Incident investigation:

Case study

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

DRUG DEALING WITH THE HELP OF A LOGISTICS COMPANY'S TRANSPORT

What happened: The policy containing a drug dictionary worked – the messages of the top manager on social networks obviously contained a code word and a car number plate details.

Investigation: It turned out that the codes were the car numbers from the corporate car park. HR Director smuggled drugs covering country's regions.

An IT specialist mirrored the top managers' email

I'll just have a look...

What happened: An IT specialist activated an additional email in a corporate mail. The letters of two top managers – chief commercial manager and CEO – were "mirrored" to his mailbox.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

Investigation: It turned out that direct competitors had access to the email box. They knew about every step and strategic decision of the company's management.

Top management email.

An employee's illegal activities in the workplace

"It started with...": Disposing acid is a paid job in production. An employee who was responsible for this was taken under control.

Investigation: it was discovered (via WhatsApp) that he was adding 5 extra tons, and because of this, the organization was losing $1000 during every deal.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

Made money on acid.

ILLEGAL BUSINESS IN A DESIGN & ARCHITECTURE COMPANY

What happened: It was revealed that one of the employees saved a draft of a corporate charter of another company in his email box.

Investigation: It turned out that this email was used by the specialist and his two colleagues. They launched a competitor company and lured customers away offering them better terms and conditions.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

Senior manager requested to hire an assistant

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

1.

4 out of 8 working hours

2.

3.

4.

6 out of 8 working hours

5.

EMPLOYEE PLOTTING AGAINST TOP MANAGEMENT

What happened: an employee is dissatisfied with the bonus system, relations with superiors are aggravating. A specialist took him under control.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

Investigation: Skype correspondence was captured and it was clear that the employee began to plot against the leadership and influence the opinion of colleagues. The company dismissed the provoker.

KICKBACKS DURING 12 YEARS

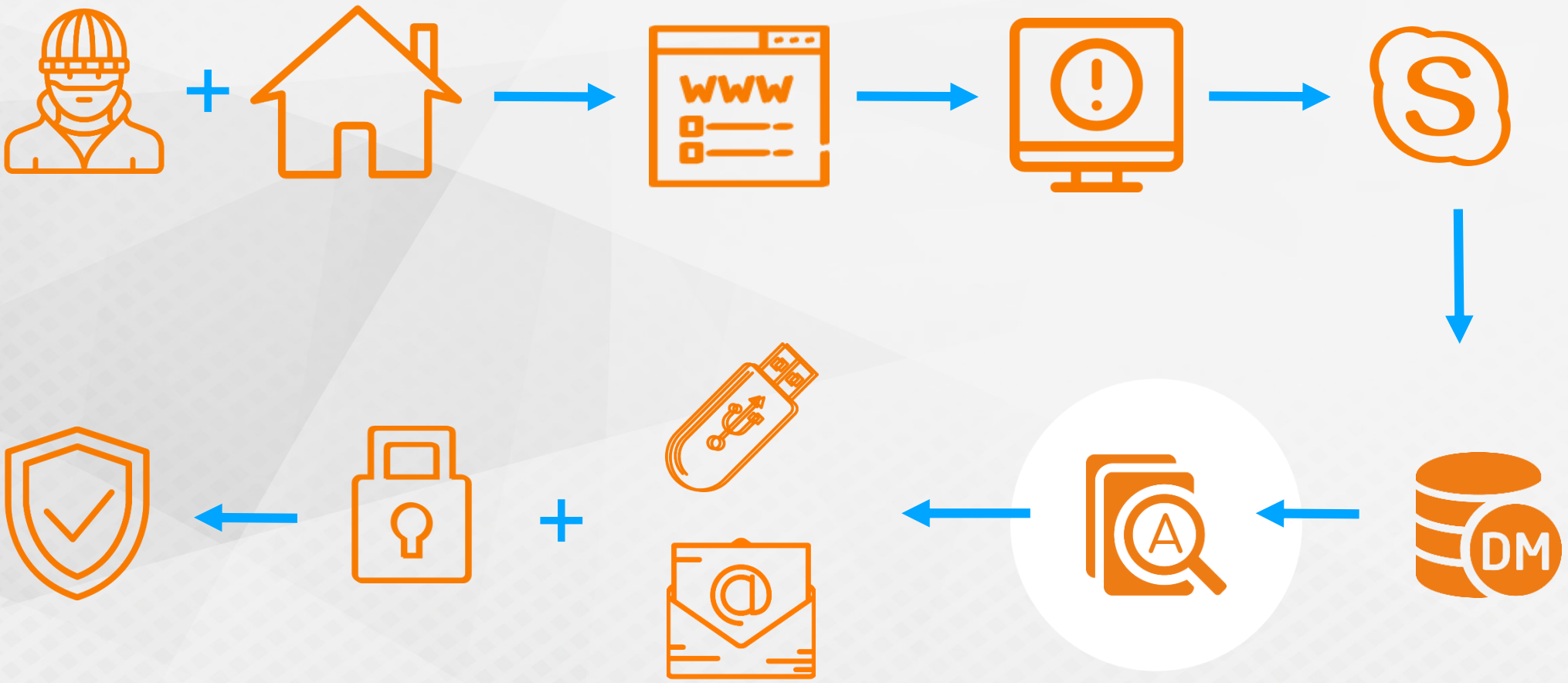
What happened: after a DLP installation, it turned out that the regional CEO and his subordinate took kickbacks.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

Investigation: analysis of data from MicrophoneController, retrospective analysis and clients' commentary revealed that the two were taking kickbacks during 12 years. The amount of kickbacks increased up to $ millions. Both pled guilty - they were fired.

The system identified a user who was visiting a suspicious website

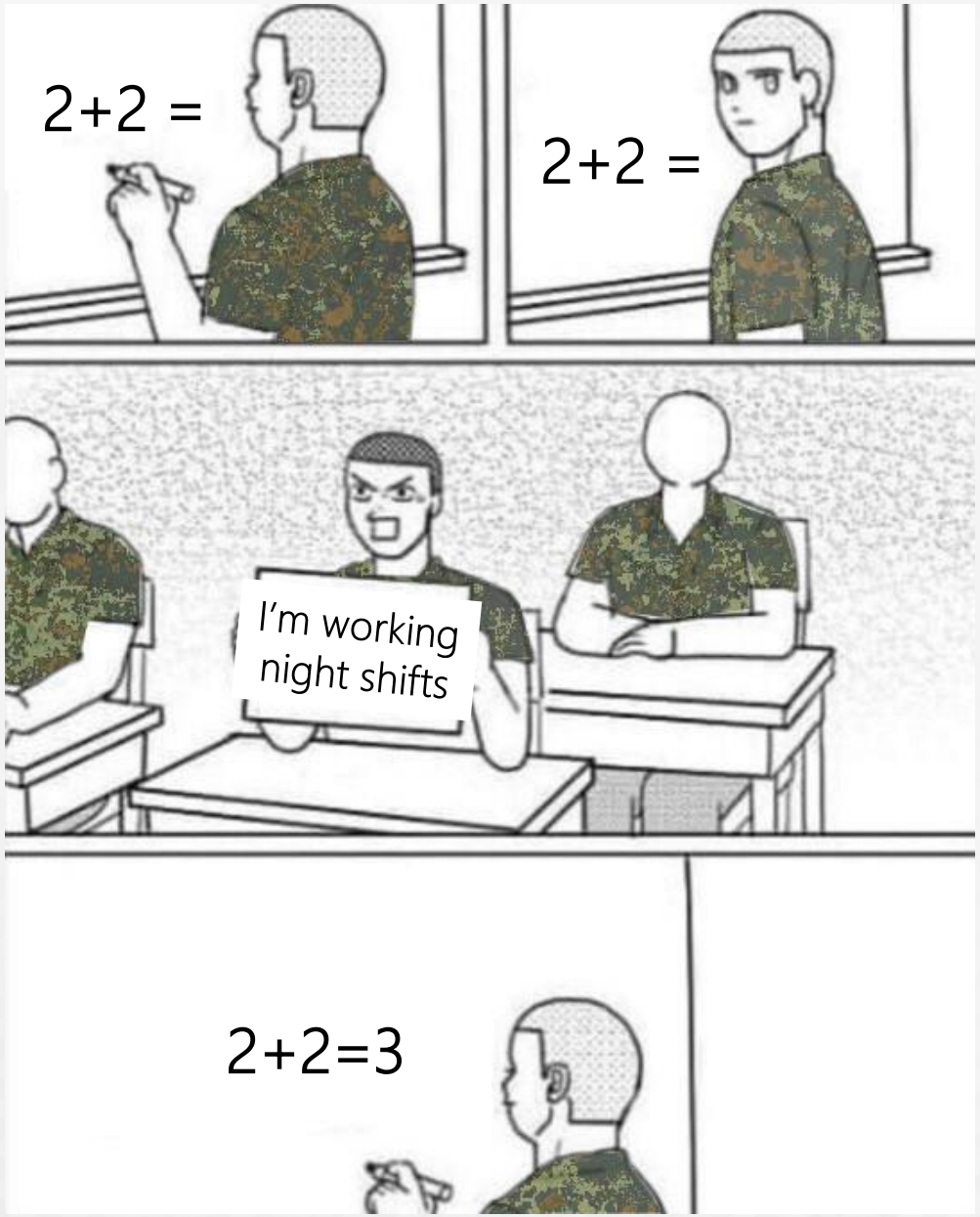
SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT



THE THEFT WITH THE HELP OF A FAKE INVOICE

What happened: pipes were stolen from the metallurgical production. The company lost $97-120 thousand a month.

Investigation: the scheme was discovered when duplicate invoices were found: one for 3, the other – for 4 pipes. 4 pipes were transported through the control, one was unloaded during the transportation, and the client received only 3 pipes.



EMPLOYEE PAWNED HIS BELONGINGS

What happened: DLP detected that the employee visited a pawnshop online.

Investigation: the employee turned out to check the information about the mortgages and loans. Further investigation revealed that he had financial problems due to the fraudulent activity at his previous job.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

EMPLOYEE ACCESSED COMPUTER OF HIS NEGLIGENT COLLEAGUE

What happened: a security policy for classified document copying alerted to a violation. The account owner denied involvement in the incident.

Investigation: it turned out that the employee didn't lock the computer, another employee inserted 2 flash drives and downloaded the documents from one to the other. The audit of the device identified the owner of flash drives. Both employees were punished.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

WORKING DURING THE WEEKEND

What happened: employees of the project department volunteered to work overtime during the weekend a few weeks. Reports showed them being active working with task-related applications and productive.

Investigation: close monitoring revealed that the employees spent part of the time preparing someone else's project. They used the company's confidential data. The cost of a third-party project amounted to $415 000.

PART-TIME JOB AT THE UNPROFITABLE INSURANCE OFFICE

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

What happened: the remote branch of the insurance company has been unprofitable for a long time. The specialist responsible for information security had to resort to extra supervision.

Investigation: the MicrophoneController module was configured to record speech every time the employees would begin to calculate the cost of the policy. It turned out that one of the agents was selling policies **after** an insured event would occur. The annual losses of the office were about $16 000.

THEFT FROM THE CASH-DESK: RETROSPECTIVE INVESTIGATION

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

What happened: several tens of thousands of dollars were stolen from the cash-desk of a manufacturing and trading company. There were no signs of hacking, it was an employee who committed the crime.

Investigation: 3 people had access to the cash-desk. After installation of the DLP and checking emails company found out that the cashier's son had large arrears and he was threatened with physical harm. The employee, his mother, appeared to be a thief.