SOME STATISTICS

100%

of companies identified the attempts of employees to **take corporate data** during the first months of using the company's services

100%

of employers found staff members with **asocial behaviour, drug and alcohol addicts, gamblers, have legal problems**

85% +

of organisations detected employees who **searched for a new job**

70% +

of those responsible for internal threat and corporate risk mitigation gained access to correspondence where a company's **employees, executives are talked about,** and other **insider information is discussed**

70% +

of companies found out that their employees do **non-work related activities** during work hours

70% +

of managers learned about **plotting and insider fraudulent activity**

40% +

of employers revealed that some employees spent time on **entertainment during work hours**

25% +

of companies detected **staff members** who **launched** their **business benefitting from a company's resources**

THE FOLLOWING INCIDENTS WERE DETECTED

34%

Taking data outside the network perimeter

20%

Job search

15%

Discussing employees, managers and a situation withing a company

7%

Second job

6%

Asocial behaviour, bad habits, problems with law

4%

Secret agreement with contractors, fraud

2%

Irrational use of work hours

2%

Nepotism

1%

Costly purchases and loans

1%

Illegal business

1%

Theft

1%

Health

6%

Others

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

WHAT CHANNELS DID DATA LEAK THROUGH?

65%
Copying data to a flash drive

24%
Data upload to the cloud

6%
Documents sent via email

5%
Documents sent via messengers

WHAT DATA WAS TAKEN?

27%
Customers and sales

26%
Technical data

10%
Purchases

10%
Agreements

10%
Financial

1%
Accounting

16%
Other

ASOCIAL BEHAVIOUR

65%
Drugs

12%
Gambling

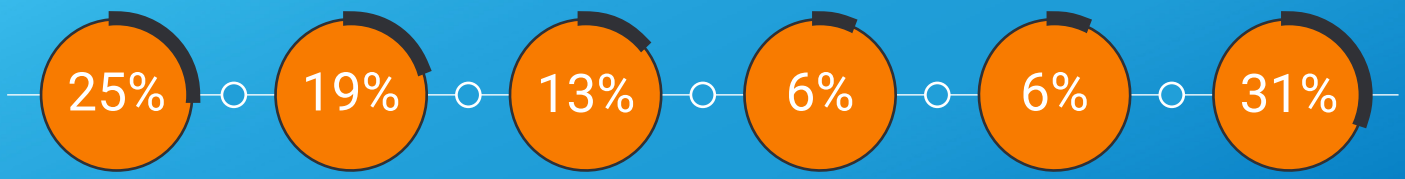
6%
Blackmail

6%
Prostitution

6%
Problems with law

6%
Alcohol

SECOND JOB OR EXTRA DURING WORK HOURS



25% Accounting

19% Adjacent scope

13% Activities not related to a company's scope

6% Business training

6% Design

31% Other

WHAT DO EMPLOYEES DISCUSS?

44%
Management

18%
Work and processes

18%
Colleagues

12%
DLP

9%
Facts an employer isn't aware of

SOME SPECIFICS

CASE

Industry: government
Time to discover an issue: 1,5 weeks

Number of staff members: 1500
Number of incidents detected: 14
Number of violators identified: 8 (30%)

WHAT WAS DETECTED?

1. Unreliable lawyer

A lawyer was looking for vacancies in other companies and spent a few work hours enjoying online entertainment: it took him 2 hours daily watching videos on youtube, and about 1.5 hours communicating on social networks. He also spent time on dating websites, where he offered women dating for money. Moreover, the episode of blackmail was detected: he threatened to post an intimate video of the woman with whom he talked on some social network if she wasn't going to do what he told her to. Even if he didn't consider the job offers from other employers, his employment at this organisation would be terminated.

2. Leak for a flat

An employee was spotted printing documents for internal use. Later she received a letter from her bank to her personal email box about a loan. It was likely that those events were related and that employee promised someone secret information in return for a remuneration that would help her solve the issue with a flat.

This is not the only detected attempt to leak information: other employees tried to send documents to personal email and copy them to a flash drive.

3. Employee with problems

It was revealed that one of the employees was in a difficult financial situation and took a loan for an apartment. Such employees are more likely than others to share secret data with third parties or quit their job looking for a higher salary. It also turned out that the employee had a conflict with her husband, who was under investigation, blaming her and threatening her. However, she was writing positive characteristics for him on her behalf and on behalf of their neighbors. The employee was manipulated by her spouse and needed money, which could lead to committing a crime involving sensitive data, and such employees should be taken under special control to prevent information leakage.

There were also discovered such facts as:

Discussing new managers, negative opinion about executives in correspondence, searching information about new managers on the Internet, sending corporate documents to a personal email box, receiving emails to a personal email box from a bank about a loan, uploading personal documents to a flash drive.

STATISTICS ON SPECIFICS

CASE

Time to discover an issue: 1,5 weeks

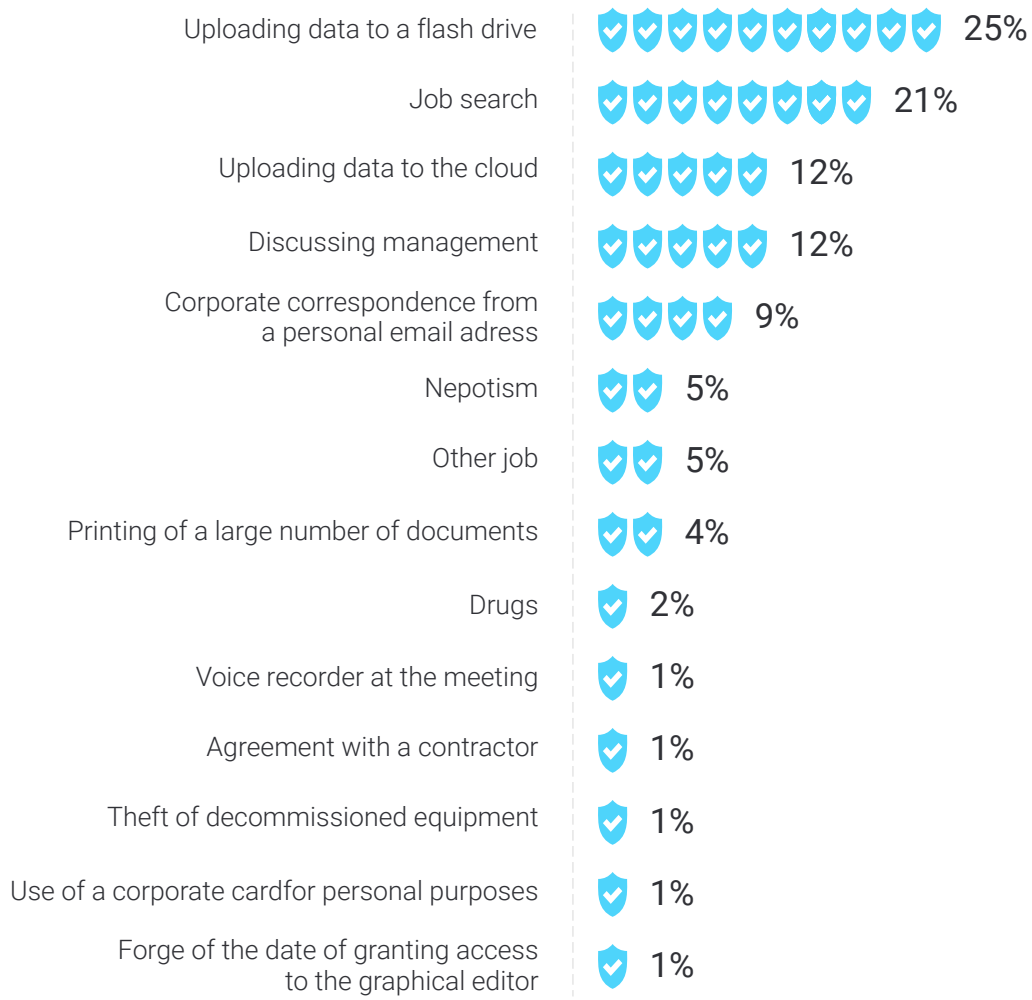
Number of staff members: 150

Number of incidents detected: 131

WHAT WAS DETECTED?

- **Every third** employee **uploads corporate data** to a flash drive or to the cloud
- **Every fifth** employee is **looking for a job**
- **Every fifth** employee **conducts unacceptable correspondence** using a personal email address or sharing negative opinion about top management

ALL INCIDENTS



SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT