ECONOMIC AND INDUSTRIAL ESPIONAGE

at Austrian Companies 2015

December 2015
ECONOMIC AND
INDUSTRIAL ESPIONAGE
at Austrian Companies 2015

December 2015
This brochure, as well as other current publications are available at the Service LLC of the Austrian Economic Chambers:
Telephone: 0590 900-5050
Fax: 0590 900-236
E-mail: mservice@wko.at
Internet: http://webshop.wko.at

IMPRESSUM:

Authors
The handbook presented here was compiled by several authors commissioned by the Ministry of the Interior/Federal Office for State Protection and Counterterrorism through the University of Applied Sciences FH Campus Wien Research and Development, LLC.

Authors
Mag. Claudia Körmer, FH-Prof. Martin Langer, University of Applied Sciences FH Campus Wien

Survey development: Mag. Claudia Körmer, Austrian Economic Chambers, Industriellenvereinigung [Federation of Austrian Industries]
Statistical evaluation: Mag. Christian Steinlechner
Editing: DI (FH) Mag. Thomas Goiser MA
Layout: Marion Gaa (www.lucid.at)

Media proprietor
Federal Ministry of the Interior
Federal Agency for State Protection and Counterterrorism
Telephone: 01-531 26-4100
E-mail: wis@bvt.gv.at
Internet: http://www.bmi.gv.at

Publisher
Designed and printed with the support of the Austrian Economic Chambers.
Wiedner Hauptstraße 75
1045 Wien

All rights reserved.
This publication has been prepared in good faith, although errors cannot be entirely ruled out. Therefore, no guarantee is assumed for the correctness of its contents. Neither the authors nor the media proprietor assume any liability.

Vienna, December 2015
CONTENTS

6  FOREWORD
10  STUDY DESIGN
11  PIVOTAL RESULTS
12  COMPOSITION OF COMPANIES
14  DETAILED RESULTS
   14  Occurrence at Companies
   24  Risk Assessment by Companies not Affected
   26  Preventive Measures
   32  Companies’ Expectations
33  CONCLUSION: DEMAND FOR GREATER INTERCONNECTEDNESS
34  Branch Descriptions According to ÖNACE 2008; Bibliography
The challenges for a company’s survival in the face of domestic and international competition are numerous. The availability of resources, including the necessary employees, a favourable legal environment, and trusting cooperation among business, academia and security agencies are the basic requirements for a safe and secure business location. They must be protected.

For its 15th legislative term (2013-2018), the Austrian federal government has set as a goal the fight, together with business, against economic and industrial espionage. As the responsible security agency, the Federal Agency for State Protection and Counterterrorism, conducted a study within the framework of the prevention program Wirtschafts- und Industriespionage [Economic and Industrial Espionage] (WIS) on the occurrence at Austrian companies of economic and industrial espionage in order to evaluate the effects of initiatives already in place and to identify practical areas for preventive work.

In the short-term, successful attacks signify the weakening of a single company. In the long-term, the appeal and reputation of Austria as a business location is weakened. Awareness of potential threats to companies by state-run industrial espionage as well as of the unfair competitive practice of industrial espionage is the basis for development of individual security measures.

The Ministry of the Interior’s task is to offer forms of prevention requested by business. The representative study here is a complement to publications available and offers an objective picture of the self-assessment of companies. It also points out once more the relevance of the identification of actual business and trade secrets. In today’s knowledge society and the constantly expanding opportunities for connectedness at an individual and a virtual level, it’s necessary to protect know-how together.

Mag. Johanna Mikl-Leitner
Minister of the Interior
Seize opportunities, bet on security.

Dear Sir or Madam,

Austrian companies are seizing the opportunities presented by globalization and the EU Single Market. Accordingly, from our entry into the EU in 1995 to the year 2014, the export of Austrian goods more than tripled, from €42bn to 12,2 Pt128bn.

Many Austrian businesses are market leaders in niche areas. With their innovative products and services, they secure jobs and income in Austria. The globally connected and highly digitalized world poses new challenges for us, though.

Many Austrian companies are exposed to the dangers of economic or industrial espionage. Offenders focus primarily on manufacturers and manufacturing-related services, as well as telecommunications and ICT companies.

What can the companies themselves do? They can tie their corporate strategy more closely to their security strategy, appoint persons responsible for corporate security, reinforce data protection, and systematically identify external hazards. How can companies be supported in the realm of prevention?

The Austrian Economic Chambers, together with the Ministry of the Interior, will further expand information on prevention of economic and industrial espionage. As such, “E-Day: 16”, under the banner "Corporate Security", is devoted to IT and data protection issues, as well as to “security training and loyal employees”, among others.

I would like to take this opportunity to thank the over 1,100 companies who, despite their intense everyday business, took the time to assist in this study by responding to the questionnaire. Thank you to the project partners: the Minister of the Interior, Industriellenvereinigung [Federation of Austrian Industries], and University of Applied Sciences FH Campus Wien for their support.

Dr. Christoph Leitl
With globalisation, domestic industry’s security demands have been increasing in complexity for years. Functioning protection of industry and business can thus only be pursued through a comprehensive approach.

Only together, through analysis of the threats, will we be able to develop a strategy suitable to Austrian business. In doing so, we will improve protection of our industry and our country as a business location. Thus, in cooperation with the Ministry of the Interior, the Austrian Economic Chambers and the University of Applied Sciences FH Campus Wien, the Industriellenvereinigung has collected data on the current situation in Austria. These data are used to evaluate the effects of initiatives already in place and to identify new areas for action. The study here offers a picture showing to what extent Austrian companies are affected by those threats, and at the same time it gives all of the stakeholders a common task: that of strengthening our business location.

The threat to Austrian industry and business is very real and does billions of euros in damage every year. In most cases, espionage is directed against companies whose products and services are globally regarded for their constant innovation and high standards of quality. Hallmarks like “Made in Austria” are an expression of this quality and make it appealing to imitate. Prevention of industrial and economic espionage will increasingly become a decisive competitive factor.

Every cloud has a silver lining, though: the issue of cyber-security as well as industrial and business protection opens up new possibilities in society for innovative companies in Austria and Europe. The global market for IT security has grown to €50bn euros, and has increased yearly over the last ten years by percentages in the double digits. Austria and Europe have to seize this chance and start catching up. Many innovations for the future, from self-driving cars to smart homes, require a digitally connected business world. For this, new ways of thinking and innovations in the area of security are in demand. These are the challenges that the state and business have to confront together.

A secure business world contributes to the security and the stability of our country’s society. Business protection is thus not only a competitive advantage, but also ensures our future. Austria’s industry is ready and willing to, actively and in close cooperation with the authorities, take on responsibility and press ahead with the steps necessary for more cybersecurity and for effective industry and business protection—without it having to come to overregulation or ubiquitous monitoring.

Ing. Mag. Peter Koren
Vice Secretary of the Industriellenvereinigung [Federation of Austrian Industries]
We are confronted daily with crises and catastrophes presented by the media, and we deal with any number of dangers in our professional and personal lives. A danger less embedded in our awareness is that of economic and industrial espionage.

In our connected world, offenders could be anywhere: at companies themselves, abroad, or at a neighbouring table at a restaurant. Their modes of attack are varied and often used in combination. In most cases, the danger to the company goes undetected, instead of watertight evidence there is only conjecture, and the effects are only noticed later.

With this study, which we conducted with our trusted partners the BMI [Ministry of the Interior], the Austrian Economic Chambers, and the Industriellenvereinigung [Federation of Austrian Industries], we would like to shed light on the actual extent and background of this problem.

I would like to offer my hearty thanks to all of the companies that participated in the survey for this study. Your help enables appropriate support from academia and politics.

Economic and industrial espionage is an all-embracing and strategic issue, which, in contrast to “classical” security, needs to be thought of in terms of markets, products, competitive situations and globalisation.

Of highest priority is protecting companies’ value: company strategy information, customers, products and processes, suppliers and prototypes.

The best means against economic and industrial espionage is prevention. That includes an all-encompassing increase in awareness and being able to recognise and understand the problem. Connectedness and the integration of cultural, organisational, technical and structural measures are crucial: a chain is only ever as strong as its weakest link. With our bachelor’s program Integrated Safety and Security Management, we train specialists who can guarantee not only the safety and security of the various company sites, but also through to and including travel safety and information security. With the Master’s program Integrated Risk Management, we train specialists for the strategic level who speak the language of business and who can adequately manage risks and dangers. For this we’re counting on international academic networking and cooperation with specialised companies primarily in German-speaking countries.

We see academic training and applied sciences as the ability to understand and solve problems. We are looking forward to continued partnerships and exchange of information with you.

FH-Prof. DI Martin Langer
Director of Studies, University of Applied Sciences FH Campus Wien
Risk and Security Management Department

ECONOMIC AND INDUSTRIAL ESPIONAGE

FH-Prof. DI Martin Langer
STUDY DESIGN

For the composition of the sampling, a universal set of \( N = 163,872 \) Austrian companies was drawn from the data pool of the Austrian Economic Chambers and the Industriellenvereinigung (IV) [Federation of Austrian Industries]. Altogether, 15,000 companies were selected for the survey using a stratified sampling according to province, industry and enterprise size. It was conducted via a standardised online questionnaire from June 23 to July 31, 2015.

The business activities of the companies surveyed were classified according to ÖNACE [Austrian Statistical Classification of Economic Activities] 2008 in order to obtain as differentiated a picture as possible. The study’s universal set represents the whole business location of Austria. Earlier international surveys drew only from specific minimum enterprise sizes, industries or numbers of employees. The results of this study are thus incomparable with other less comprehensive surveys, as due to their modified sampling, different ratios emerge.

The questionnaire covered, besides company information [province, subsidiaries, and turnover, for example], the areas innovation, possible instances of espionage in the past five years, assessment of possible instances of espionage in the future (at companies with none to date), preventive measures, and expectations. The long observation period of five years lends greater validity to the central question of whether a company has been affected by economic and industrial espionage, especially in regards to subsequent damage. Content-wise, special focus was placed on questions regarding companies’ awareness of the fact that employees and dealings with them is a central element of company security.

A total of 1,149 surveys were fully completed and analysed. This correlates to a return rate of 7.7%.
PIVOTAL RESULTS

1. 5.1% of the companies surveyed indicated that at least once in the past five years they were victims of economic or industrial espionage (many of them multiple times). A third of the incidents occurred at industrial firms. Based on the universal set used, that would mean around 8,400 companies affected.

2. The offenders reside domestically and abroad, and attack Austrian companies at their domestic sites as well as those abroad using various means (often in combination). Regardless of the tools used, people are behind every attack. In almost half of the cases, employees are suspected of being behind the crimes.

3. Companies affected have up to now low expectations of the success of criminal prosecution: only a fourth of respondents admitted to having involved the authorities; the most common reason named is lack of evidence.

4. Besides imminent financial damage, a series of further types of damage occurs at companies: 71% of companies affected indicated having suffered from consequential damage critical to their business, for example operating losses and/or loss of clientel, damage to their reputation, etc.

5. A large portion of the companies considers a great part of their information to be particularly confidential trade or industrial secrets: almost 30% indicated that more than half of the information at the company constitutes trade or industrial secrets. That makes effective protection thereof difficult in practice.

6. In regards to enterprise size, there are no significant differences. Each company is a potential victim. Large companies generally have more extensive mechanisms and know-how available for how to protect their trade and industrial secrets. In more heavily regulated industries, the quality of measures adopted is rated as higher.

7. Companies want, above all, a targeted range of information from the authorities in the form of online information platforms and brochures, as well as industry events.
MIX OF COMPANIES

Industries

The companies are categorised by their business activities according to ÖNACE 2008 as follows:

**Table 1: Industry or main activity**

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>EXPECTED VALUE</th>
<th>OBSERVED VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trade, maintenance and repair of motor vehicles</td>
<td>25.5 %</td>
<td>10.3 %</td>
</tr>
<tr>
<td>Professional, scientific and technical services</td>
<td>15.2 %</td>
<td>7.7 %</td>
</tr>
<tr>
<td>Construction</td>
<td>10.9 %</td>
<td>10.2 %</td>
</tr>
<tr>
<td>Accommodation and food service activities</td>
<td>10.9 %</td>
<td>6.6 %</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>8.4 %</td>
<td>15.6 %</td>
</tr>
<tr>
<td>Information and communications services</td>
<td>6.5 %</td>
<td>10.5 %</td>
</tr>
<tr>
<td>Administrative and support services</td>
<td>4.2 %</td>
<td>7.2 %</td>
</tr>
<tr>
<td>Miscellaneous services</td>
<td>4.1 %</td>
<td>12.1 %</td>
</tr>
<tr>
<td>Transportation and storage services</td>
<td>3.6 %</td>
<td>3.7 %</td>
</tr>
<tr>
<td>Financial and insurance sector</td>
<td>2.8 %</td>
<td>4.5 %</td>
</tr>
<tr>
<td>Real estate activities</td>
<td>2.3 %</td>
<td>1.6 %</td>
</tr>
<tr>
<td>Health and social services</td>
<td>1.9 %</td>
<td>3 %</td>
</tr>
<tr>
<td>Art, entertainment and recreation</td>
<td>1.4 %</td>
<td>1.7 %</td>
</tr>
<tr>
<td>Education</td>
<td>1.1 %</td>
<td>0.7 %</td>
</tr>
<tr>
<td>Agriculture, forestry, fishing</td>
<td>0.6 %</td>
<td>1.2 %</td>
</tr>
<tr>
<td>Water supply, sewerage, waste management and remediation activities</td>
<td>0.3 %</td>
<td>0.6 %</td>
</tr>
<tr>
<td>Mining and quarrying</td>
<td>0.1 %</td>
<td>1 %</td>
</tr>
<tr>
<td>Electricity, gas, steam and air conditioning supply</td>
<td>0.1 %</td>
<td>1.8 %</td>
</tr>
</tbody>
</table>

\(n = 1,149\)
Enterprise size

Companies were grouped by number of employees according to established definitions of small and mid-sized enterprises. Micro-enterprises have up to nine employees; small, 10-49 employees; mid-sized enterprises, 50-249 employees; and large enterprises, over 250 employees (these companies themselves being grouped into further categories).

Table 2: Enterprise size

<table>
<thead>
<tr>
<th>EMPLOYEES</th>
<th>EXPECTED VALUE</th>
<th>OBSERVED VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 9</td>
<td>82.0 %</td>
<td>63.2 %</td>
</tr>
<tr>
<td>10 to 49</td>
<td>15.2 %</td>
<td>16.6 %</td>
</tr>
<tr>
<td>50 to 249</td>
<td>2.4 %</td>
<td>8.2 %</td>
</tr>
<tr>
<td>250 to 999</td>
<td>0.2 %</td>
<td>6.4 %</td>
</tr>
<tr>
<td>1,000 to 9,999</td>
<td>0.1 %</td>
<td>4.5 %</td>
</tr>
<tr>
<td>over 10,000</td>
<td>0.1 %</td>
<td>1.0 %</td>
</tr>
</tbody>
</table>

n = 1.149

Sites and subsidiaries abroad

The 1,149 companies, grouped according to the province where their headquarters is located, are predominantly in Vienna and Lower Austria (around 20% each), followed by Styria (13%), Upper Austria (12%), Tyrol (9%), Salzburg (9%), Carinthia (7%), Vorarlberg (4%), and Burgenland (3%). About 2% of the companies' headquarters are located outside of Austria.

255 of the 1,149 companies surveyed have subsidiaries abroad, and an average of three was specified.

Business relations

Almost all (over 94%) of the companies surveyed maintain constant or frequent business relations domestically, almost half in Western Europe and just over a quarter in Central and Eastern Europe. Around 10 to 14% of the companies maintain constant or frequent business relations each with CIS countries, North America and Asia. Less than 10% of Austrian companies maintain constant or frequent business relations with the Middle and Far East, Central and South America, or Africa.

Annual turnover

Seven of ten companies attained an annual turnover of up to €2 million in their most recent fiscal year; approximately 10% had up to €10 million. Around 5% of the companies sold up to €50 million; 4% sold up to €100 million. Lastly, approximately 10% reported turnover of over €100 million.

Research and development, and innovations

A third of the companies surveyed indicated conducting research and development activities. 61% of the companies (702 in all) have introduced no new products or methods to the market in the past five years. Of the remaining 39% (447 companies), nearly three quarters of them introduced up to ten innovations to the market.

---

1 This corresponds in terms of magnitude with the distribution of companies in the Austrian provinces: Vienna (18%), Lower Austria (17%), Styria (15%), Tyrol (12%), Upper Austria (11%), Salzburg (10%), Carinthia (8%), Vorarlberg (6%), and Burgenland (just under 3%)

2 Most of those subsidiaries (over 43%) are in Europe (25.8% in Western Europe and 17.4% in Central and Eastern Europe), followed by Asia and North America (at somewhat over 11% each). The last third is distributed across the Commonwealth of Independent States, Central and North America, the Middle and Far East, Australia, Oceania and Africa.
DETAILED RESULTS

OCCURRENCE AT COMPANIES

In answer to the question of whether they have been affected by espionage in the past five years, 5.1% (fifty-nine) of the 1,149 companies indicated having been victim of at least one instance of espionage. 38.2% responded that they know of no instance of espionage at their companies, 56.7% stated that they have not been affected by espionage.\(^3\)

Out of the 59 companies affected, according to their own data, 23 reported having been victim to one espionage attack, 15 reported two, 7 reported three, one company reported four attacks, and 13 companies reported five or more.

\(^3\) In 2010, almost a third of Austrian companies (31%) surveyed reported having been victim in the past. However, direct comparison is not possible due to differing study designs, questions and areas of focus.
Occurrence according to industry and province

In a third of the cases, industrial firms were affected by economic or industrial espionage. The five industries affected most were manufacturing, followed by information and communications services, accommodation and food services activities, administrative and support services, and miscellaneous services.

That corresponds to other surveys and public discussions; included here are large international industrial firms, just as telecommunications and ICT companies.

Table 3: Occurrence by industry

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>FREQUENCY</th>
<th>PERCENTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>14</td>
<td>26.4 %</td>
</tr>
<tr>
<td>Information and communications services</td>
<td>10</td>
<td>17.5 %</td>
</tr>
<tr>
<td>Administrative and support services</td>
<td>5</td>
<td>8.8 %</td>
</tr>
<tr>
<td>Miscellaneous services</td>
<td>5</td>
<td>8.8 %</td>
</tr>
<tr>
<td>Accommodation and food service activities</td>
<td>5</td>
<td>8.8 %</td>
</tr>
<tr>
<td>Trade, maintenance and repair of motor vehicles</td>
<td>3</td>
<td>5.3 %</td>
</tr>
<tr>
<td>Transportation and storage services</td>
<td>3</td>
<td>5.3 %</td>
</tr>
<tr>
<td>Construction</td>
<td>2</td>
<td>3.5 %</td>
</tr>
<tr>
<td>Professional, scientific and technical services</td>
<td>2</td>
<td>3.5 %</td>
</tr>
<tr>
<td>Education</td>
<td>2</td>
<td>3.5 %</td>
</tr>
<tr>
<td>Financial and insurance sector</td>
<td>1</td>
<td>1.8 %</td>
</tr>
<tr>
<td>Electricity, gas, steam and air conditioning supply</td>
<td>1</td>
<td>1.8 %</td>
</tr>
<tr>
<td>Art, entertainment and recreation</td>
<td>1</td>
<td>1.8 %</td>
</tr>
<tr>
<td>Real estate activities</td>
<td>1</td>
<td>1.8 %</td>
</tr>
<tr>
<td>Mining and quarrying</td>
<td>1</td>
<td>1.8 %</td>
</tr>
</tbody>
</table>

n = 53; no response from 6 companies
Occurrence by enterprise size and turnover

A synopsis of the total number of participating companies grouped according to number of employees further confirms the results indicating that small and mid-sized enterprises are particularly affected by instances of espionage.

More than half of the companies affected have a turnover of less than €2 million annually.
Subsidiaries

Twenty-nine of the companies affected have subsidiaries abroad; 30 have none. Of those companies having subsidiaries, those from the manufacturing industry all over the country are most affected by espionage attacks, followed by those from service industries and information and communications services.

Frequency of espionage attacks

In the past five years, if anyone, micro- and small enterprises have been affected by five or more instances of espionage. From a purely statistical point of view, however, no assertions can be made based on these data regarding whether or not the size of a company has any impact on the occurrence of espionage.

Innovation, research and development

Nearly half of the companies affected conduct research and development. The results show that industrial companies play the leading role here and that especially the manufacturing industry, as a rule, develops at least one marketable innovation per year.

A total of just under three quarters of companies affected by economic and industrial espionage over the past five years have put new products or methods on the market. In most cases, up to five innovations were created.

---

4 In Western Europe, Central and Eastern Europe, as well as in Asia and in North America.
Extent of damage

Next, the financial as well as other damage to companies affected will be presented. This is based on the medium- and long-term outlook for implications. It appears that a large portion of the companies suffered from further damage as well, ranging from a decrease in turnover to operating losses and even staff reduction.

Financial damage

Of the 59 companies affected, 35 (59%) indicated having suffered financial damage; at 24 of the companies (41%), no direct financial damage was detected.

Figure 7: Financial damage at companies affected

Distribution according to industry

Companies from almost all industries documented financial damage due to at least one instance of espionage. According to companies from the construction industry, transportation and storage services, the financial and insurance sector, and from real estate, they were affected by espionage but without any financial loss.

Predominantly, losses of up to €100,000 were recorded. Losses from €1m to €5m affect two companies from manufacturing and one company each from hospitality and administrative and support services. Losses of over €5m were assessed in accommodation and food service. In all, three industrial firms identified damage of over €10m: two manufacturing companies and one from electricity, gas, steam and air conditioning supply.

Distribution based on enterprise size

- Of the 16 micro-enterprises [up to 9 employees] affected, the greatest financial losses add up to €100,000 (14 companies have up to €50,000, and two companies up to €100,000).
- Damage of up to €500,000 occurred at a total of four small enterprises with up to 49 employees [two companies suffered up to €50,000 and one had between €100,000 and €500,000].
- Financial damage at middle-sized enterprises [having up to 249 employees] is distributed as follows: at four out of nine middle-sized enterprises, financial damage of up to €50,000 occurred; at two companies, up to €100,000; and at one company each, damage occurred in the amounts of €500,000 to €5m and over €10m.
- The greatest financial damage is to be found at six large enterprises [with over 250 employees]. One company affected adds its financial losses up to €50,000; two up to €100,000; two more up to €5m; one up to €10m; and one up to over €10m.
Possible implications: damage critical to business

Besides financial damage, often other losses are suffered. This is confirmed by the experience of 42 out of 59 companies affected (71%): they suffered, above all, loss of customers (38%), loss of contracts (34%) and damage to their reputation or to the company’s image (30%).

Figure 8: Critical damage to companies affected

Out of 59 companies
- 42 companies suffered other damage
- 17 suffered no other damage

Loss of customers: 37.5% (12)
Operating losses: 34.3% (11)
Damage to reputation: 30.4% (10)
Other damage: 18.8% (6)
Staff reduction: 11.1% (3)

As points of origin, Austria and abroad tied

Just over half of the companies affected suspect that the espionage attacks originated from abroad. Close to half of the companies affected assume that the espionage had its origins in Austria.

Figure 9: Espionage attacks’ suspected origin

Out of 59 companies
- 52% (30) in Austria
- 48% (29) abroad
According to the BVT [Federal Office of State Protection and Counterterrorism], economic espionage is defined as the targeted seeking of trade or business secrets (industrial secrets) of domestic companies or research institutions in order to strengthen the economy of another country. In conjunction with the interpretation of § 124 StGB [sec. 124 of the Austrian penal code], reconnaissance of trade or business secrets to the benefit of another country, as “economic treason”, espionage attacks from abroad constitute not only a danger to the competitiveness of individual companies affected, but also to the entire Austrian economy.

On the other hand, domestic espionage attacks on Austrian companies are to be seen from a competition law perspective, because classic competitive espionage (industrial espionage) by an Austrian competitor decreases the competitiveness of the company attacked, and can lead to its being totally ousted from the market.

In terms of the damage that occurs, the line between economic and industrial espionage may be irrelevant to a company affected, but is important when it comes to options for [criminal] prosecution. Jurisdiction of the authorities, the burden of proof, and the company resources required are all associated with it. However, the origin is seldom immediately locatable when a case of espionage comes to light at a company.

**Competitors suspected almost half of the time**

**Figure 10: Offenders**

- **Competitors** 45.7% (27)
- **Employees** 12.5% (9)
- **Origin unknown** 10.2% (6)
- **Intelligence agencies** 10.2% (6)
- **Customers** 8.5% (5)
- **Suppliers** 8.5% (5)
- **Other** 1.7% (1)

n = 59
Criminal acts

On average, one to two criminal acts per company affected were reported. Hacker attacks on IT systems or other equipment were most frequently cited. A third of companies affected also mentioned flow of information (customer/supplier), followed by disclosure of information by employees.

Of note is that most of the criminal acts are not of a technical nature, but rather require the direct intervention of humans (in a total of 71.2%, as opposed to 58.2% of the cases).

Table 4: Criminal acts committed at companies affected

<table>
<thead>
<tr>
<th>CRIMINAL ACT</th>
<th>PERCENTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow of information (customer/supplier)</td>
<td>33.2 %</td>
</tr>
<tr>
<td>Disclosure of information by employees</td>
<td>14.4 %</td>
</tr>
<tr>
<td>Social engineering attacks</td>
<td>12.8 %</td>
</tr>
<tr>
<td>Theft of information media</td>
<td>10.8 %</td>
</tr>
<tr>
<td>Surveillance or interception of communication</td>
<td>13.6 %</td>
</tr>
<tr>
<td>Hacker attacks on IT or other equipment</td>
<td>44.6 %</td>
</tr>
<tr>
<td>Other</td>
<td>12.8 %</td>
</tr>
<tr>
<td>Number of criminal acts (ø)</td>
<td>1.4</td>
</tr>
</tbody>
</table>

n = 59, multiple answers possible

Peculiarities: criminal acts according to enterprise size

Table 5: Criminal acts carried out according to enterprise size

<table>
<thead>
<tr>
<th>CRIMINAL ACT</th>
<th>EMPLOYEES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 TO 9</td>
</tr>
<tr>
<td>Hacker attacks on IT or other equipment</td>
<td>19.1 %</td>
</tr>
<tr>
<td>Surveillance or interception of communication</td>
<td>29.8 %</td>
</tr>
<tr>
<td>Theft of information media</td>
<td>14.2 %</td>
</tr>
<tr>
<td>Social engineering attacks</td>
<td>2.6 %</td>
</tr>
<tr>
<td>Disclosure of information by employees</td>
<td>2.0 %</td>
</tr>
<tr>
<td>Flow of information (customer/supplier)</td>
<td>26.7 %</td>
</tr>
</tbody>
</table>

n = a total of 59 companies; data weighted, more than one answer possible
Austria and abroad as origin of espionage attacks

Analysis of the espionage attacks named according to the criminal act’s point of origin showed that attacks on Austrian companies from abroad occur significantly more often by way of hacker attacks on IT or other equipment. In contrast, criminal acts which, according to companies, originate domestically are mostly through flow of information (customer/supplier). In addition, due to multiple answers being possible, it is also appears that often, various criminal acts are combined (domestically, on average 1.55; from abroad, 1.3).

Figure 11: Criminal acts that originated from Austria or abroad

<table>
<thead>
<tr>
<th>Category</th>
<th>Austria, n = 27</th>
<th>Abroad, n = 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow of information (customers/suppliers)</td>
<td>48.3%</td>
<td>18.8%</td>
</tr>
<tr>
<td>Hacker attacks on IT or other equipment</td>
<td>28.3%</td>
<td>60.9%</td>
</tr>
<tr>
<td>Disclosure of information by employees</td>
<td>21.7%</td>
<td>10.9%</td>
</tr>
<tr>
<td>Surveillance or interception of communication</td>
<td>16.7%</td>
<td>14.0%</td>
</tr>
<tr>
<td>Theft of information media</td>
<td>16.7%</td>
<td>7.8%</td>
</tr>
<tr>
<td>Other</td>
<td>13.3%</td>
<td>1.6%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>10.0%</td>
<td>15.6%</td>
</tr>
</tbody>
</table>
Notification of authorities and subsequent measures

Around three quarters of the companies affected notified no authorities after occurrence of an espionage attack. Only almost a quarter of the companies contacted the authorities. In six instances a police station\(^5\) was contacted; in four, the public prosecutor’s office; in three cases, the federal or provincial criminal intelligence service; in two, the BVT [Federal Office for State Protection and Counterterrorism] was contacted directly. In five instances, “other authorities” were reported to.\(^6\) On average, one to two different authorities were notified per instance of espionage.

\(^5\) In practice, reports are referred by police stations, which are often the first point of contact for companies, to the BVT according to jurisdiction.

\(^6\) The Austrian Economic Chambers, attorneys, and telecommunications authorities were listed; the Abwehramt des Österreichischen Bundesheeres [Austrian Army’s Counterintelligence Service] was not listed by any of the companies affected.

Here it is clear that the widely-claimed fear of loss of reputation is not a decisive factor in whether the authorities are notified. Instead, low expectations regarding [criminal] prosecution as well as lack of evidence against the offender constitute the most important reasons why no authorities are contacted. Apparently, companies affected see little point in notifying authorities, as in many cases the current legal framework offers insufficient prospects.

The more often a company is affected by espionage, the less often the authorities are notified. After the second instance, the willingness of companies affected to notify authorities drops considerably. This could account for the data regarding the generally low expectations for a conviction and the lack of evidence against offenders.

In most cases, after few instances, organisational measures are put in place, and after repeated attacks, willingness to implement technical measures increases.

\[Figure 12: Reasons why no authorities were notified after an instance of espionage\]

- Lack of evidence against the offender: 58.2%
- Low expectations for a conviction: 45.1%
- Lack of trust in law enforcement authorities: 28.4%
- Uncertainty as to whether espionage is a criminal offense punishable by law: 23.7%
- Fear of loss of reputation: 13.7%
- Other (e.g. “bad experience with judicial authorities”): 7.9%

n = 59, multiple responses possible
RISK ASSESSMENT BY COMPANIES NOT AFFECTED

Widely differing expectations of potential effects

In the survey, out of the 1,090 companies not affected, almost three-quarters (773) believe that they will continue to remain unaffected by espionage.

Figure 13: Assessment of risk in the next five years

n = 1,090

The remaining 317 companies (29%) assume there is danger in this regard, and of those, just under half anticipate one instance of espionage at their company; more than a third of the companies believe that they will be attacked at least five times.

Figure 14: Risk assessment (of occurrence in the next five years) grouped by province

n = 317
**Potential threat:** 60% of the companies not affected to date assume that the greatest potential threat comes from the competition; 13% list their own employees; nearly 8%, intelligence agencies, followed by customers, suppliers and others (especially IT, hackers, former employees, terrorism and suppliers).

Still, 5.5% (mentioned 60 times) assert that there is no potential threat at all.

**Potential origin:** domestic or from abroad? Two thirds of the companies unaffected to date would expect an espionage attack to originate domestically, while one third would expect it to come from abroad. 7

**Crimes expected:** Of the 1,090 companies not yet affected, over 20% of them believe that they would most likely be affected by hacker attacks on their IT systems or other equipment; over 20%, by the flow of information (customer/supplier). Around 15% suspect that their company would be affected by disclosure of information by employees; around another 15%, by surveillance or interception of communication; and approximately another 15%, by theft of information. Almost 12% guess that they could be affected by social engineering attacks.

**Estimated extent of damage**

**Financial damage:** Almost 60% of the companies surveyed who have not yet been affected believe that no financial losses would occur at their companies during an espionage attack, whereas over 40% would expect financial losses.

Of the companies that expect financial damage due to a potential espionage attack, around two-thirds of them estimate it to total up to €100,000; around 16%, up to €500,000; some 7%, up to €1m; 8% up to €5m, and around 2% each, up to €10m and over €10m.

**Damage critical to business:** Of the 1,090 companies not affected, 763 (70%) believe that they would suffer at least one loss critical to their business during an espionage attack. Above all, they expect loss of customers and operating losses, as well as damage to their reputations. Staff reduction or other damage such as fraudulence or other interpersonal conflicts were hardly mentioned.

**Possible notification of authorities**

Regarding the question placed to those companies not yet affected as to whether they would notify the authorities in the case of an espionage attack, three quarters answered “most likely”. Most of them would inform the closest police station or the regional or federal criminal intelligence service. Few companies would call in the public prosecutor’s office, the Federal Agency for State Protection and Counterterrorism or the Abwehramt des Österreichischen Bundesheeres [Austrian Army’s Counterintelligence Service], nor other authorities such as the Austrian Economic Chamber, the Chamber of Labour, the Ministry of Health, the Financial Market Authority, or a lawyer.

Of the companies that would not notify the authorities in the case of espionage, almost 40% reason that they would not have enough evidence against suspected offenders. Approximately a third has low expectations for a conviction. These assessments basically match up with those of the companies who have actually experienced an espionage attack [see page 23].

Furthermore, a “lack of trust in law enforcement authorities”, uncertainty as to whether espionage attacks are punishable by law, and fear of potential loss of reputation were cited. In two instances, companies indicated not being aware of any suitable authority to report espionage attacks to.

---

7 There were a total of 678 responses to this question.
PREVENTIVE MEASURES

Acquaintance with authorities and collaboration

At the time, according to those surveyed’s responses, only 4% collaborate with or are in contact with authorities in charge of economic and corporate espionage (mentioned 36 times). Out of those, almost all of them are satisfied with the collaboration. The remaining 96% of companies surveyed have no collaboration or ongoing contact with authorities.\(^8\)

Nine out of ten companies indicated that they know of no authorities that offer proactive opportunities for preventive support against economic or corporate espionage.

Corporate and security strategy

According to their own statements, the companies surveyed have room for improvement regarding tying their corporate strategy to their security strategy. A significant percentage of the companies did not answer this section, which suggests that they have no strategy. That lays bare companies' potential vulnerability to future espionage attacks. The only question which received an overwhelmingly positive answer was as to whether the current corporate strategy was under review for security risks.

Figure 15: Corporate and security strategy

<table>
<thead>
<tr>
<th>Statement</th>
<th>n = 933</th>
<th>n = 929</th>
<th>n = 852</th>
<th>n = 892</th>
<th>n = 882</th>
</tr>
</thead>
<tbody>
<tr>
<td>The current corporate strategy has been reviewed for potential security risks.</td>
<td>15.9</td>
<td>15.9</td>
<td>9.6</td>
<td>11.4</td>
<td>9.5</td>
</tr>
<tr>
<td>The company has a security strategy.</td>
<td>38.3</td>
<td>29.6</td>
<td>29.7</td>
<td>23.9</td>
<td>25.3</td>
</tr>
<tr>
<td>The company’s security strategy has been fully implemented.</td>
<td>22.6</td>
<td>21.3</td>
<td>21.9</td>
<td>23</td>
<td>23.8</td>
</tr>
<tr>
<td>Prevention of economic and corporate espionage is an element of the company’s security strategy.</td>
<td>23.3</td>
<td>33.7</td>
<td>38.7</td>
<td>41.7</td>
<td>41.4</td>
</tr>
</tbody>
</table>

Figures in percentages

Company activities

The highest possible security at companies can only be realised together with employees. Numerous measures already in place at companies today are vital to security. Referred to here are the company culture in general, satisfaction and motivation, campaigns and training, and hiring and review of new employees through to the establishment of appropriate bodies for reporting economic and industrial espionage. In the following summary, some measures and their implementation will be presented.

\(^8\) n = 1,015; 134 companies gave no response.
Those responsible for prevention of economic and industrial espionage

Almost 90% of the companies surveyed have no one responsible for prevention of economic and industrial espionage; around 12% of the companies do have their own person in charge of it.

Figure 16: Personnel management measures

- At the company there are measures that have a positive impact on the satisfaction and motivation of employees. (n = 931)
- At the company there are periodic surveys on employee satisfaction and motivation. (n = 931)
- At the company there are campaigns intended to have a positive influence on company culture. (n = 896)
- Job applicants’ CV’s are actively checked for accuracy. (n = 917)
- Job applicants undergo a background check before being hired by the company. (n = 896)
- There are campaigns for raising employee awareness in regards to information and data security. (n = 891)
- The company’s culture is measured and presented using standardised observation tools. (n = 888)
- All employees receive training on data protection. (n = 887)
- Employees who have access to sensitive information undergo routine security checks. (n = 859)
- There is a body to report suspicions of economic or industrial espionage to. (n = 858)

Figures in percentages

Those responsible for prevention of economic and industrial espionage

n = 943; no answer: 206 companies
Here a considerable difference emerges according to enterprise size: around a quarter of all large enterprises has its own person responsible for prevention of economic and industrial espionage. Only about an eighth of middle-sized enterprises employs its own person responsible for or authorised to perform this task, and less than a tenth of small and micro-enterprises has anyone.

**Systems in place and certification models**

For risk management and questions of security, there is a array of systems used. Major reasons for that are, for example, client requests, increase in competition or the ability to better control companies. Out of the companies surveyed, about every fifth one uses systems or a certification model.

**Figure 18: Use of systems or certification models**

Out of the companies that use systems or a certification model, in a fifth of the cases they use ISO 31000 risk management standards; somewhat less common are 27001 information security systems standards and the German BSI’s [Bundesamt für Sicherheit in der Informationstechnik, or Federal Office for Information Security] IT baseline protection catalog. In addition, ONR 49000 risk management standards, IT Infrastructure Library, COSO ERM [Enterprise Risk Management], ISO 9001 and other systems are used.

**Strictly confidential trade secrets and data protection**

Nearly 30% of the companies surveyed contend that 21-50% of their information consists of strictly confidential trade secrets. An equal amount regards over 51% of their information as strictly confidential.

**Figure 19: Estimation of proportion of strictly confidential trade secrets to the sum total of information at the company**
In practice, one can assume a much lower percentage of company information to be trade or company secrets capable of being appropriately protected, otherwise, the following questions would arise: how could need-to-know restrictions be organised and maintained with around 50% of the company’s information? Or, for example, how could prohibited access (physical or technical) be effectively prevented?

**Insufficient data protection?**

The companies were asked to what extent they protect their data, grant employees access, and how sensitive information is identified at their companies. At more than three-quarters of the companies, access to information is restricted on a need-to-know basis or there are restrictions to access of electronic data. At some 60% of the companies, there are restrictions to physical access, and at about half of the companies, sensitive information has been identified of whose loss would lead to great damage to their business.

**Figure 20: Data protection and access restrictions at companies**

- Employees only have access to information which they need for their work.
  - Totally agree: 39.2%
  - Somewhat agree: 38.7%
  - Somewhat disagree: 9.7%
  - Totally disagree: 12.4%

- There are restrictions to electronically-stored information.
  - Totally agree: 46.6%
  - Somewhat agree: 30.7%
  - Somewhat disagree: 6.4%
  - Totally disagree: 16.3%

- There are restrictions to physical access of areas where data is stored or processed.
  - Totally agree: 35.4%
  - Somewhat agree: 24.3%
  - Somewhat disagree: 11.8%
  - Totally disagree: 28.4%

- At the company, sensitive data has been identified of whose loss could result in great material or immaterial damage.
  - Totally agree: 21.4%
  - Somewhat agree: 28.3%
  - Somewhat disagree: 24.4%
  - Totally disagree: 25.8%

- Information accessible only to a particular group of people is identified as such.
  - Totally agree: 20.5%
  - Somewhat agree: 23.2%
  - Somewhat disagree: 23.7%
  - Totally disagree: 32.6%

- Assets worth protecting have been deemed as such and declared in writing.
  - Totally agree: 13.1%
  - Somewhat agree: 20.8%
  - Somewhat disagree: 25.9%
  - Totally disagree: 40.2%

- Where all information is to be found has been laid down in writing.
  - Totally agree: 9.0%
  - Somewhat agree: 20.5%
  - Somewhat disagree: 23.6%
  - Totally disagree: 46.3%

- Risk analyses are carried out to determine the threats and risks of unauthorised outward flow of information.
  - Totally agree: 7.8%
  - Somewhat agree: 19.8%
  - Somewhat disagree: 26.4%
  - Totally disagree: 46%

Figures in percentages
n = 930
Analysis of external sources of danger

The percentage of companies who deal with their outside world in matters of economic and industrial espionage is considerably lower: almost 30% of the companies surveyed analyse competitors, just under 20% analyse customers, more than 15%, suppliers, and less than 10%, intelligence agencies. Slightly more than two percent of the companies report analysing other individual threats such as those from IT (hackers, viruses and network threats), former and current employees.

Companies already affected keep a closer eye on their environment

The fifty-nine companies who have already suffered espionage attacks analyse external threats considerably more: 48% of them analyse both their customers and their competitors each. Suppliers and other threats (IT, current/former employees) are each analysed at around a third of the companies, and the media at around 18%. On average, companies who have already been affected analyse one to two external threats.

Often, critical quality of security measures in place

Companies are very critical in their assessment of their own efforts to date. Everyday prevention of economic and industrial espionage continues to be a stepchild. Just under 60% of the 1,149 companies surveyed think that the security measures in place at their own companies are hardly or not at all suitable.
In regards to enterprise size, clear differences emerged: according to over 60% of micro-, small and mid-sized enterprises, their own security measures are completely unsuitable or hardly suitable. At larger companies (with over 250 employees), on the other hand, the security measures are judged by almost 70% as “quite” or “extremely suitable”.

Differences according to industry

It appears that special branch-related regulations, customer demands, previous instances of espionage, and a high level of attention from the public can be quite strong in driving the introduction of security measures. Another factor is employees’ heightened awareness. In five industries, security measures adopted are prevailingly assessed as quite or extremely suitable. In the financial and insurance sector, two-thirds say so. Almost 60% of companies in the following industries say so, as well: health and social services; electricity, gas, steam and air conditioning supply; professional, scientific and technical services. And in ICT, somewhat more than half say so. In the other industries, security measures are not so positively assessed.
COMPANIES’ EXPECTATIONS

Preferred sources of information

In previous years, special interest groups responded to demand with a range of information and consulting services in cooperation with the authorities. 80% of the companies surveyed (915) want to receive more information from the authorities on the dangers of economic and industrial espionage and on possible preventive measures. Information is expected on these topics from the following institutions: Federal Office for State Protection and Counterterrorism, Ministry of the Interior, the Industriellenvereinigung, the Austrian Economic Chambers, state police headquarters, federal and state offices of criminal investigation, and the public prosecutor’s office.

40% each would prefer online information platforms and brochures; industry events were cited as well by more than 25%, and personalised advice was listed by over 18%. At 6%, information from trade fairs and conferences fell at the bottom end of the scale. Micro- and small enterprises would prefer to get information via brochures or online information platforms. Middle-sized enterprises list brochures, industry events or online information platforms; large enterprises do so as well, though they further expect personalised advice.

Desire for further research

Regarding the question as to where companies see further need for research in the area of economic and industrial espionage, two distinct dimensions were mainly named: in technology and in the area of organisation.

Statements, listed in order according to response frequency, are:

Organisation
- information for employees
- psychological training for employees/staff under stress
- copyright protection/patent rights
- balance sheets and accounting
- better collaboration of the judiciary with companies

Technology
- prevention of/defense against hacker attacks (including trojans, spam and phishing)
- IT encryption measures/protective measures (especially abroad)
- Data storage
- IT guidelines
- early warning systems
- a distinct European operating system
CONCLUSION: DEMAND FOR STRONGER NETWORKING

As the results of this study show, this topic is complex and includes company structure, organisation and management, as well as technology. Corporate activities encounter governmental support that often, for various reasons, is not sufficiently accepted. Because of heightened awareness resulting from public discussion of the issue and, partially, concrete instances of companies being affected, in future greater prevention at companies and increased collaboration with authorities and public agencies is to be expected. Stronger networking among companies and with security agencies on specially-designed platforms would contribute to that.

Broken down further, intensive collaboration among B2B companies is needed because highly specialised service companies providing their customers with a lot of [technical] know-how and involved in research and development projects of large companies could increasingly become the focus of economic and industrial espionage. Agreement on unified approaches in the business world in the form of collaboration and exchange on current practices used by economic and industrial spies could considerably increase protection of individual companies.

Intellectual property and human intelligence drive innovation. In the years to come, one can expect even greater digitalisation, automation and networking of companies. With that comes companies’ increasing dependence on the appropriate know-how for maintaining their competitiveness. As a consequence, the threat of economic and industrial espionage to these companies also increases. Progress towards Industry 4.0 should likewise be seen within this context.

The planned EU guidelines on a unified understanding of trade secrets will help to increase protection of the immaterial wealth of companies based in the EU (as a large-scale economic hub). That is a basis for social stability.
INDUSTRY DENOMINATIONS IN ACCORDANCE TO ÖNACE 2008

Agriculture, forestry, fishing
Mining and quarrying
Manufacturing
Electricity, gas, steam and air conditioning supply
Water supply, sewerage, waste management and remediation activities
Construction
Trade, maintenance and repair of motor vehicles
Transportation and storage services
Accommodation and food service activities
Information and communications technology
Financial and insurance sector
Real estate activities
Professional, scientific and technical services
Administrative and support services
Education
Health and social services
Art, entertainment and recreation
Miscellaneous services

BIBLIOGRAPHY

Verfassungsschutzbericht 2014
www.bmi.gv.at/cms/bmi_verfassungsschutz

Sicherheitsbericht 2014
www.bmi.gv.at/cms/bmi_service

Arbeitsprogramm der Österreichischen Bundesregierung
www.bundeskanzleramt.at/site/3354/default.aspx

Handbuch WIS
www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis

Struktur ÖNACE 2008:

Definition von kleinen und mittleren Unternehmen;
Empfehlung der EU-Kommission 2003/361/EG, zusammengefasst in:
This brochure, as well as other current publications are available at the Service LLC, Austrian Economic Chamber.
Telephone: 0590 900-5050
Fax: 0590 900-236
E-mail: mservice@wko.at
Internet: http://webshop.wko.at

Available online at:
http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis