SEARCHINFORM
INFORMATION SECURITY

INFORMATION SECURITY

[Guide for protecting your company against insider threats]

CONTROL OF EMPLOYEES

2017

INTRODUCTION

We have accumulated the experience of the clients of SearchInform and identified typical risks and subtle threats, including data leakage and insider activities, with which IS specialists have to deal on a daily basis.

According to the survey of IBM and Ponemon Institute (2016), during which the experts interviewed 2,000 IT and IS specialists from the USA, UK, France, Germany, Australia, UAE and Brazil, human factor played a crucial role in 74% of the incidents.

The user who accesses the data on a corporate network represents the most likely insider threat. In this document, we will concentrate on potentially dangerous actions of employees and different prevention measures for the incidents connected with user behavior. The recommendations are provided with the information security cases of the companies from different business areas.

COMMUNICATION WITH COMPETITORS

The competitors of a company poach experts, bribe employees to make them spy or cause them to leak information via blackmailing.

In order to detect a threat at the negotiation phase, it is necessary to control the communication of the employees with external addressees through all possible channels:

- Corporate mailbox
- Personal mailbox, the one that an employee uses on his/her work computer
- Social networks
- Messengers
- Skype and other similar applications

WHAT SHOULD YOU CHECK PRIMARILY?

In the mail, you should search for messages sent or received from a mailbox on a competitor's corporate domain (xxx@competitor.net).

In the correspondence of an employee, regardless of methods of communication, you should look for references to the name of a competing company and your own projects / products that may be of interest to a competing company.

CASE: COMMUNICATION WITH COMPETITORS

Entry: Construction company, current security control using DLP system.

Case description: An employee working in the Tender Department of a company received a message on Facebook from a competitor's specialist with an offer to meet and discuss "some common issues".

INCIDENT INVESTIGATION AND PREVENTION:

The employee was on the list of the risk group because of debts, therefore she was under control of the IS Department. She took out a mortgage to buy a flat and a loan for home improvement, and often discussed her financial problems with colleagues and friends on the Internet.

The IS Department suggested monitoring the employee, because the competitor could learn about the situation and use it as a lever of pressure. The observation confirmed the hypothesis: the competitor promised the employee to repay the loan in exchange for the information about a tender. Due to such a proactive approach, the IS Department managed to prevent the debtor from submitting confidential data.

NEW JOB SEARCH

An abrupt firing of an employee jeopardizes the work processes of a department or entire company, depending on the employee's position in the corporate hierarchy.

It is recommended to take into account activities in web browser, email correspondence and communication via messengers to insure a company against such surprises.

The first step is to find out which one of the employees visits employment sites. DLP tools allow creating a group in which the system will automatically distribute online resources with vacancies and notify an IS specialist about activities on such sites.

> *PLEASE NOTE: It's not worthwhile to include in monitoring the employees who are engaged in recruitment and use employment sites as a working tool.*

The second step is to check which one of the employees receives mailings from www.indeed.com, www.upwork.com, www.job-hunt.org and other employment sites and / or sends out a resume.

Employees who hide the intention to change the job often come up with tricks and change the name or extension of the file to give out a resume for a different document. Therefore, it is important to use search tools that analyze the content of sent documents against key phrases. As search queries you can use standard phrases from a resume, for example, "work experience", "job duties", "personal skills", "additional information."

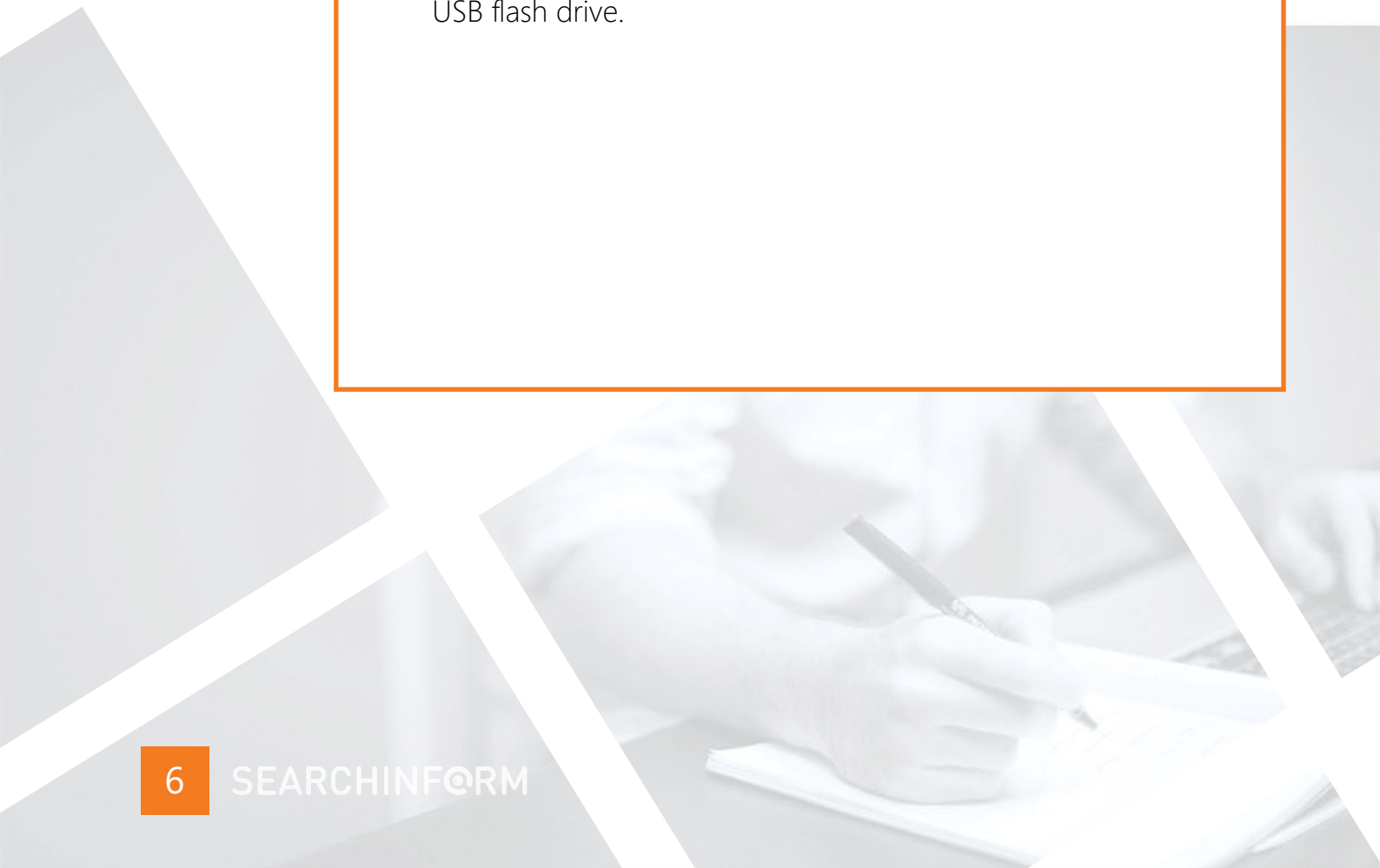
CASE: NEW JOB SEARCH

Entry: Consulting company; current security control using DLP system.

Case description: The IS Department found out that an employee was monitoring vacancies on employment sites and received invitations to job interviews from competitors. The employee was taken under control.

INCIDENT INVESTIGATION AND PREVENTION:

After receiving another invitation, the employee began to copy working documents (several thousand files, including commercial secret) to a USB flash drive. Using a DLP system, the IS Department encrypted all the copied information to make reading impossible. The employee was immediately deprived of the access rights. The departure clearance checklist was signed only when the IS Department got the USB flash drive.



GAMBLERS, DEBTORS, ADDICTS AND OTHER RISK GROUPS

In any team, there are potentially dangerous employees – debtors can steal to redeem a debt, alcoholics and other addicts can fall back into old habits and let their colleagues down. People from risk groups are often victims of blackmail: being under pressure, they choose to commit crimes in order to keep personal secrets.

The tool for identifying and controlling such employees is the search with dictionaries on various subjects. For example, to search for drug addicts, a DLP system will check the intercepted information for the names of addictive substances and slang related to drugs. To find gamblers, the system will monitor the discussions of games and the relevant vocabulary. There is a thematic dictionary for each risk group.

The effectiveness of monitoring is increased by the phrase search, for example, when you use the search by words and phrases indicating the discussion of loan payments searching for debtors. You should search for incidents in mail correspondence and instant messengers, excluding spam and attachments.

Within the framework of policies, it is also appropriate to control the hits of topical websites – online casinos and online bookmakers, dating website for people of non-traditional orientation, etc.

CASE: GAMBLERS, DEBTORS, ADDICTS AND OTHER RISK GROUPS

Entry: Transport company; current security control using DLP system.

Case description: A competitor began to entice customers systematically at the stage of signing agreements. The IS Department of a company also drew attention to the changed behavior of one of the top managers.

INCIDENT INVESTIGATION AND PREVENTION:

An in-depth analysis and notification of the violation of security policy used to identify relations between colleagues showed that a married top manager was intimate with one of the employees who got pregnant.

The employee herself would actively communicate on social networks with an employee from a competing company. The IS Department suggested that having learnt about the "skeleton in the closet", the competitors decided to blackmail the top manager and forced him to leak data. To test the hypothesis, the top manager was told deliberately false information about the upcoming transaction – and the competitors really took advantage of this.

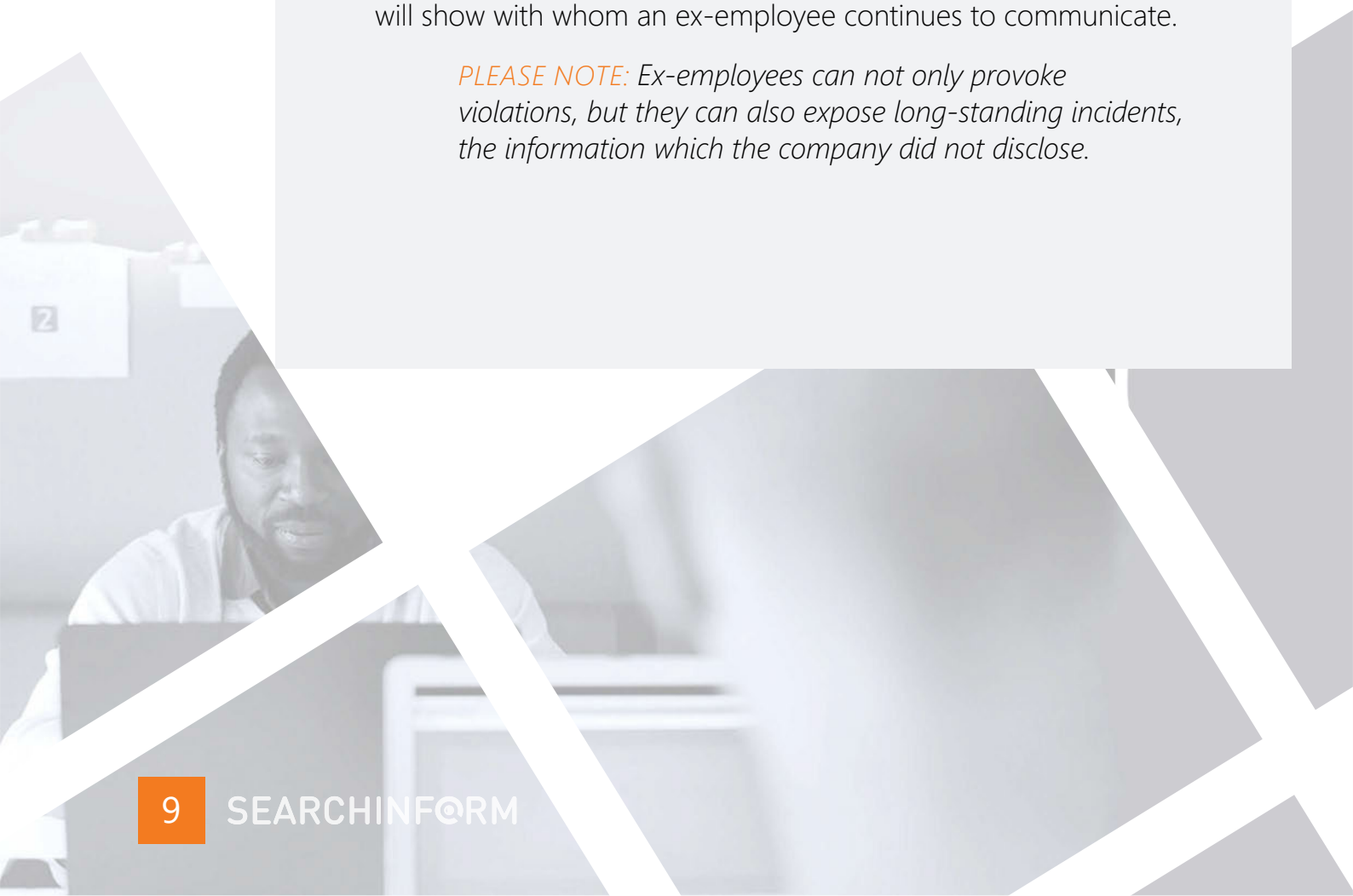
COMMUNICATION WITH EX-EMPLOYEES

Ex-employees, especially those who left with a scandal or went to competitors, often try to find out confidential information through ex-colleagues with whom they maintain friendly relations. Control of correspondence between current employees and ex-employees will ensure protection from "friendly" leaks.

To detect the chain of letters, where the sender or the addressee is an ex-employee, you will need his/her personal e-mail. If the ex-employee was prudent enough and never used personal email at work, the resume of this employee will be useful for finding the right email. Usually candidates write up-to-date information for communication.

There is a similar approach to the search for suspicious correspondence via Skype, ICQ, Viber and other communication channels. Filtering by the sender / the addressee of the messages will show with whom an ex-employee continues to communicate.

> *PLEASE NOTE: Ex-employees can not only provoke violations, but they can also expose long-standing incidents, the information which the company did not disclose.*



CASE: COMMUNICATION WITH EX-EMPLOYEES

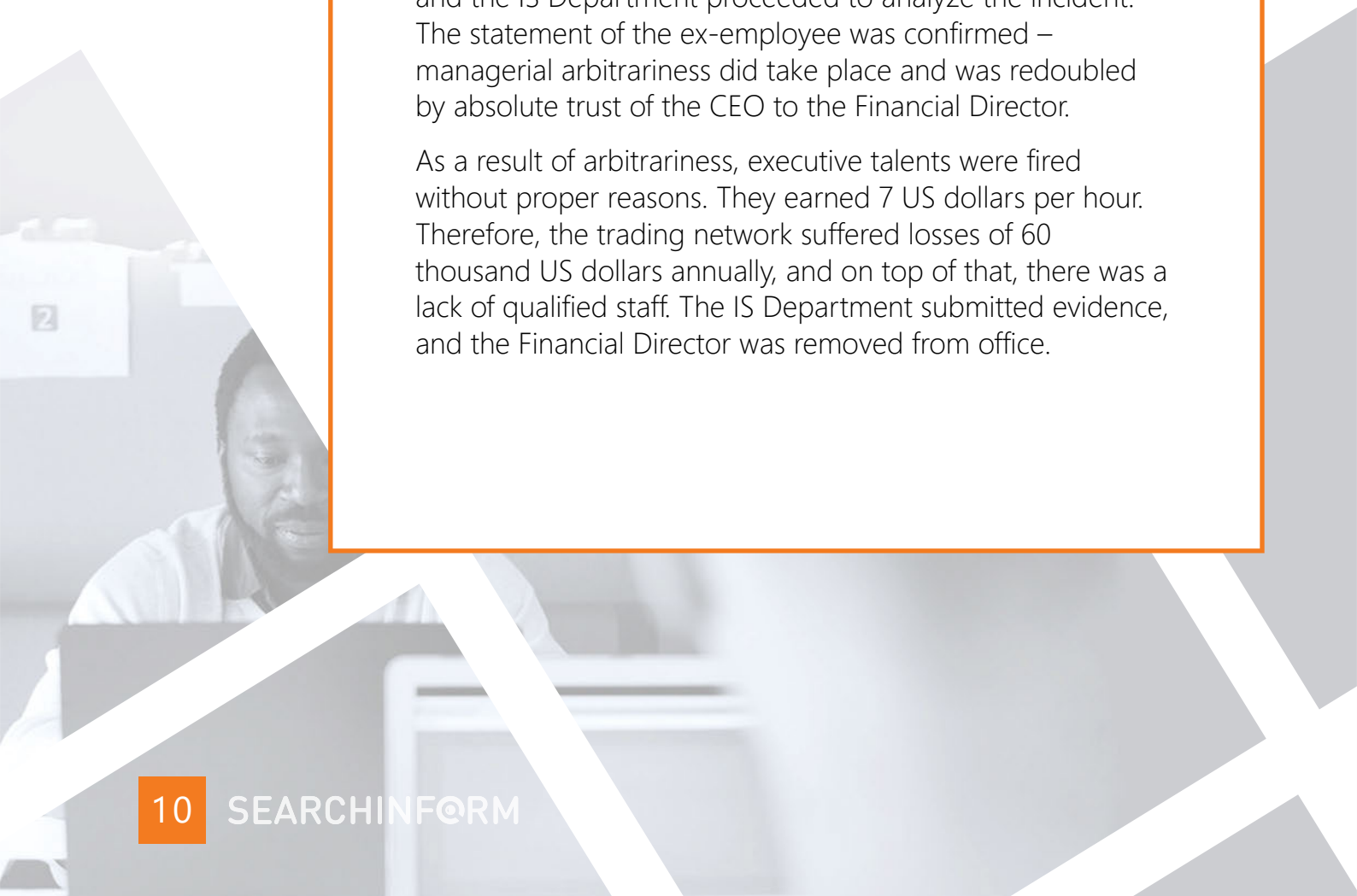
Entry: Supermarket chain; DLP system testing.

Case description: DLP system intercepted a letter that the Financial Director received from a dismissed employee. In this letter the ex-employee accused the Financial Director of arbitrariness. In addition to emotions, the letter contained references to people who were fired not for violation of employment obligations, but simply at the request of the top manager.

INCIDENT INVESTIGATION AND PREVENTION:

The information was reported to the CEO of the company, and the IS Department proceeded to analyze the incident. The statement of the ex-employee was confirmed – managerial arbitrariness did take place and was redoubled by absolute trust of the CEO to the Financial Director.

As a result of arbitrariness, executive talents were fired without proper reasons. They earned 7 US dollars per hour. Therefore, the trading network suffered losses of 60 thousand US dollars annually, and on top of that, there was a lack of qualified staff. The IS Department submitted evidence, and the Financial Director was removed from office.



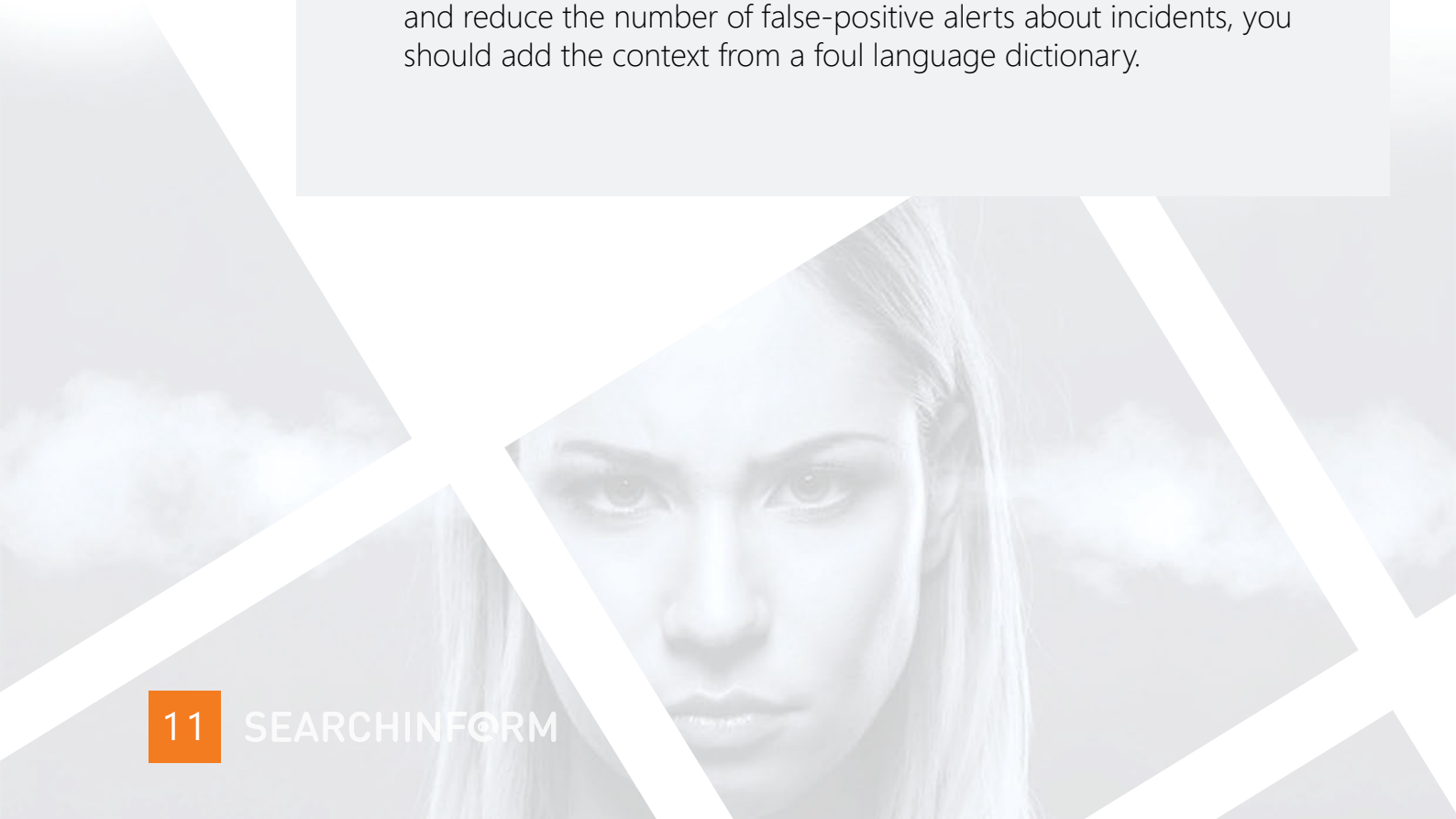
NEGATIVE OPINION ABOUT TOP MANAGEMENT OR BUSINESS PLANS

Disloyal employees are automatically included in the risk group, they pit staff against top management, damage your company's online corporate reputation, delete, forge, leak or steal company documents. When it comes to the global changes in the company, rebels can provoke a mass exodus of employees.

To monitor the mood of your team and to detect disloyal employees in time, you have to include the following items in the search criteria:

- Job titles of managers and top managers
- Full names of top managers and their nicknames
- Common words and slang phrases indicating top managers, for example, "boss", "top", "biggie", "bigwig", "foreman", "master", "head", "leader."

To exclude neutral and positive statements from the search results and reduce the number of false-positive alerts about incidents, you should add the context from a foul language dictionary.



CASE: NEGATIVE OPINION ABOUT TOP MANAGEMENT OR BUSINESS PLANS

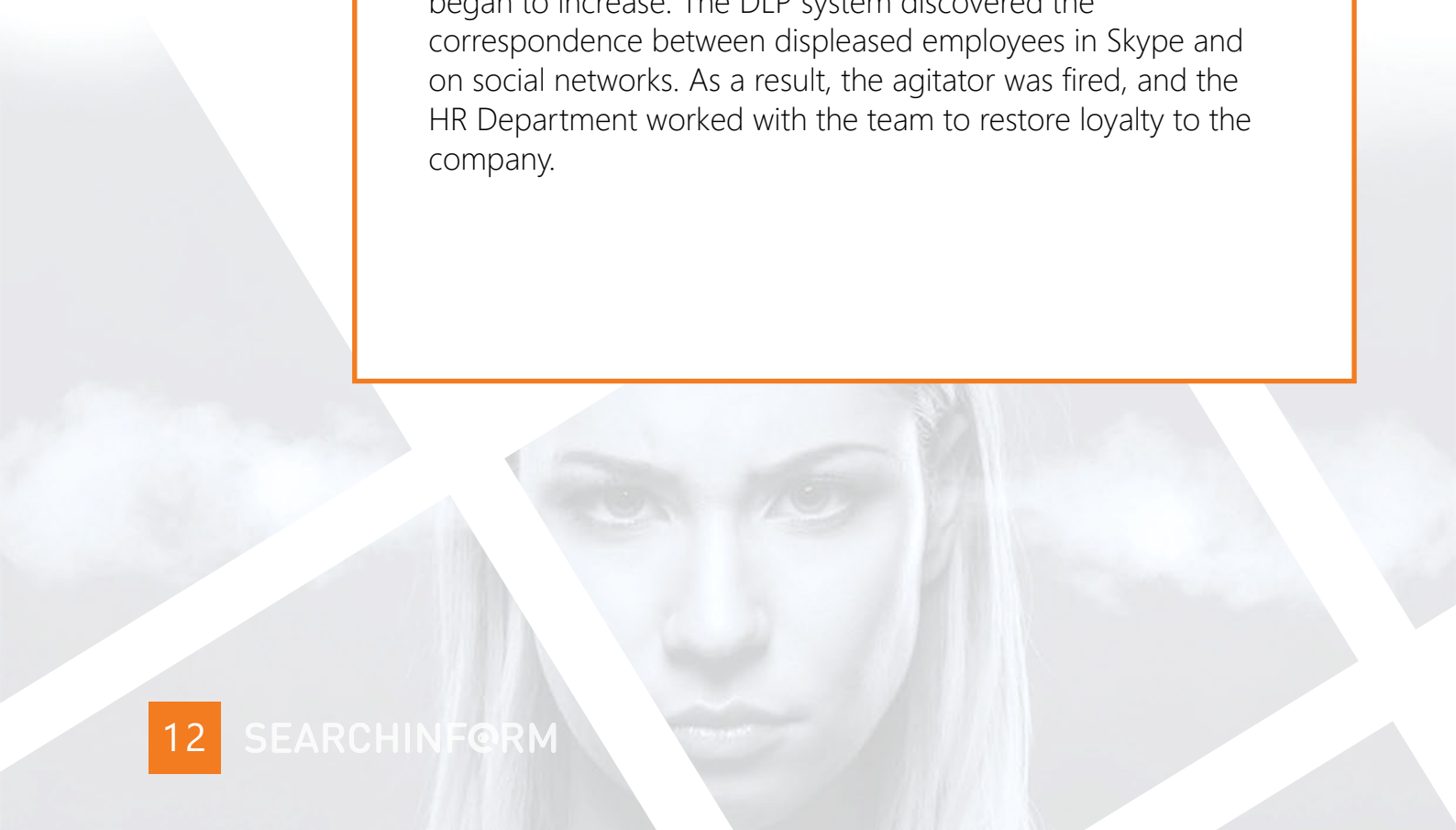
Entry: Product company; DLP system testing.

Case description: The system showed the correspondence between colleagues in which one of the employees was outraged by the incentive system and other aspects of the relationship with the management.

INCIDENT INVESTIGATION AND PREVENTION:

A troublemaker had worked in the company for a long time and gained authority, so many employees would consider his words. As the relationship with the top management was heating up, the employee could hardly restrain his emotions and, eventually, almost openly pitted staff against the top management.

The investigation showed that the dissatisfaction of the team began to increase. The DLP system discovered the correspondence between displeased employees in Skype and on social networks. As a result, the agitator was fired, and the HR Department worked with the team to restore loyalty to the company.



IDENTIFYING TERROR THREATS

After mass terror attacks in Europe, the aim to identify "strangers" became particularly relevant.

To detect extremist mood in a team, you should use the search for correspondence containing the following:

- **Slang phrases** ("Kalashnikov", "thumper", "armor", "mortar", "chest rig", etc.)
- **Specific words** ("fatwa", "shahadah", "ummah", "kaafir", "kafir", "munafiq", etc.)
- **Synonymic rows** (for the word Moslem, for example, "muzzy", "true believer", "Druze", "haji", "Hajji", "Islamite", etc.)

It is necessary to control all channels of communication, including corporate and personal webmail accounts (if an employee uses the latter at work), social networks, instant messengers, Skype and similar apps.

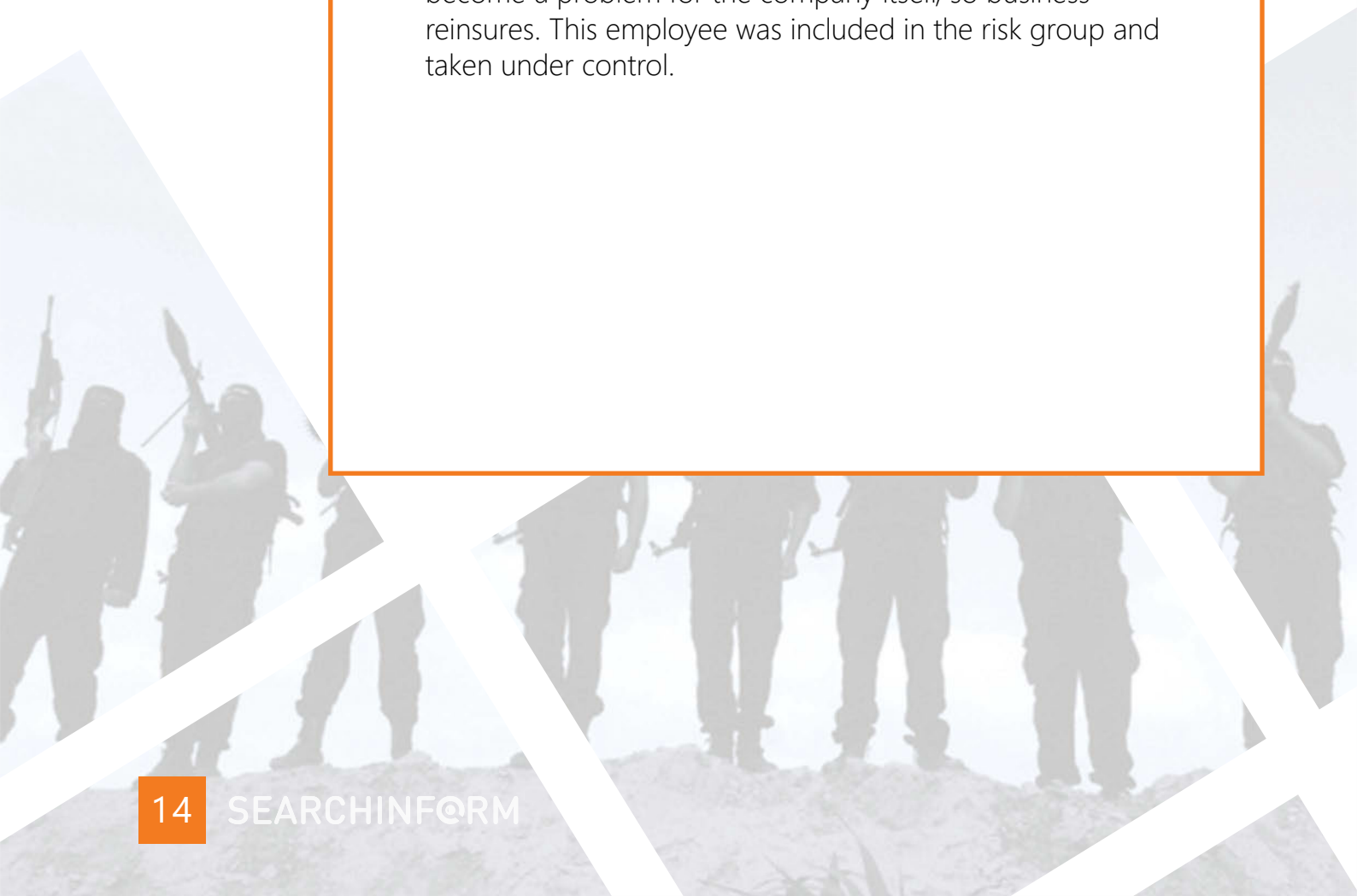
CASE: IDENTIFYING TERROR THREATS

Entry: Retail company; current security control using DLP system.

Case description: The correspondence of employees in the corporate chat was intercepted. The employees were discussing the war in Syria, and one of them spoke negatively of Russia's role in the conflict.

INCIDENT INVESTIGATION AND PREVENTION:

The IS officers checked the unreliable employee and found out that this person downloaded and printed out brochures on religious topics at work. Terrorist supporters can always become a problem for the company itself, so business reinsures. This employee was included in the risk group and taken under control.



DISCUSSION OF WAGES

The level of wages in most companies is a sensitive data for a reason, and the employees do not have the right to disclose it, because the difference in numbers can provoke resignations.

The security policies that are based on text search algorithms can help you to find the correspondence where employees discuss somebody's dissatisfaction with the salary, compare the salaries, agitate to arrange a riot or leave for another job.

To detect the above-mentioned discussions, you can use search by words, phrases or thematic dictionary – salary, coinage, raise, smalary, daily bread, bees and other synonyms in combination with the words indicating a certain amount of money.

NEGATIVE COMMENTS

Outraged employees in a fit of emotion leave negative comments and thus damage the reputation of a company. An employer can quickly learn about such attacks and take actions to counter them correctly.

Similarly to employment sites, first of all you should detect when employees visit sites with negative comments about employers. At the same time, you need to control if employees post comments on such sites. DLP systems also allow you to specify what exactly was written, even if employees did it incognito.

DISCUSSION OF THE IS DEPARTMENT

The fact that a company controls employees can cause discontent. The employees can demonstrate their indignation in the correspondence, discussing the IS specialists, control policy, wiretapping and reading of correspondence. In such correspondence, which is often maintained in a group chat, you can find a reference to the means and channels of communication through which employees are going to communicate instead of corporate ones.

The search query should include:

- Full names and nicknames of the IS officers
- Synonyms of the IS Department name (IS, Security, security team, etc.)
- Names of control systems (DLP, surveillance, control, watching)
- Topics-specific synonyms such as "bugged", "ears", "watched", "supervision", "big brother".

EMPLOYMENT OF FRIENDS AND RELATIVES

Friends or relatives can be promoted to managerial positions in order to receive payoff later. They may have free pass status or receive confidential information, so family ties and personal relationships automatically include colleagues in the risk group.

In this case, employees' email correspondence and communication via messengers are to be checked.

> *PLEASE NOTE: To improve the search results, you should exclude spam and attachments from monitoring.*

The search query that combines the search by words and phrases, indicating the degree of kinship ("brother", "matchmaker"), with the search by words and expressions from the employment vocabulary reveals potentially dangerous relations. At the discretion of the IS Department, the search criteria can be supplemented with the search by words and expressions on bribery topic. The system will search for the proper names in the context of the correspondence about payoff and employment.

REACTION OF A TEAM TO INNOVATIONS

A staff does not accept all changes at once, especially in a time of crisis when top management has to take drastic measures.

> *PLEASE NOTE: During significant changes in a company, it also makes sense to focus on controlling negative comments on the websites of "black employers".*

To study the mood of your team, the information protection system should identify the messages that simultaneously satisfy two following conditions as suspicious:

- The messages contain words indicating an innovation: "order", "decision", "resolution", "protocol"
- The messages contain keywords with a relevant content, primarily, negative, strong language.

EXPENSES EXCEEDING REVENUES

A purchase, the cost of which is much more than an employee's salary, may indicate a shadow income.

The control of emails, social networks, as well as the analysis of search queries on the Internet, help collect the evidence of self-indulgence on this employee.

The algorithm of the search by phrases consisting of a purchase item ("yacht", "house", "car", etc.) and a verb ("buy", "purchase", "order") helps determine a suspicious content.

The control of employees' big-budget purchases is especially relevant when a major deal is near completion. If there is a strong possibility that employees are receiving payoffs, these employees should be added to the black list to run the search only by potential violators. In this case, the search criteria are supplemented with the words like "interest", "share", "bonus", etc.

SEARCHINFORM

INFORMATION SECURITY

ABOUT US

SearchInform is the leading developer of information security solutions. Our technology secures business and government institutions against data loss and leakage, provides for managing information security threats and events, and for monitoring the efficiency of employees.

CONTACTS

BELARUS
Phone: +375 29 649-77-79
E-mail: ab@searchinform.ru

BENELUX
Phone: +31 6 44 78 62 93
E-mail: benelux@searchinform.com

EMEA
Phone: +44 (0) 20 7043 7152
E-mail: sy@searchinform.com

KAZAKHSTAN
Phone: +7 (727) 222-17-95
E-mail: d.stelchenko@searchinform.ru

LATAM
Phones: +54 11 5984 2618
+54 911 5158 8557
E-mail: r.martinez@searchinform.com

RUSSIA
Phones: +7 (495) 721-84-06
+7 (499) 703-04-57
E-mail: info@searchinform.ru

UK
Phone: +44 (0) 20 3808 4340
E-mail: uk@searchinform.com

UKRAINE
Phone: +380 (67) 476-15-18
E-mail: a.bugaenko@searchinform.com