# Contents

- Contents .............................................................................................................................. 2
- Some figures ........................................................................................................................ 3
- Abstract ................................................................................................................................ 4
- Methodology ........................................................................................................................ 5
- General Statistics ................................................................................................................. 7
- Leak channels .................................................................................................................... 13
- Industry map ...................................................................................................................... 16
- Conclusions and expectations ......................................................................................... 211
- Leak Monitoring on the InfoWatch website ................................................................. 222
- Glossary ........................................................................................................................... 233
Some figures

- In 2014, InfoWatch Analytical Center uncovered (in the media and other sources) and registered 1395 cases of data leak, which is 22% more than in 2013.
- Most often (92% of cases), data leaks were related to personal data. Over 767 mn personal records were compromised by insiders accidental or deliberate actions, as well as external attacks.
- 2014 has seen 14 megaleaks that disclosed over 10 mn personal records. 89% of all compromised records were attributed to megaleaks.
- Banks — along with Internet services, retailers, and health care institutions — are the biggest sources of personal data leaks.
- In 55% of cases, company employees were responsible for leaks. In 1% of cases, it was senior executives.
- Russia held second place in terms of number of registered leaks. Within the observed period, the study registered 167 cases of data leaks from Russian companies and public agencies. As compared to 2013, the number of "Russian" leaks grew by 73%.
Abstract

InfoWatch Analytical Center presents this report on the study of confidential data leaks in 2014. The authors attempt to reflect a comprehensive picture of information leaks on a global scale, identify the factors forming this picture, and demonstrate the consequences of data leaks for commercial companies, public agencies and individuals.

2014 could be called the "year of personal data megaleaks". There were over 30 cases registered when the compromised data amount exceeded 1 mn records. Half of those leaks were really enormous — 10 mn records and more.

Mass media provided extensive coverage of the attacks against infrastructures of such retailers as Home Depot, Michaels Stores, Neiman Marcus, and Sally Beauty Holdings. Each time, it was personal data including bank card details compromised. Along with retailers, banks and Internet-services suffered significantly from external attacks. Among the victims were Evernote, Experian, HSBC Turkey, JPMorgan Chase, Korea Credit Bureau, Google, Orange, and Snapchat.

The situation with leaks in Russia is rapidly getting closer to American. So far, Russia has not registered leaks worth millions of dollars caused by external attacks. But fraud with other people's personal data is quite regular for some employees of banks, insurance companies, and mobile phone outlets. Such crimes have become a general practice in Russia, even though quite recently they would have seemed alien.

The authors of this study believe that comprehensive analysis of the global leak picture (with the prevailing number of leaks in foreign countries, more advanced in information security) will benefit both the Russian market and the countries in similar conditions concerning data security.
Methodology

The report is based on the Center's own database, managed by its experts since 2004. InfoWatch Analytical Center's base includes public information\(^1\) concerning data leaks\(^2\) from commercial and non-commercial (public, municipal) organizations as a result of malicious or negligent actions\(^3\) by employees or intruders\(^4\). InfoWatch data leak base contains several thousand incidents.

When updating the database, each leak (if possible and such information is included in the relevant report) is classified according to a number of criteria: size of the organization\(^5\), area of activity (industry), amount of damage\(^6\), type of leak (by intention), leak channel\(^7\), type of leaked data.

Since 2014, data leaks resulting from external influence (targeted attacks, phishing, web hacking etc.) have been added to the database. To provide a reliable comparison between data from 2014 and data of previous periods, the authors have adjusted the figures of 2013.

Also, since 2014, incidents have been classified by the nature of a violator’s activities. Along with leaks, the report authors register cases when an employee having legitimate access to data uses it for the fraudulent purposes (payment data and insider information manipulation), and when an employee obtains access to data that is not required for his/her duties performance (exceeding access rights).

The report covers no more than 1% of cases out of the assumed total number of leaks. However, the leak categorization criteria are selected so that the studied quantities (categories) contain a sufficient or abundant amount of elements (actual leak cases). This approach to forming the research field makes it possible to consider the final sample to be theoretical, and the study's findings and revealed trends as representative of the general population.

In order to maintain uniformity of the sample when compiling the industry map, we intentionally excluded leaks with a disproportionately large (more than 10 mn) number of personal data leaks, or megaleaks. When compiling the industry map, leaks with an insignificant (fewer than 100) number of "leaking" records were also excluded from the sample.

---

\(^1\) Information on data leaks published by public agencies, mass media, bloggers, Internet forums, and other open sources.

\(^2\) An Information (data) leak is an act or omission by someone who has legitimate access to confidential information, when such an act entails a loss of control over information or a breach of confidentiality of that information, as well as a loss control of control over confidential information as a result of an external attack.

\(^3\) Data leaks are divided into intentional (malicious) and unintentional (accidental), depending on whether the person bringing about the data leak acts with intent. The terms "intentional — malicious", and "unintentional — accidental" are equivalent and used here as synonyms.

\(^4\) In this report, the authors present a picture of leaks in terms of guilty parties. For the first time, along with insiders, the classification includes intruders.

\(^5\) InfoWatch Center's analysts classify the organizations by size depending on the known or estimated number of personal computers (PCs). Small companies — up to 50 PCs, average — 50 to 500 PCs, large — more than 500 PCs.

\(^6\) Data on damage and number of compromised records is taken directly from publications in the mass media.

\(^7\) By "leak channel" we mean such scenarios (a corporate information system user's actions or omissions aimed at equipment or software services), as a result of which control over information is lost and its confidentiality is breached. The classification of the leak channels is provided in the glossary.
Cases of breaching confidential information (detected vulnerabilities) and other incidents (DDoS-attacks) not involving data leaks, as well as leaks without a clear data source (when it is now known to which company or organization the compromised data belonged), have been excluded from the sample.
General Statistics

In 2014, InfoWatch Analytical Center registered 1395\(^8\) cases of data leaks (3.8 per day, 116 per month). The leaks have compromised 767 mn personal data records — Social security numbers, bank card details, and other critical information (see Fig. 1).

\[\text{Fig. 1. Number of data leaks and volume of personal data records thus compromised. 2011-2014}\]

In 2014, the rate of data leaks continued to rise (see Fig. 2).

\[\text{Fig. 2. Number of registered data leaks, 2006-2014}\]

Over the observed period, the leak growth rate was equal to that of the previous year and amounted to 22% as compared to the leaks of 2013. Meanwhile, the growth of the compromised personal data amount decreased to amount to 37% as compared to the previous year's figure. An average leak disclosed 0.55 mn personal data records, 12% more than in 2013 (see Fig. 3).

---

8 Since 2014, InfoWatch Analytical Center has recorded — along with leaks caused by insiders — leaks caused by external influences (targeted attacks etc.).
1016 (73%) information leaks caused by insiders have been recorded. In 353 (25%) cases, an information leak occurred through an external attack. In 2% of cases, it has been impossible to define the attack source (see Fig. 4).

Due to insiders’ actions, 350 million personal data records have been compromised (0.34 mn per leak). External attacks have compromised 410 million records (1.16 mn per leak).

According to guilty party classification, the guilty person\(^9\) has not been found in 13% of cases. In 55% of cases, leaks have been caused by current or formal employees — 54% and 1% correspondingly (see Fig. 5)\(^{10}\).

---

\(^{9}\) Guilty person is a person who unintentionally allowed an information breach or committed abusive acts that resulted in compromise of proprietary information.

\(^{10}\) Guilty person is a person who unintentionally allowed an information breach or committed abusive acts that resulted in compromise of proprietary information.
Fig. 5. Distribution of leaks by guilty person, 2014

There is a high percentage of contractor edge leaks whose personnel had legitimate access to sensitive information (4%). More than 1% of cases represent the guilt of organization executives (top-managers, heads of departments) and privileged users (system administrators).

In 2014, less than half of the leaks were unintentional. Compared to 2013, the share of unintentional leaks has decreased correspondingly (see Fig. 6).

Fig. 6. Distribution of leaks by intention, 2013-2014

The redistribution of leaks according to intention parameter is due to the expansion of data protection tools (including DLP-solutions), and consequently, the growing number of unintentional leaks recorded. The number of intentional leaks is not growing so fast, as their registration requires more expensive protection tools.

---

10 This sample omits leaks with the attack source unknown. Therefore, the same number of leaks attributed to external attacks is shown as 25.3% (Fig. 4) and 25.8% (Fig. 6).

11 Leaks caused by intruders are considered intentional herein. The share of intentional leaks in 2013 is adjusted upward with account of the share of leaks caused by intruders recorded in 2014.
The share of leaks unattributed to any of the two mentioned groups, undetermined leaks, has decreased from 9% in 2013 to 7% in 2014. This trend has been maintained since 2012 (see Fig. 7).

<table>
<thead>
<tr>
<th>Year</th>
<th>Accidental</th>
<th>Intentional</th>
<th>Undetermined</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>96</td>
<td>102</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>38</td>
<td>295</td>
<td>0</td>
</tr>
<tr>
<td>2008</td>
<td>242</td>
<td>223</td>
<td>65</td>
</tr>
<tr>
<td>2009</td>
<td>325</td>
<td>382</td>
<td>40</td>
</tr>
<tr>
<td>2010</td>
<td>420</td>
<td>334</td>
<td>40</td>
</tr>
<tr>
<td>2011</td>
<td>336</td>
<td>344</td>
<td>121</td>
</tr>
<tr>
<td>2012</td>
<td>352</td>
<td>430</td>
<td>152</td>
</tr>
<tr>
<td>2013</td>
<td>522</td>
<td>687</td>
<td>117</td>
</tr>
<tr>
<td>2014</td>
<td>693</td>
<td>609</td>
<td>93</td>
</tr>
</tbody>
</table>

![Fig. 7. Rates of accidental and intentional leaks, 2006-2014](image)

The researchers explain the smaller share of undetermined leaks by improvement of IT specialists skills successfully detecting the leak source, malefactor and intention. Eventually, there are fewer and fewer reports on leaks with an unknown transfer channel and unknown intention.

The share of personal and payment data in leak distribution according to information type has grown by 7 p. p. as compared with 2013 and amounted to 92% (Fig. 8).

![Fig. 8. Distribution of leaks by data type, 2014](image)

The megaleaks with over 10 mn personal records each totaled 89% of all compromised records. Mass media provided extended coverage of the attack against the infrastructure of Target Corp. One more significant external attack was against another retailer, Home Depot, in 2014:

**Reuters.com**: The world's largest seller of construction materials and repair tools, Home Depot announced that 53 mn e-mail addresses of the trade network clients were compromised. By estimate, Home Depot lost 56 mn dollars due to the incident. The hackers managed to access Home Depot's network with a password belonging to a third-party software developer. Through manipulations with access
rights, the malefactors gained control over several segments of the company’s network. The hackers embedded malware into the company’s network that stole the information — e-mail addresses and bank card details. Home Depot experts note that the attack applied unique malware. The antiviruses used by Home Depot failed to detect the suspicious activity of the hacker programs.

In 2014, a huge number of information leaks have been associated with the use of personal data for fraudulent purposes, known as identity theft.

**Daily Mail:** The names, addresses, phone numbers and e-mail addresses belonging to over 83 mn company owners and householders were stolen through JPMorgan Chase. This is one of the biggest personal data leaks ever. 76 mn private accounts and 7 mn accounts of small businesses were under attack.

In terms of malefactor's nature of actions (see Fig. 9), 81% of cases represent a "classic" leak — loss of control over information.

![Fig. 9. Distribution of incidents by nature of action, 2014](image)

8% of the registered incidents have been classified as breaches related to unauthorized access to data (exceeding access rights, manipulations with information not required for employee's duties performance).

**databreaches.net:** Office employee of Spanish bank Santander in Leicestershire County (Great Britain) was sentenced to a penalty of 880 pounds. 29-years-old Dalvinder Singh had worked at the anti money laundering department and had legitimate access to the clients' accounts. He decided to use his privileged rights to find out how much his colleagues earned. After the incident, the curious employee was fired. The bank’s spokesmen told that shortly before, Singh had passed a training session about principles of handling sensitive information. But it did not help.

