearance (a "door gap") to ensure the efficient operation of ventilation and air conditioning systems.

However, the danger does not stem solely from the weakness of the systems, but from the blind trust placed in them. On the one hand, it is often observed that **employees heavily rely on the physical and technical security measures in place, which leads to a decline in their awareness of social engineering attacks.** If an unknown person is encountered in the internal area, no critical questions are asked because an access control system is in place. At that moment, very few people consider that the person might have initially gained access to the internal area through tailgating or piggybacking.

**Explanations for the terms in the glossary*



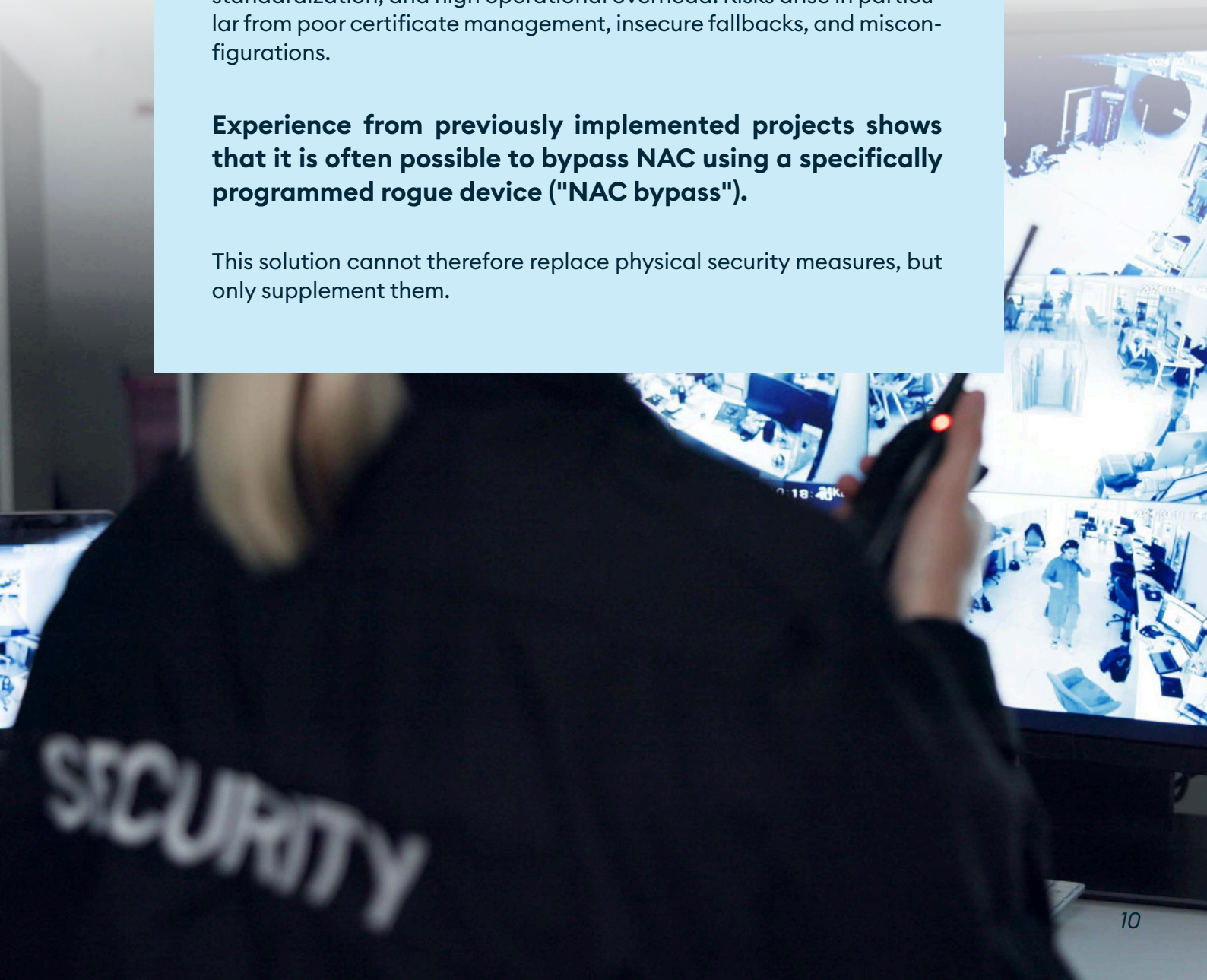
The Digital Factor: Often Uncertain

Network Access Control (NAC) regulates access to corporate networks based on identity, device, and security policies. In practice, this is usually based on 802.1X with certificate-based authentication, supplemented by fallback mechanisms such as MAC Authentication Bypass (MAB).

Implementing NAC is challenging because heterogeneous systems, mobile work environments, and complex policies make deployment difficult. Common constraints include legacy infrastructure, a lack of standardization, and high operational overhead. Risks arise in particular from poor certificate management, insecure fallbacks, and misconfigurations.

Experience from previously implemented projects shows that it is often possible to bypass NAC using a specifically programmed rogue device ("NAC bypass").

This solution cannot therefore replace physical security measures, but only supplement them.



The Organizational Factor: Often Overlooked

The aforementioned protective measures – human, constructional-technical, and digital – are often considered in isolation. This is partly because responsibilities within companies are frequently divided among different individuals. Furthermore, the necessary expertise is not always available in all areas when all areas of expertise are assigned to a single person.

