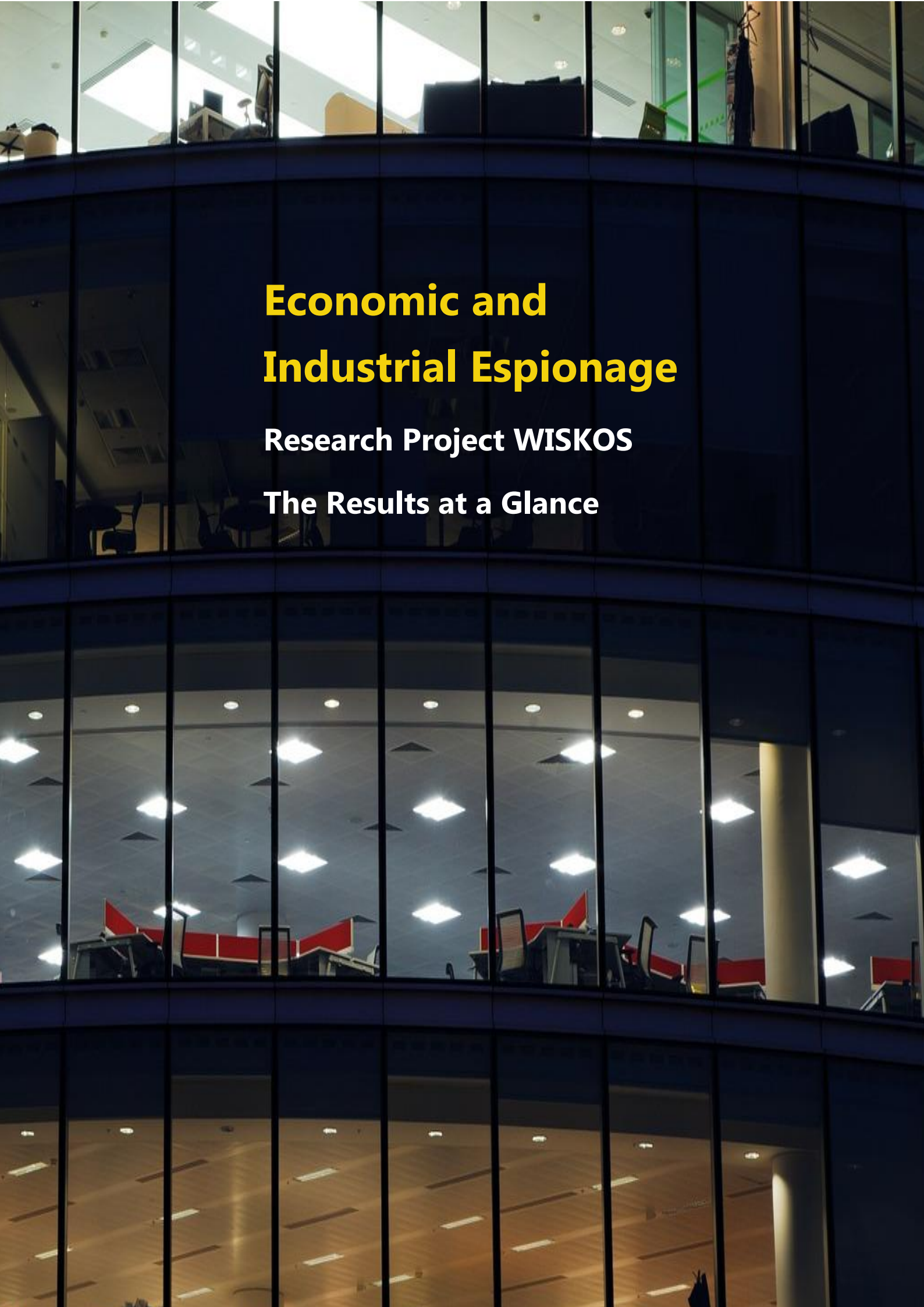

Economic and Industrial Espionage

Research Project WISKOS

The Results at a Glance

WISKOS

Text
Elisa Wallwaey, M.A.
Max Planck Institute for Foreign and International Criminal Law
Department of Criminology

As phenomena of economic and industrial espionage are quite complex due to the versatile possible combinations of offenders and modi operandi, victims of such offences have difficulties detecting those. Aggravating this problem is the fact that victimized businesses and organizations are quite reluctant when it comes to reporting incidents or suspicious cases to the authorities.