In 12% of cases, information theft was aggravated with its abusive use for personal advantage (usually, it was fraud).
Conclusion:

The increasing amount of compromised personal data results from megaleaks; the increasing number of leaks has been mostly caused by external attack. The main values reflecting the global picture — leak growth rates, shares of personal data and commercial secrets, share of guilty insiders — remain almost constant year by year. The share of undetermined leaks is reducing gradually.
Leak channels

Study of leaks in terms of the channels through which the information is exiting has direct practical significance. The frequency of leaks through a given channel may help to specify the recommended security equipment for a company or industry in order to determine which channels should be addressed first. 2014 has seen less leaks through removable media (-0.4 p. p), e-mail (-0.5 p. p), voice/video channels and instant messages (-3.9 p. p). The percentage of paper document leaks has changed negligibly (+0.2 p. p). Against other categories, a high increase has been demonstrated by leaks related to theft or loss of equipment, especially user devices, such as notebooks, smartphones etc. (+4.5 p. p).

In 18% of cases, a leak report contains no information about the channel. The share of such cases has decreased by 7.8 p. p. (see Fig. 10).

The share of network leaks totaled 35% (+10.7 p. p.) and it is quite reasonable, since this is the channel external attackers use\(^\text{12}\).

**The Wall Street Journal:** A hacker attack compromised the data of the employees, managers and clients of American Post USPS. The hackers might steal 800,000 records including the names, addresses and SSN of Americans. Among the victims are both current and retired employees. The attack affected the Postal Service’s departments and inspection department.

The number of leaks through mobile devices has decreased (-3 p. p.). The small share of mobile device leaks is due to the low efficiency of the existing security solutions for smartphones and tablets. However, it does not mean that mobile device leaks cannot be tracked:

\(^\text{12}\) The distribution by channel takes into account data leaks caused by external attacks. Such leaks occur exclusively through the network. Therefore, for the data of 2013, the authors have increased the percentage of the network channel proportionately to the equal percentage of leaks in 2014 caused by external attacks.
*Triblive:* Eileen Daly, a PNC Bank top manager, took a photograph of her computer screen on her personal mobile phone not long before she went to work for PNC’s competitors, Morgan Stanley. The bank’s information security system prevented Eileen from simply making an electronic copy of the clients’ data, so she had to take a picture of her computer screen. According to PNC Bank’s estimates, the actions of the former top manager caused a 250 million dollar damage. The bank’s representatives speak of at least 15 major clients who left for the competitor together with Ms. Daly.

The shares of intentional leaks through removable media, e-mail and paper documents have been insignificant. For reference: In 2013 the share of intentional leaks through e-mail amounted to 5.8%; in 2014, this channel gave 1.2% of intentional leaks. The shares of accidental and intentional leaks through mobile devices amounted to 1% and 0.2% correspondingly (see Fig. 11).

---

**Accidental**

- Theft/loss of equipment: 22.0%
- Mobile devices: 10.2%
- Removable media: 1.0%
- Network (browser, cloud): 7.5%
- E-mail: 1.2%
- Paper documents: 0.6%
- IM (text, voice, video): 0.0%
- Undetermined: 0.0%

**Intentional**

- Theft/loss of equipment: 26.3%
- Mobile devices: 6.5%
- Removable media: 0.0%
- Network (browser, cloud): 2.0%
- E-mail: 1.2%
- Paper documents: 0.6%
- IM (text, voice, video): 0.0%
- Undetermined: 0.0%

---

*Fig. 11. Distribution of accidental and intentional leaks, 2013-2014*

We should note that the percentage of leaks does not always reflect the degree of danger related to a specific channel. Thus, the e-mail channel registers 13% of all accidental leaks and only 1% of intentional leaks. Still it is obvious that a single leak of critical information is enough for a company to lose millions of dollars.

*Bloomberg:* Kang Gao, a former analyst of Two Sigma Investments LLC, was charged with the theft of confidential information from his employer. The analyst was arrested in January after he announced his leaving Two Sigma Investments. The spokesmen of Two Sigma told that Kang Gao had used a decompiler program to obtain access to information in the off-screen modules of the corporate software and had sent that information to his personal e-mail. The company admits that distribution of the stolen data would cause irreparable harm to its business.

The last, rather exotic channel to be mentioned is information leaks through video/text messengers. This channel is represented with insignificant 1.5% on the accidental leak diagram and 0.6% on the intentional leak diagram. However, the appearance itself of such
leaks is an argument for the old truth: there are no "small things" or unimportant "peripheral" channels in information security.