A typical example is the shortcomings in zone and access control concepts. A zone plan does not automatically correspond to a physical access control concept: Areas that are uniformly classified in the zone concept are often made accessible to all employees in that zone without additional physical barriers. Once attackers have gained entry, they can move largely unhindered within the internal area. Internal risks, such as those posed by a "malicious insider", are also reinforced by this, as employees gain access to areas that are not necessary for their work. In practice, badge authorizations are often assigned hierarchically rather than on a "need-to-go" basis, which means that even administrative roles gain access to critical infrastructure areas such as the power supply without any operational necessity.

Visitor management also regularly reveals weaknesses. The departments involved are often not sufficiently informed, making social control virtually impossible. In some cases, only entry times are recorded, while exits are not documented. Inadequate handoffs during shift changes and paper-based logs also make it difficult to keep track of people in the building. These gaps not only impair operational security controls but can also have safety-critical consequences in the event of a fire or during evacuations.

Even when security and surveillance systems, such as video surveillance, are in place, there is often no clearly defined response protocol. Staff reserves for exceptional situations are rarely available. If security personnel must respond to an incident, the monitored area remains unguarded during that time. This creates an opportunity for unauthorized entry through distraction tactics.

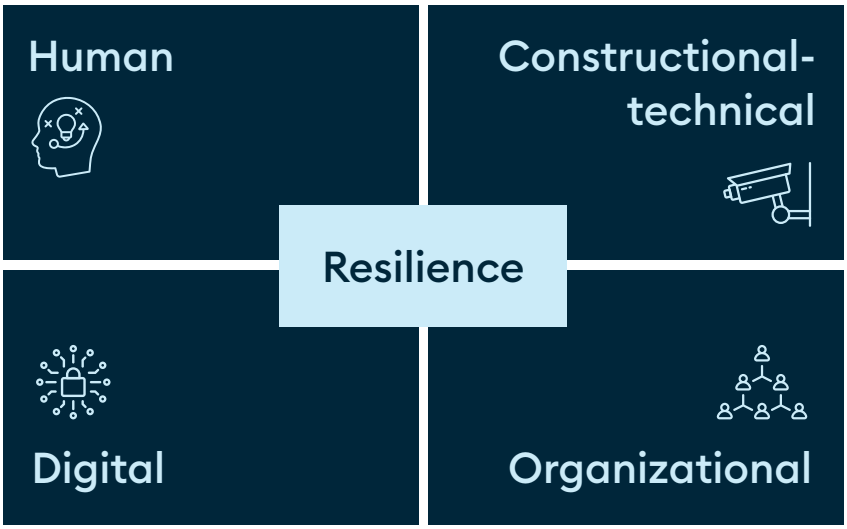
Finally, it should be noted that organizational and technical security measures are subject to constant change: construction specifications are updated, rooms are repurposed, and security systems are replaced. Without regular reviews, this can lead to undetected security vulnerabilities. In practice, however, existing security concepts are often updated only as part of major overhauls. Continuous review and updating are therefore crucial to ensuring the long-term effectiveness of the security architecture.



Conclusion on the Protective Factors

When taken individually, protective factors have only a limited effect. Security is achieved only when measures are harmonized. Since every security measure may have weaknesses or vulnerabilities, a multi-layered, redundant implementation is essential. Otherwise, attackers can find a path to the critical target area by exploiting individual vulnerabilities. In such cases, the failure of a single security measure can compromise the effectiveness of the entire security concept.

Organizational measures and employees' adherence to security practices in their day-to-day work are particularly crucial. Extensive investments in technical and construction-related security measures have only limited impact if awareness and organizational processes are not taken into account. Companies should therefore allocate their financial resources in a balanced manner to ensure an effective and sustainable security architecture.



To ensure the effectiveness of these protective measures in combination, they should be tested not only individually but also in combination. Physical penetration tests offer a practical approach to this, as they verify the interaction of all measures under realistic conditions. Since security architectures are constantly evolving, such tests cannot be considered a one-time measure. Instead, they should be conducted regularly and following significant changes to ensure a reliable picture of the current security level.

10 Common Vulnerabilities in Businesses

Common areas near entrances	Common areas (e.g., smoking areas) are often located in the immediate vicinity of exterior doors. This allows attackers to appear legitimate while lingering there and to deliberately attempt tailgating.
Underground garage accessible on foot	If vehicle access is controlled, employees often perceive the area as an internal zone. Unauthorized persons are therefore rarely questioned and are sometimes granted access to the building.
Burglar alarm system on the ground floor only	If upper floors are not secured, attackers can enter the building unnoticed through windows or alternative access points (e.g., using ladders).
Insufficient video surveillance image quality	If the image quality is insufficient, this can make it impossible to identify individuals afterwards. The system's forensic effectiveness is thus severely limited.
Information visible from outside	Sensitive information displayed on screens, whiteboards, or flipcharts can be viewed through the window and captured using technical devices.
Elevator without access control	Even if the elevator can only be operated with a badge, unrestricted access to the cabin allows attackers to enter unhindered. By waiting for a call to their destination, they can thus gain access to internal areas.
Orientation boards and room signage	Orientation boards and room signage make it easier for attackers to navigate the building and enable a targeted approach. Internal employees usually do not rely on this information.
Unlocked basement rooms	Rarely used rooms can serve as hideouts or waiting areas. Attackers can hide there and move around the building undisturbed outside of business hours.
Central key boxes	Often inadequately secured against forced entry or removal. Once opened, they allow attackers access to a wide range of rooms or containers.
Open document storage areas	Confidential information is freely accessible as soon as attackers are inside the premises. This allows for a direct outflow of information without additional security barriers.

oneconsult
together against cyberattacks

Attack Simulations as a Solution Strategy

Companies that strive for true security – rather than merely meeting compliance requirements – have no choice but to test their security measures comprehensively. After all, attackers do not need many – or even any major – security vulnerabilities; a single attack vector that leads them to the company's crown jewels is enough.

Attack simulations allow attacks on an organization to be realistically recreated under controlled conditions in order to identify vulnerabilities. They combine methods drawn from physical security testing, social engineering, and cybersecurity to obtain the most realistic picture possible of the actual security situation.

In this process, individual attack phases can be evaluated in isolation or as part of an integrated attack cycle, for example:

Gaining physical access to the network through a **physical access assessment**

Obtaining credentials for initial access to the IT infrastructure through **vishing**

Compromising critical corporate data and systems through **technical red teaming**

Procedure of a Physical Attack Simulation

A professional physical attack simulation follows a structured process modeled after the methods used by real attackers:



The four main operational phases are explained in more detail below.



Open Source Intelligence (OSINT) refers to the systematic collection, evaluation, and analysis of freely available information from public sources to derive actionable insights. This involves, for example, reviewing a company's official web presence as well as the private profiles of key employees for useful information. In particular, corporate videos, publicly accessible video content, and job postings often allow conclusions to be drawn about the building structure, the security technology used, and operational procedures. Furthermore, tenders are a valuable source, as they frequently contain references to the systems in use. The individual pieces of information are usually inconsequential on their own and only reveal their security-relevant potential when considered as a whole.

Public mentions of the company by third parties, such as suppliers and service providers, should not be underestimated either, as they often allow for a relatively accurate mapping of the network of business relationships. In the context of projects, this primarily serves to create a pretext . Real-world attackers use this knowledge about third parties for supply chain attacks in order to gain access to the target company's system through indirect channels or to cause damage to it. For instance, 41 percent of affected German companies report tangible consequences – such as delivery failures or reputational damage – when a supplier has been affected by data theft, industrial espionage, or sabotage.[11]

OSINT offers attackers the advantage of efficient and secure remote research. For opportunistic and primarily financially motivated actors, the identified attack surface is a key factor in determining which company to target in the first place. Therefore, the careful handling of publicly available information is an important preventive measure for a company.



On-site reconnaissance, together with OSINT research, forms the basis for the operational planning of an effective social engineering campaign. It serves to gather information about current local conditions as well as the actual workflows of employees.

Professional attackers sometimes go a step further: They observe key individuals over an extended period of time, even in their private lives. This allows them to create detailed personal and personality profiles. Using this information, they can, for example, guess passwords more accurately, blackmail individuals, or prepare for covert contact.[12]



Real-world attacks are often complex and multi-stage. **Advance actions** provide the groundwork for a successful intrusion into the company. For example, vishing calls to the reception desk can be used to obtain the code for the front door under a pretext or to gather information about the exact delivery process for goods through clever, inconspicuous questions.



After several weeks of preparation, the actual physical entry takes place on-site. This **physical penetration test** includes the phases of infiltration, lateral movement, and exfiltration. As mentioned earlier, the time spent inside the building can be extremely short – sometimes just a few minutes – if the operation is well-planned and the circumstances are favorable.

Using various social engineering and technical methods, access routes to internal areas are tested by exploiting a combination of vulnerabilities in employee behavior, operational processes, and structural and technical security measures. Once the mission objectives (flags) agreed upon with the client have been achieved, covert exfiltration typically follows. Alternatively, the response of the defense team can be deliberately provoked to test intervention and escalation processes.

Requirements for a Good Attack Simulation

Physical attack simulations provide insights that cannot be obtained through any other type of evaluation: a realistic assessment of the actual security situation under conditions that closely resemble a real attack. They make it possible to identify vulnerabilities before real attackers do and form the basis for targeted and prioritized improvement measures.

The value of such tests is high, but they require significant planning and resources. Structured preparation is therefore crucial to ensure the effectiveness of the simulation and maximize the benefits of the results.

Findings and Recommendations

The findings presented in this white paper lead to a clear conclusion: Physical attacks are real, measurable, and increasingly sophisticated. They exploit a combination of human, construction-technical, digital, and organizational vulnerabilities. Organizations that base their security strategy exclusively on digital measures systematically overlook a significant portion of the actual threat landscape.

Security is systemic: Every company is both a service recipient and a service provider. Weaknesses within an organization can have ripple effects on other stakeholders throughout the value chain.

Lack of operational ICT resilience is not merely a cyber issue: The threat landscape encompasses digital, human, and physical dimensions, all of which must be given equal consideration.

Attackers think in a hybrid manner: Modern attackers combine methods from various domains. A defense strategy organized in silos cannot effectively counter this approach.

True security maturity is only revealed through comprehensive testing: Isolated tests of individual security measures provide only limited insight into actual resilience. Only through holistic attack simulations does it become clear how effectively the security measures work together.

Physical attack simulations address specific gaps in reality: They particularly reveal vulnerabilities arising from human behavior, constructional-technical conditions, and organizational processes, thereby providing an indispensable foundation for targeted improvement measures.



Specific Recommendations for Action

Evaluating threat actors: Assess which attacker groups are relevant to you, what capabilities they possess, and how they typically operate. If necessary, have a threat intelligence report prepared.

Checking protective measures for relevance to your ICT: Systematically evaluate how physical and human vulnerabilities impact your information security. Address these with the same priority as cyber threats.

Conducting attack simulations: Test the effectiveness of protective measures in combination to identify real vulnerabilities. Repeat such assessments regularly.

Meeting compliance requirements: Several regulators also require regular physical security audits. These include the ISO 2700x standard, the NIS 2 Directive, and DORA for the EU financial sector and its ICT service providers.

oneconsult
together against cyberattacks

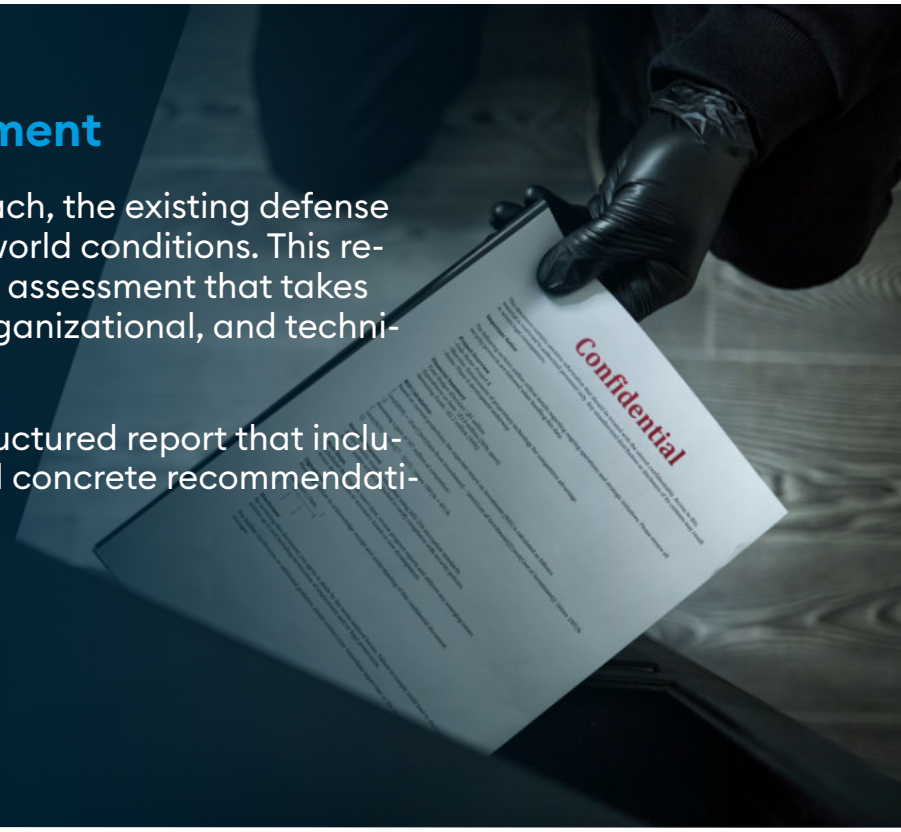
Protect Your Organisation

A realistic assessment of the security posture requires the identification of remaining vulnerabilities before they are exploited by real attackers. Attack simulations help systematically test resilience under realistic conditions.

Physical Access Assessment

Using a black-box testing approach, the existing defense posture is evaluated under real-world conditions. This results in a comprehensive security assessment that takes into account various physical, organizational, and technical attack vectors.

The results are presented in a structured report that includes prioritized vulnerabilities and concrete recommendations for action.



› Learn more now

We would be happy to assist you in assessing your current security situation and planning appropriate testing approaches.

Our subject matter experts are available for a confidential, no-obligation consultation.



Antonio Rainelli

Senior Client Services Manager

antonio.rainelli@oneconsult.com
T +41 43 377 22 52
M +41 79 630 36 78
Book appointment: calendly.com/antonio-rainelli

Glossary

Card Trick	Simple doors can be opened by pushing back the latch with a flexible card.
Lockpicking	Lockpicking refers to the manipulation of a lock cylinder or the opening of a door using special tools.
Piggybacking	In piggybacking, an unauthorized person is deliberately allowed entry by an authorized person, for example, by claiming to have forgotten their badge.
Pretexting	Pretexting is a social engineering technique in which attackers fabricate a plausible story ("pretext") to gain a target's trust and persuade them to disclose sensitive information or perform specific actions.
Supply Chain Attack	In a supply chain attack, attackers specifically exploit vulnerabilities in a company's supply chain – such as in software, hardware, service providers, or third-party vendors – to gain indirect access to a target system.
Tailgating	Tailgating refers to the act of discreetly following an authorized person through a secured door.
Under Door Tool (UDT)	The UDT is a tool for operating door handles from the outside. It is inserted through the gap between the door and the floor.

Bibliography

1. **SPAC Alliance.** (September 2025). IBM Cost of a Data Breach Report 2025 – Analyse, S. 17.

2. **Bitkom/Bundesamt für Verfassungsschutz.** (September 2025). Wirtschaftsschutz 2025, S. 24. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschafts-schutz-2025_2.pdf

3. **Bitkom/Bundesamt für Verfassungsschutz.** (September 2025). Wirtschaftsschutz 2025, S. 19. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschafts-schutz-2025_2.pdf

4. **Bitkom/Bundesamt für Verfassungsschutz.** (September 2025). Wirtschaftsschutz 2025, S. 16. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschafts-schutz-2025_2.pdf

5. **Tagesanzeiger.** (Oktober 2025). ETH hat 80 Bewerber aus dem Ausland abgewiesen. https://www.tagesschau.de

6. **Tagesschau.** (April 2024). Geheimprojekt "Harmonie". https://www.tagesschau.de/investigativ/ndr-wdr/spionage-technik-russland-deutschland-100.html

7. **Brombacher & Vorrath.** (Juli 2025). Die Transformation transnationaler organisierter Kriminalität - Neue Risiken verlangen neue Antworten von Europa, S. 4. SWP-Aktuell, Nr. 37. https://www.swp-berlin.org/publications/products/aktuell/2025A37_transnationale_organisierte_kriminalitaet.pdf

8. **Norddeutscher Rundfunk NDR.** (Oktober 2025). Verfassungsschutz: So wirbt der russische Geheimdienst Agenten an. https://www.ndr.de/nachrichten/niedersachsen/verfassungsschutz-so-wirbt-der-russische-geheimdienst-in-deutschland-agenten-an,verfassungsschutz-176.html

9. **Verizon.** (2025). Data Breach Investigations Report (DBIR), S. 46. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

10. **Verizon.** (2025). Data Breach Investigations Report (DBIR), S. 20. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

11. **Bitkom/Bundesamt für Verfassungsschutz.** (September 2025). Wirtschaftsschutz 2025, S. 15. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschafts-schutz-2025_2.pdf

12. **Nachrichtendienst des Bundes.** (Mai 2016). "Im Visier" – Wirtschaftsspionage in der Schweiz. https://www.youtube.com/watch?v=ad6td7NNsAc&list=PLAorZm3BkjdC6qDb-4Pr6vlXpO6E79jJt&index=6

Additional Resources

Blog Posts

- Enhancing Cyber Resilience Through Attack Simulations According to DORA and TIBER
- Social Engineering – Introduction and Techniques (Part 1)
- Social Engineering – Risks and Prevention for Businesses (Part 2)

Webinar (in German)

- Inside the Mind of a Social Engineer

Podcast (in German)

- Der Mensch als Schwachstelle (Cyberfunk)