In order to analyze this to date largely unexplored subject area systematically and on an international level, WISKOS applied diverse methodological approaches to economic and industrial espionage in Germany, the other EU member states and Switzerland. The multilevel research concept covered the following topics: the legal and regulatory control structures, the prevalence of such crimes in the areas of reported and unreported crime as well as operational and governmental preventive concepts. Over the course of time, the situation in Germany increasingly came to the fore with the aim to develop preventive strategies against espionage and to enhance the communication between and willingness to cooperate with state authorities on the part of businesses and scientific organizations.

The resulting information material and recommendations for action are only available in German. They can be download here.

SMEs

Due to the rapid technological advancement and the digitization of society, SMEs are exposed to the same threat level of economic and industrial espionage as large enterprises or corporations as their perceptibility on a national as well as international scale is growing. However, unlike the latter SMEs usually lack a sufficient amount of financial resources and personnel to provide for comprehensive corporate protection. As **almost 50% of SMEs report that at least one (suspicious) case has happened in the last five years**, such protection is clearly needed.

Estimating the amount of loss is quite difficult, but when using the duration of business constraints that result from espionage as a substitute, the tremendous damage potential becomes apparent: **Nearly a quarter of businesses having fallen victim to espionage reported constraints lasting at least 48 hours (23%). Five percent thereof even considered the constraint threatening the company's existence**.

Scientific Organizations

Since many years, the international research community has paid great attention to the German science sector. Attention that is not always welcome as research findings may be a rewarding target for foreign states, fellow scientific organizations and businesses alike.

As **no reliable data** on the amount of loss exist, it is (once again) difficult to assess the damage potential of espionage. Furthermore, aggravating the problem, the **value of research results can hardly be expressed in numbers**.

Characteristics of Espionage

The aim of espionage is the same whether a company or a scientific organization is targeted: protected information, e.g. product sketches, prototypes, customer data, manufacturing formula, research results and the like. The potential perpetrators, their modi operandi and their motives are the same, too.

The Offenders and their Methods

Due to their expert knowledge about internal processes, products, customers, investments to mention but a few, **internal offenders (34%) pose the greatest threat to a company's knowhow**. Using their knowledge, they identify and steal the most valuable information. However, external persons acting on behalf of a foreign intelligence service, a competing company or for his/her own benefit account for an even larger portion of offenders (44%). In 15% of the cases, internal and external actors worked together be it intentional or unintentional. A typical procedure is **social engineering**, whereby the target person is deliberately manipulated to perform (or refrain from performing) a certain act, e.g. disclosing protected information.

The concrete procedure depends, of course, on the perpetrator's position in relation to the company/ organization. After having identified valuable information, internal offenders may e.g. copy, photograph or send the information via email, while external ones may photograph production facilities or prototypes during a factory tour or trade fair or gain access to the company's/organization's network or its machinery and equipment by means of a cyberattack.

Proceedings in Case of Damage

When it is too late to take preventive action because an incident has already been detected, insecurity about how to deal with it usually prevails among affected companies/organizations. Besides own measures towards the perpetrator (25%), **external specialists** are frequently consulted (22%). By contrast, **22% of the victims filed a complaint while 27% expressly stated that they did not seize this opportunity**. This fact might indicate the uncertainty of victims about the official competencies. A cost-benefit-calculation assesses the expense going along with a criminal trial as high while the benefit is considered low. Thus, companies/organizations refrain from filing a complaint on a regular basis.

Possibilities of Prevention

Like the modi operandi possible preventive actions and the protection of knowhow are equally important and feasible for businesses and scientific organizations alike. Nevertheless, companies and organizations are often not sufficiently aware of their information's value and the huge potential material as well as immaterial damages caused by the theft of knowhow. Therefore, protective measures and the systematic monitoring of suspicious indicators do not receive the necessary diligence and attention, which in turn leads to a high share of undetected cases and open security gaps.

Measures to prevent the loss of knowhow are manifold and oftentimes implementable without great expenses. The possibilities cover a wide range such as IT protection, access controls, employee trainings or data protection rules. The prevalence of these and further measures in SMEs have been analyzed.

On average, medium-sized enterprises (≥ 50 employees) have a more comprehensive protection concept in place than smaller ones. Furthermore, irrespective of the company size, the measures implemented in at least a third of the businesses clearly focus on IT security leaving other crucial areas largely neglected. A differentiated look on the data reveals that irrespective of a company's size the following preventive actions are rather common (69-97%):

1. **Firewalls, anti-spam-protection and/or virus scanners**

Irrespective of the company size, over 90% report having such software implemented: 94% of small enterprises with less than 50 employees and 97% of those with more than 50 employees (medium-sized).

2. **Access controls**

74% of the small businesses and 89% of the larger ones restrict the access to the premises, specific areas and/or data.

3. **Employee sensitization**

Sensitizing employees regarding the value and protection of proprietary knowledge, costumer data and the like is important for companies of all sizes and 77% small companies as well as 86% of the medium-sized ones report doing so.

4. **Data backup concept**

An operational IT system is crucial for a business as well as organizational success. Thus, in case of a malfunction, e.g. due to the deletion or manipulation of data, it is important to quickly restore the system’s functioning in order to prevent losses. This is why 73% of the small and 84% of the medium-sized business have a data backup concept at their disposal.

5. **Employment contracts**

As the own personnel might pose a threat to a company’s/organization’s proprietary knowledge, it is important to make sure employment contracts are complete and include e.g. non-disclosure agreements in employment contracts. 69% of small businesses and 81% of those with at least 50 employees report paying due attention to the design of contracts.

Table 1 shows the prevalence of these and other preventive strategies among German SMEs.

Table 1: Implemented preventive strategies in percent

Preventive Strategy	SE*	ME**
Firewalls, anti-spam-protection and virus scanners	90%	97%
Access controls	74%	89%
Employee sensitization	77%	86%
Data backup concept	73%	84%
Design of and conditions included in employment contracts	69%	81%
IT security system meeting common standards	33%	62%
Physical separation of networks, DMZ and patch management	30%	51%
Employing a security officer	17%	39%
Email encryption	26%	33%
Regulations concerning BYOD, social media and (private) data storages	14%	30%
Codified security concept	11%	27%
Eavesdropping protection and video surveillance	12%	23%
Special provisions for external staff, leasing personnel or other service staff	5%	19%
Periodic penetration testing and emergency/crisis simulation	5%	16%

Source: WiSKoS-Erhebung 2017, Fraunhofer ISI
Note: *Small businesses (< 50 employees) / **Medium-sized businesses (≥ 50 employees)

In addition, the cooperation between businesses as well as scientific organizations and prosecution authorities is a crucial element of a comprehensive protective concept. The willingness to cooperate, in turn, builds on a trustful relationship that is not naturally given. Developing trust is a time-consuming but helpful task as the willingness to file a complaint depends to a large degree on a trustful relationship between the two parties.

The development opportunities are promising: Only 2% of the SMEs are under no circumstances willing to cooperate with the authorities, while about a quarter (26%) would do so in any case. Others attach conditions thereto, the most prominent of which are:

1. **Appropriate cost-benefit ratio**

For more than half of the companies (55%) a positive outcome of a cost-benefit calculation is a precondition for reporting a case of espionage.

2. **Belief in the investigation's success**

About half of the sample (51%) would report an incident to the police if they believed in the investigation's success.

3. **Non-bureaucratic incident report**

Of the queried SMEs 48% make their reporting behavior dependent on the bureaucratic operations attached to a complaint.

An overview of these and further conditions attached to the reporting behavior is shown in table 2 below.

Table 2: Conditions for cooperation in percent

Condition	Share of companies
Appropriate cost-benefit ratio	55%
Belief in the investigation's success	51%
Non-bureaucratic incident report	48%
Appropriate case processing	42%
Establishing effective preventive strategies	42%
Damage threatens the business' existence	42%
Receiving information about the ongoing investigations	37%
Pre-evaluation by the official contact person	30%
Insurance conditions include reporting the offence	29%
The existence of a reporting obligation	24%
The offender has been identified	21%
I already know whom to contact	16%
Reporting is anonymous and online	9%
A voluntary commitment by the industry to report incidents	8%

Source: WiSKoS-Erhebung 2017, Fraunhofer ISI

Conclusion

The threat of espionage pertains to businesses no matter their size and scientific organizations alike. Even though no reliable data on the amount of damage exists, the damage potential is large and poses potentially a threat to the company's or organization's existence. Thus, the need for comprehensive protective strategies is self-evident. Developing and implementing these is a crucial task of the parties potentially concerned as well as the police. A suitable starting point would be to build trust by resolving the uncertainties about whom to contact in which case and about the prosecution and the proceedings. This would facilitate long-term cooperation and, as a future prospect, improve the reporting behavior in the long-term.