Baobab
Risk Solutions

Data Breach Report

The Mid-Market: A Target of Opportunity

Introduction

As an MGA specializing in digital risks, Baobab continuously evaluates both dimensions of cyber risk: the technical vulnerability prior to an attack and the financial damage thereafter. Our data analysis reveals a significant rift in the security landscape.

While large corporations are increasingly locking their digital doors, they often remain wide open across the mid-market. However, our data also offers hope: the majority of attacks are not highly complex, but opportunistic. This means that companies are not helpless in the face of these risks; with the right measures, the danger can be drastically reduced.

Our findings are based on the continuous analysis of deep scans and quoting data from our application processes. While this dataset does not claim total statistical representativeness for the entire market, the sheer volume of cases examined and our long-term observations reveal clear, actionable trends.

Table of Content

Data Basis

>10,000 of attack surface scans evaluated.

57,660 leaked credentials analyzed from 5,000 different sources.

Hundreds of real-world claims categorized.

Hundreds of external ransomware cases investigated.

Summary

88,7% of leaked data is recurrent

Hackers don't need to reinvent the wheel. The majority of credentials found on the dark web originate from historical breaches. Once an individual falls into the net of info-stealers, they remain a marked target for years, as data is systematically repackaged and deployed against networks via automation.

Passwords are insufficient as a defensive wall

Password complexity is secondary when credentials are for sale in plaintext within databases. Our analysis shows that without multi-factor authentication (MFA), initial access remains trivial. Attackers don’t break in; they simply log in using valid, cheaply acquired credentials.

The 75% Rule: Danger Is Concentrated, Not Spread

External pressure is overwhelmingly centered on the network edge (VPNs/firewalls) and collaboration tools (email). These two categories drive three-quarters of the total threat score and almost all "Zero-Day" signals. For businesses, the priority is clear: Secure your internet-exposed layers first, as this is where attacks are most persistent.

Data wealth outweighs revenue size

The fallacy of being "too small to be a target" is life-threatening. Hackers measure attractiveness not by revenue, but by the volume of personally identifiable information (PII). Even among companies with less than €5 million in revenue, 31% manage more than 10,000 records—making them a perfect target for attacks.

Instead of Breaking In, Just Sign Up

It is a common misconception that cybercriminals need to develop highly complex code to bypass firewalls. The reality is much more mundane and economical: Why break in laboriously when you can buy the key for a few euros on the dark web? Compromised identities are the cheapest and most effective weapon in the attackers' arsenal.

The Archive of Horror

Our analysis shows that hackers rarely need to bypass sophisticated encryption. The majority of leaked credentials found on the dark web are available in plaintext—immediately readable and ready to use.

91% of analyzed leaks contain plaintext passwords, making initial access for attackers trivial and cost-effective.

This scale of accessibility has industrialised cybercrime. In one Telegram channel we analyzed, a simple subscription provides buyers with weekly access to at least 5,000 fresh datasets, proving that for attackers, the path of least resistance is often a wide-open door.

Example of a Darknet Offer

Source: Darknet Telegram Channel

Offer

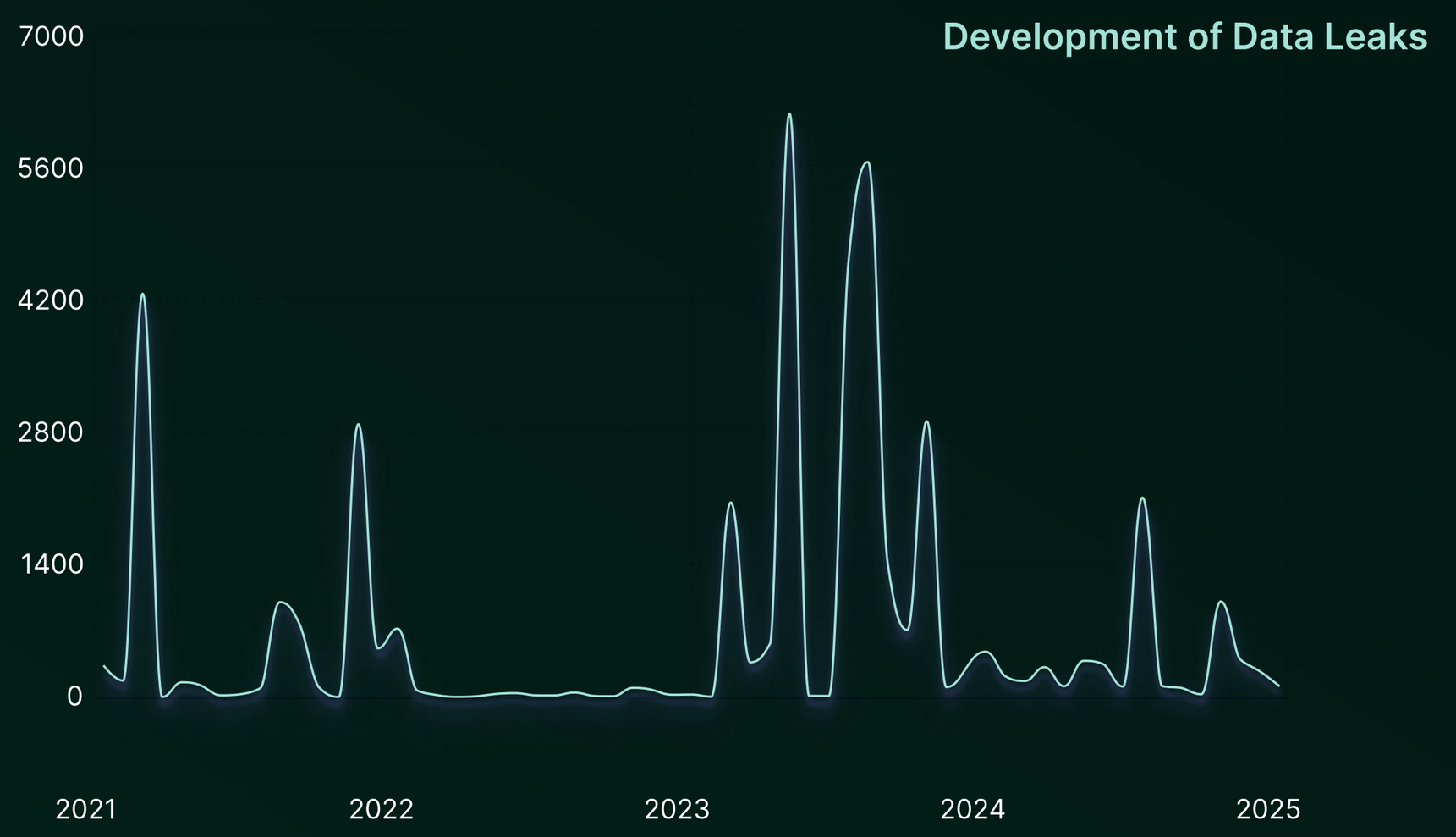
- Access to the exclusive channel
- Daily 5,000 - 15,000 stolen data
- Monthly subscription includes transfer of 45,000 logs

Prices

- One week: $75
- Two weeks: $150
- One month: $250
- Three months: $600

Trend Shift: From Mega Breaches to Info Stealers

While in the past individual breaches at companies like Adobe or LinkedIn dominated the headlines, we are currently seeing a shift towards info stealer logs.



What Are Info Stealers?

Info stealers are a type of malware that secretly embeds themselves on devices such as laptops or mobile phones and extract credentials directly from the browser, password managers, or active sessions (session cookies).

These logs are particularly dangerous as they often contain current passwords, and once leaked data remains in circulation. Our data shows a duplication rate of around 88.7% – this means the same stolen data keeps appearing in various data collections.

Chandan Raj Nivanda
Cyber Security Researcher

"We are observing a significant shift in attack strategy: moving away from singular, massive server hacks towards scaling through thousands of small info stealer infections."

The Severity of the Vulnerability

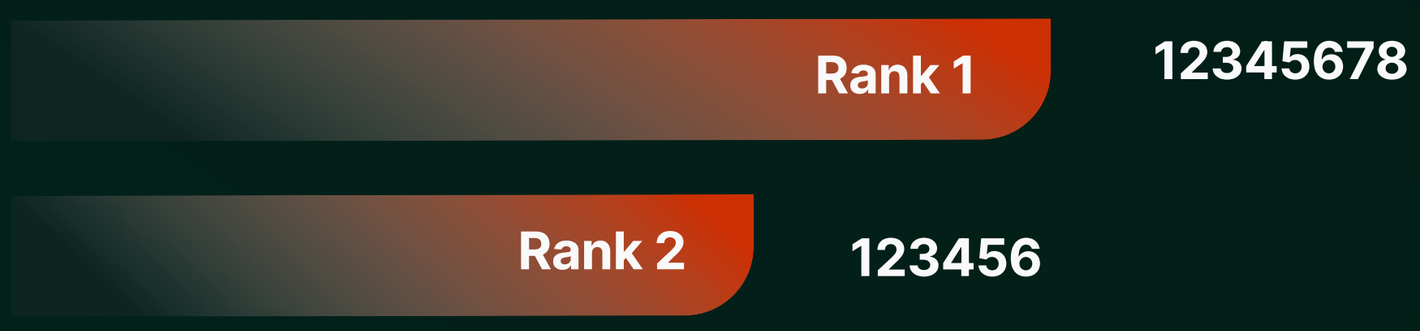
Many companies believe a data leak affects only one or two isolated accounts. Our analysis reveals a far more systemic risk: for the average company, exposure is not a minor oversight, but a significant issue involving multiple compromised passwords.

Multiple Leaks	On average, **our analysis identified 18 unique sets of credentials per organization.**
Extreme Exposure	The risk is not evenly distributed. In several cases, we identified extreme vulnerability, with 23 companies having between 100 and 400 unique passwords exposed on the dark web.
Persistence of Risk	If a domain repeatedly appears in these datasets, it often indicates that security gaps have remained unaddressed for years, allowing stolen data to accumulate.

The Password Paradox

Despite warnings from system providers regarding password hygiene, alarmingly predictable patterns continue to dominate the threat landscape. Our analysis reveals that the vast majority of compromised credentials still rely on simple numeric sequences, with '123' being the most prevalent starting point.

Most Common Passwords in Leaks



Typical Patterns

Common first names like Hannah and Michael, as well as terms like backend, doorbell, and Star Wars, frequently appear.

Patterns Found

- Mix of letters and numbers
- Cities
- Numbers
- Short Words
- Names
- Movie Titles

The Risk

Whether simple number sequences like 123456 or trivial terms like Star Wars, the use of weak passwords remains a significant risk. While such passwords are increasingly used in private contexts, such as for digital food ordering.

However, the danger runs deeper: our analysis shows that even complex, randomly generated strings appear en masse in leaks.

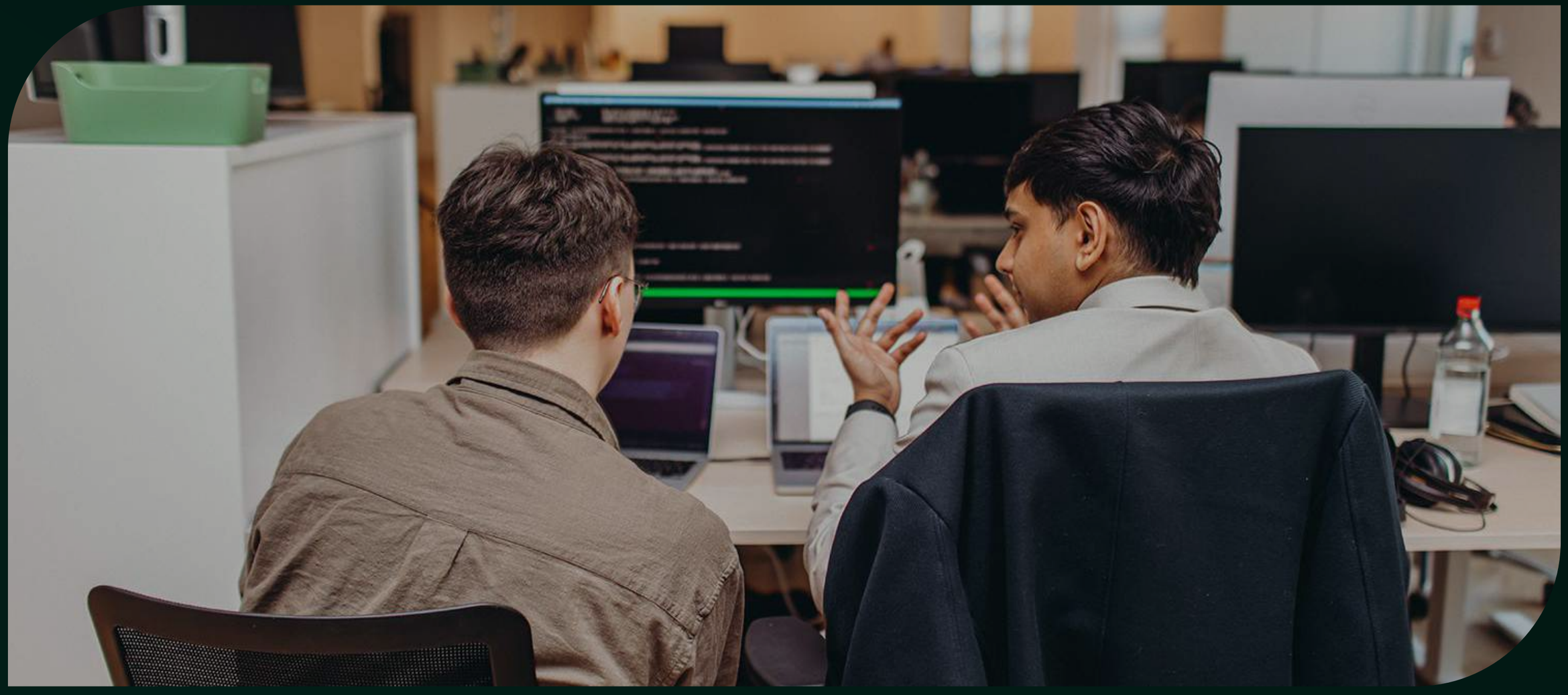
Andrew Saula
Head of Cybersecurity

"Criminal groups no longer bother to painstakingly crack passwords; they simply insert compromised credentials directly into automated tools (Credential Stuffing).

The conclusion: without additional factors like Multi-Factor Authentication (MFA), initial access to the corporate architecture remains trivial, completely disregarding password complexity."

The Attack Surface

While compromised passwords bypass primary access control, software vulnerabilities act like invisible cracks in the foundation of IT architecture. To identify these risks, our Deep Scan technology scans our clients' IT infrastructure and checks for 10,355 vulnerabilities (CVEs) with each run.



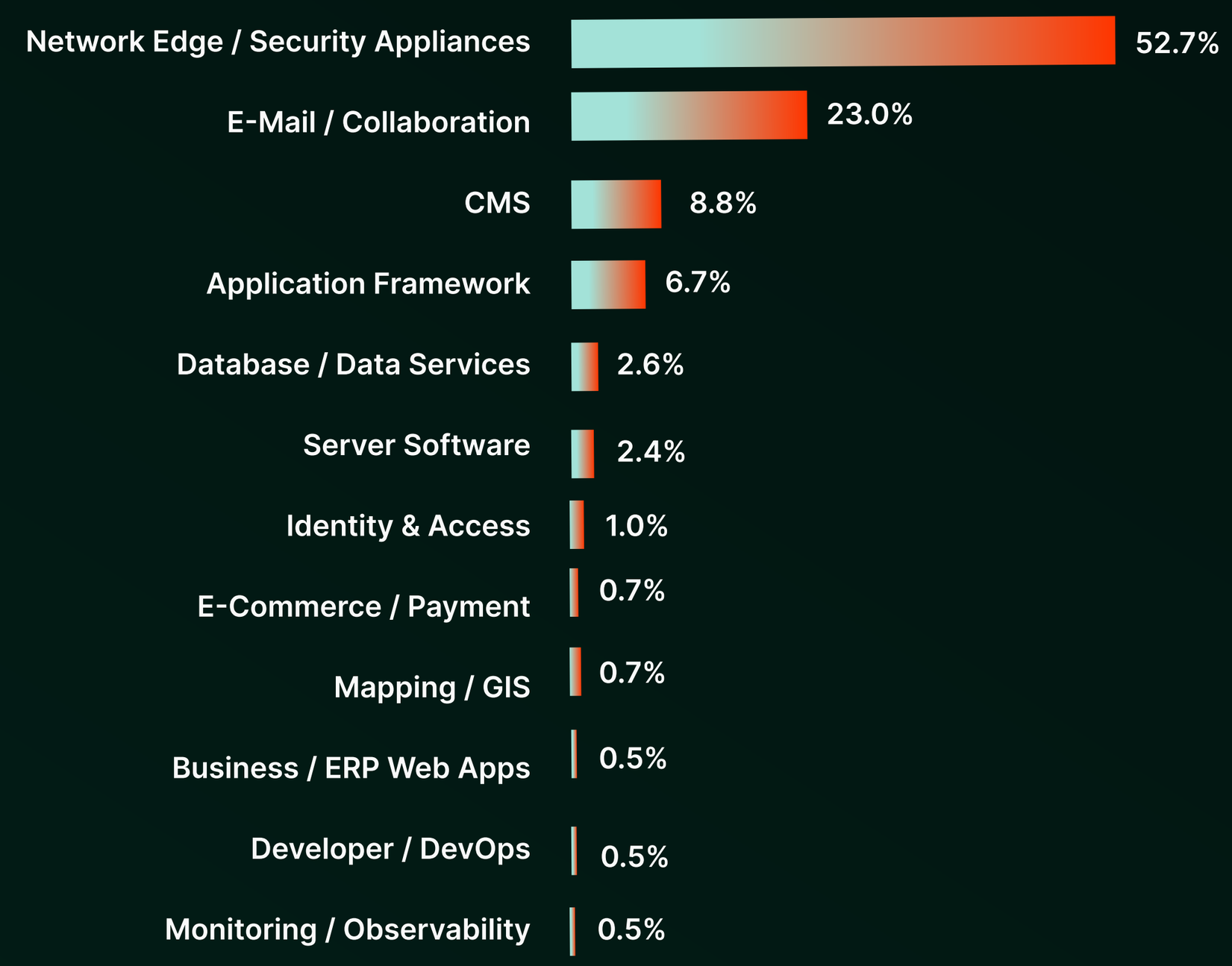
The Underestimated Gaps

When it comes to cyber threats, the danger is concentrated rather than spread. External pressure is overwhelmingly centered on network edge and collaboration technologies in small and medium sized enterprises, with those two categories driving three quarters of the total score and almost all of the active or zero-day signal. CMS and application frameworks remain relevant, but they sit clearly below that first tier.

For businesses, the defensive priority is clear: Secure your internet-exposed layers first. This is where attacks are most persistent, and where the damage is most significant.

75% of all critical threat activity focuses on just two areas: the network edge (VPNs/Firewalls) and collaboration tools (Email).

Top Targeted Technologies in Detail



Small Businesses, Big Opportunities

Our data shows a clear correlation between company size and patch discipline: While large enterprises often have dedicated teams for vulnerability management, smaller organizations frequently fall behind:

12.7%

critical vulnerabilities are found in companies with less than €1 million in revenue.

6.23%

critical vulnerabilities are found in companies with more than €100 million in revenue.

Outdated Software

The smaller the company, the older the software often is. Outdated VPN gateways or unpatched Exchange servers are like open windows on the ground floor – an invitation for ransomware groups.

While system maintenance in corporations is managed by dedicated IT departments, in SMEs it is often only done reactively or as a side task due to a lack of personnel. This absence of dedicated resources explains why critical vulnerabilities in companies with revenues of 100 million euros or more are almost halved.

Small in Revenue, Big in Risk

A dangerous misconception stubbornly persists among the management of smaller companies: "We are too small to be a target." This fallacy is based on the assumption that attackers manually select their targets. However, today's reality is dominated by massive automation. Criminal groups scan the entire internet in seconds for open vulnerabilities and unprotected interfaces. An automated bot scan merely looks for the path of least resistance. Anyone with a vulnerability becomes a target.

Our analysis shows: The attractiveness for hackers is not measured by revenue, but by data.

The Hidden Treasure

We have analyzed companies with an annual turnover of less than 5 million euros. The results debunk the myth of insignificance:

31% of all small businesses manage more than 10,000 PII records.

PII Prices

A single stolen data record costs on average about 134 euros. If a company loses 10,000 records, the theoretical total damage quickly amounts to 1.34 million euros. For a company with less than 5 million euros in annual turnover, this is existentially threatening.

11% of small businesses manage between 100,000 and even 500,000 records.

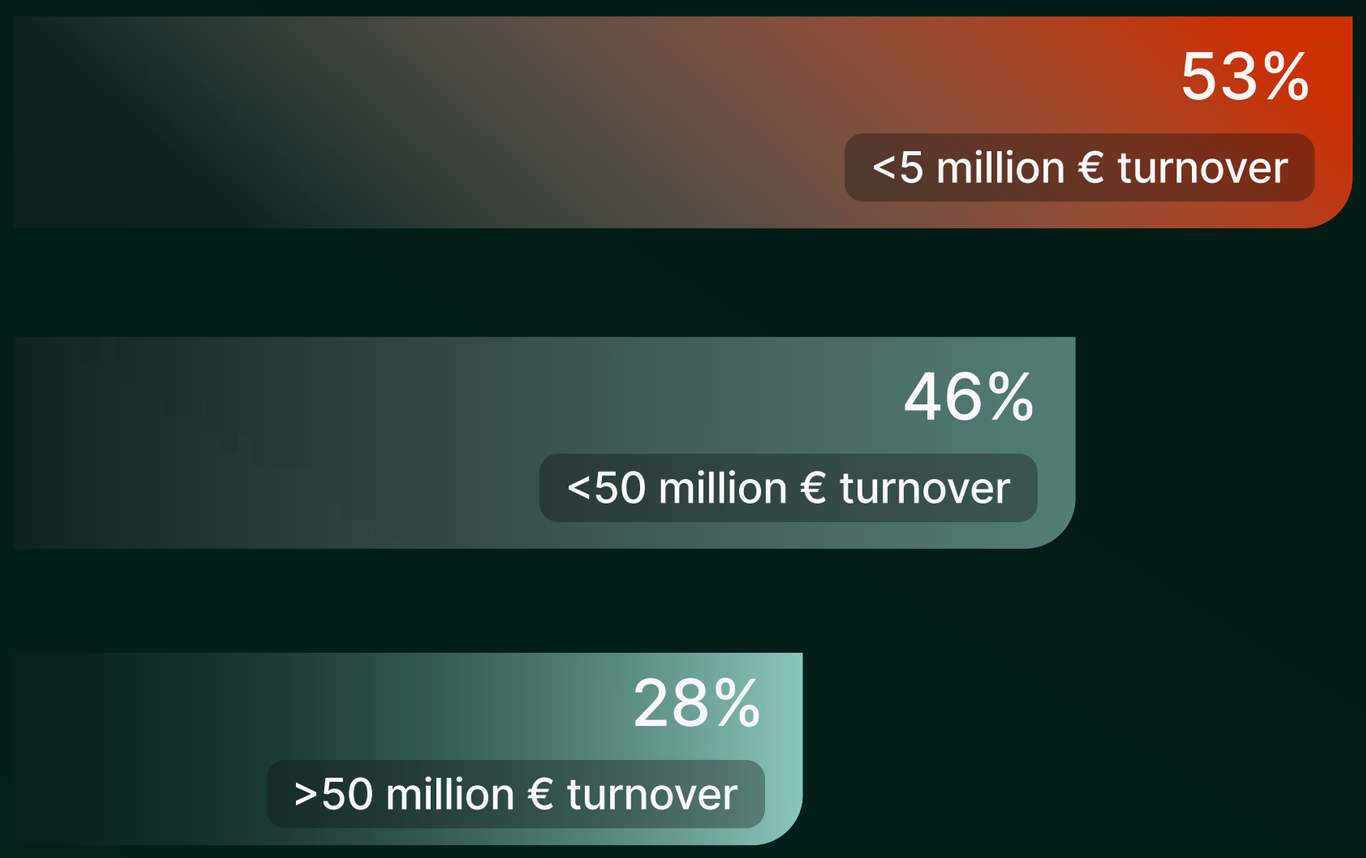
For an attacker, such a company is a goldmine. A data record is worth real money on the black market – the hacker does not care about the revenue. Even if the hacker does not resell the data, it is extremely valuable.
In modern ransomware attacks like Double Extortion, systems are no longer just encrypted; the data is also copied and exfiltrated unnoticed beforehand.

The hacker then threatens the company: "If you do not pay the ransom, I will publish your customers' data." The fear of hefty GDPR fines, lawsuits from customers, and reputational damage often forces the company to pay. Their own data thus becomes the perfect hostage.

The Missing Shield

Despite this risk, the most important protection is often missing: Multi-Factor Authentication (MFA). Our data shows that only companies with a turnover of over 50 million euros have MFA as a standard in IT security.

Statistic: Companies Without MFA



Dangerous Gap

Fatih Kenar
Cyber Security Analyst

"The gap is obvious: Small businesses have as much important data as large corporations, yet they still forget fundamental security standards. MFA could easily close this gap. It ensures that a login is only successful if, in addition to the password, a second personal proof, such as a code on the company mobile, is provided. Even if hackers possess a stolen password, they fail at this crucial hurdle."

MFA as a NIS2 Requirement

It is important to point out that with the implementation of the NIS2 directive, Multi-Factor Authentication (MFA) has officially transitioned from a "best practice" to a legal requirement across Europe. Under Article 21, MFA is defined as a mandatory baseline security measure for all affected organizations.

For companies operating within the EU, failing to implement MFA is no longer just a security oversight, it is a regulatory liability that can lead to significant fines and legal exposure.

6.12.2025 marks the date the NIS2 Directive became legally applicable for affected companies in Germany.

Frederik Schwarz
Cyber Security Analyst

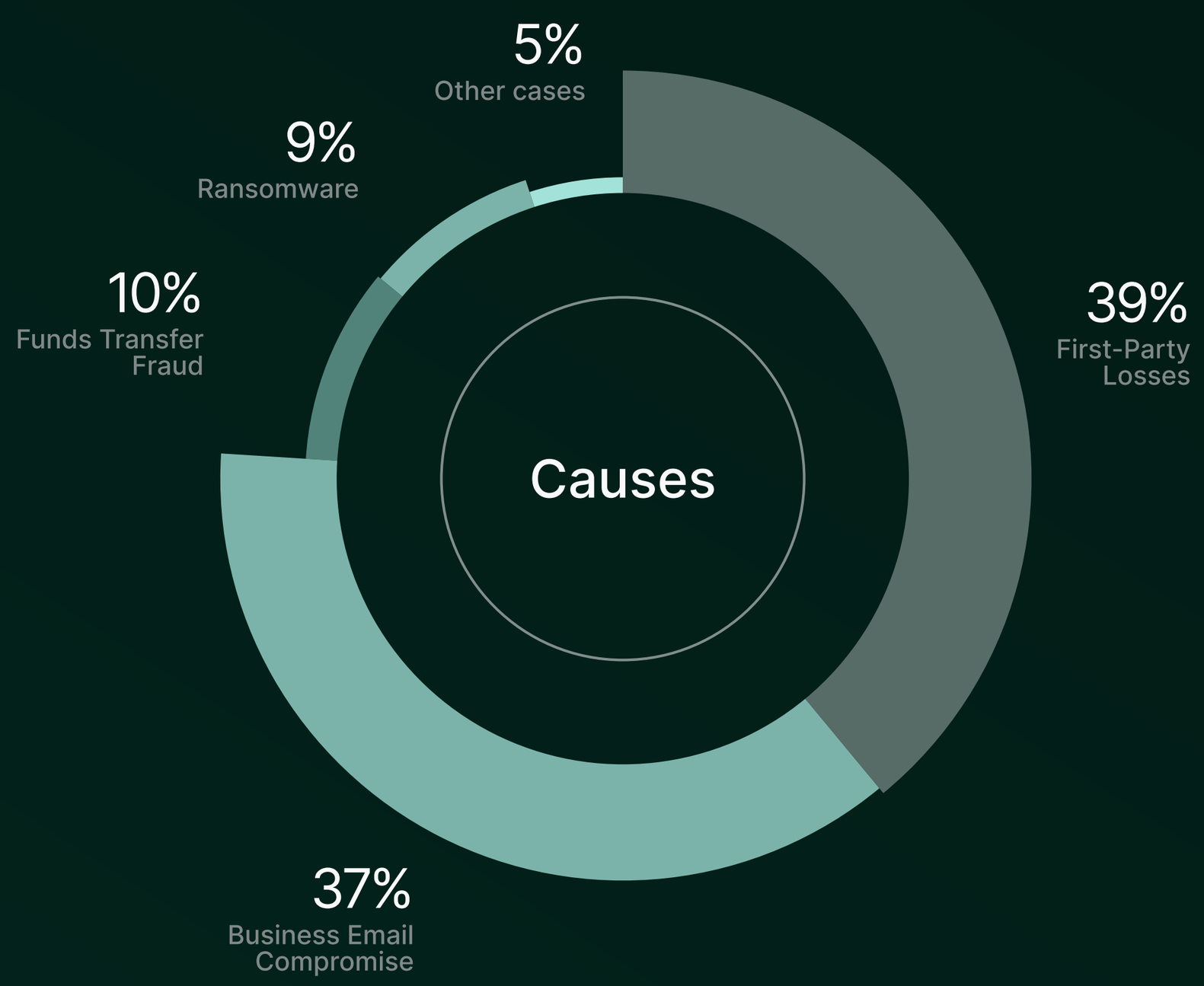
"NIS2 is a necessary evolution for European security, bringing long-overdue accountability to companies. But the real challenge remains the implementation: the legal pressure is immediate, but internal resources are scarce. It’s no longer about whether to improve security, but how fast you can bridge that resource gap."

The Art of Damage Control

When prevention fails, crisis management takes over. Our damage data provides a sober insight into the reality during and after the attack.

Causes of Financial Losses

Technical hacks are less often the cause of financial losses. In most cases, human error is the key factor. The leading drivers for financial losses are:



Awareness Training

Source: ENISA Threat Landscape 2025

Since First-Party Losses (such as phishing) is the leading cause of financial loss at 39%, a widespread awareness campaign for employees is absolutely necessary.

However, the reality is alarming: Our data shows that 46% of large companies (with over 100 million euros in revenue) do not conduct phishing simulations. The fact that nearly half of these resource-rich organizations neglect these awareness standards reveals a critical vulnerability in IT security.

This negligence is particularly fatal in 2026: By 2025, 80%* of social engineering attacks had been perfected by artificial intelligence. Without regular training, such phishing emails are hardly distinguishable from genuine messages.

The Cost of Ransom

Ransomware remains the most expensive scenario. Our analysis of 245 real ransomware cases reveals a shocking reality: Initial demands can reach as high as 2.59 million dollars. While the majority of demands fall between 100,000 and 500,000 dollars, nearly 30% of demands exceed the 1 million dollar mark.

Negotiating is Worthwhile

Contrary to the panic reaction of many victims, our analysis shows: The initial demand is almost never the final price. With professional help, the financial damage can be significantly reduced.

51% average price reduction through negotiation with an incident response expert.

Oliver Derwisch
Incident Response Manager

"Paying a ransom is rarely the right answer. True resilience comes from preparation and structured incident response – containing the damage, enabling recovery, and in most cases making payment unnecessary."

Negotiation Example

Source: Ransomware.live

$260,000 if you pay today.

We can pay $155,000 today.

$220,000 today. Here is our BTC wallet. Let us know when you are ready to pay.

Don't Just Pay

Paying a ransom is rarely the answer—and the data proves it. In most instances, the attackers walked away empty-handed. This success is driven by two key factors: robust backup systems and the rapid, strategic intervention of incident response teams.

Around 77% of affected companies did not pay the ransom.

The Backup Illusion

However, a functioning backup is not a given. Our data also reveals a dangerous complacency among corporations.

A shocking 21% of large companies (with over €100 million in revenue) do not regularly test their full recovery.

Without regular validation of recovery processes, backups provide no operational security in a crisis, but rather an unpredictable residual risk.

Resilience Instead of Panic

A professional implementation of IT security is not a project that can be completed in an afternoon – it is an ongoing process. But the good news is: companies do not need to build a digital fortress to successfully fend off the majority of opportunistic and automated attacks. For SMEs, establishing selected protective mechanisms is the crucial lever. We recommend three concrete practices that increase your resilience with manageable effort.

1. Secure Digital Identities with MFA

Strict multi-factor authentication (MFA) should be implemented across the entire IT infrastructure – for all internal employees, external service providers, and all access points (VPN, cloud services, email tenants). MFA is the best mechanism to neutralize compromised credentials and stolen passwords.

2. Beyond the Click

AI-powered phishing has made fakes nearly indistinguishable from reality. To build true resilience, the focus must shift to technological safety nets. While phishing simulations help maintain alertness, organizations should prioritize Managed Detection and Response (MDR). By combining Zero-Trust with 24/7 monitoring, threats are neutralized in real-time even if a link is clicked.

3. Ensure Operational Resilience with Verified Backups

An untested backup is not a security measure, but merely a vague hope. Many large companies make the mistake of blindly relying on automated storage routines. At least once a year, a full disaster recovery test should be conducted. A verified, offline-available data backup remains the strongest and only reliable tool against double-extortion ransomware.

We Close the Gap

Baobab Risk Solutions is one of the leading European providers of digital risk insurance. As a specialized Managing General Agent (MGA), Baobab understands digital risks through in-depth, data-driven analyses and offers proactive protection as a fundamental component of the insurance policy.

The company collaborates with highly rated Lloyd's syndicates as well as Zurich and Liberty Specialty Markets, which act as capacity providers. Established venture capital providers – such as Viola FinTech or eCapital – ensure long-term financial stability.

Since 2022, Baobab has been offering the Cyber Insurance Cyber Safe in the market. The fidelity insurance Crime and the IT liability insurance oneIT-protect complement the product portfolio.

Baobab Risk Solutions, headquartered in Germany, also operates in Austria and the Benelux countries.

Baobab Risk Solutions
Cyber Security, Insurance and Underwriting Experts

BRS collaborates with established capacity providers.

Baobab
Risk Solutions

baobab.io