It is known that DLP systems are the most successful in detecting and preventing accidental leaks. The extending use of DLP solutions enables companies to register and properly classify the accidental leaks that used to pass unnoticed. It explains why the share of accidental leaks through undetermined channels has decreased.

However, sometimes the channels of even major leaks remain unknown:

The Baltic Course: A leak during the sale of Citadele, a state controlled bank, cost Latvia 7 mn euros, reports delfi.lv with reference to Minister of Economics Vyacheslav Dombrovsky. The minister notes that the data leak and geopolitical conditions have hampered competition. According to Mr. Dombrovsky, the number of possible buyers of the bank has decreased, some investors have learned of their competitors’ interests. Eventually, the asset price has fallen considerably.

The shares of leaks through removable media, e-mail and paper documents (especially against the remarkable shares of these channels for accidental leaks) are small, since malefactors tend to use these channels more rarely. "Advanced" malefactors know that the modern monitoring tools can successfully intercept leaks through these channels, so it is not worth the risk.

Conclusion:

The considerable gap between intentional and accidental leaks distributed among the channels proves the improving skills of the malicious insider. The “traditional” channels register fewer leaks, since malefactors know enough about the functionality of their protection and do not use them.
Industry map

In 2014, the share of leaks from state and municipal institutions within the observed period decreased by 16 p. p. to amount to 16%; meanwhile, the share for commercial companies increased by 13 p. p. (see Fig. 12).

Fig. 12. Distribution of leaks by organization type, 2013-2014

Most often, leaks have been registered in health care (25%); most seldom — in municipal institutions (2%). In terms of amount of compromised data, the leader is banking structures — 41%; hi-tech companies demonstrate half the number of leaks — 17%; trade companies — 15% (see Fig. 13).

Fig. 13. Distribution of leaks number and volume of compromised personal data by industry, 2013-2014.

This distribution is under great influence of megaleaks with over 10 mn leaks each. Again, the distribution includes "empty" leaks (when the amount of compromised records is less than 100 or unknown). To level out the effect of "empty" leaks and megaleaks, the authors...
adjusted the sample by considering leaks with 100 to 10 mn personal records only. The further diagrams rely on the adjusted data.

The distribution of compromised records per leak within a single industry makes it possible to distinguish the industries being the principal victims of personal data leaks (see Fig. 14).

Fig. 14. Amount of compromised personal records per "non-empty" leak according to industry. 2014, mn

The leader in this regard is the hi-tech industry (due to Internet services), where a single leak corresponds with 0.66 mn compromised records (including financial details of employees and clients).

The Irish Times: 500,000 euros were spent by Loyaltybuild, an Irish loyalty program operator, to update the information security system and eliminate the consequences of the greatest breach in Ireland's history, during which personal data of 1.5 million European users was compromised. Not only were customers' names and addresses stolen, but also the payment information, including credit card details and CSV codes stored in unencrypted format. While the investigation was in progress, all operations of Loyaltybuild were suspended. The company managed to resume activity only three months after the event.

Along with retailers, banks are major black-market "suppliers" of personal data.

The industry map gives a broader view. The diagrams show the total amount of the compromised personal data per industry (the size of the bubbles) with distribution according to the company size and with indication of the number of registered leaks (vertical position of the bubbles) see Fig. 15.
Fig. 15. Industry map of personal data leaks, mn, 2014

The industry map for the studied period is not uniform. The biggest amount of compromised data is referred to hi-tech companies (including Internet services). Public agencies, healthcare and trade companies demonstrate a negative trend too.

The Telegraph: Medical data of 47 million patients of NHS healthcare system are sold to an insurance company. Using this information, the insurance company is intended to "improve" its payment and bonus system by reviewing, in particular, the risks of health insurance. Thus, on the basis of the information sold, it has been found that people under 50 get ill more often than the insurance providers used...
to suppose. So far it is not clear what measures the relevant British authorities will apply to these healthcare and insurance companies.

57% of leaks from middle-sized companies are accidental. 36% are intentional. Large companies present another proportion. In this case, 36% are accidental leaks and over half (52%) are intentional leaks (see Fig. 16).

Fig. 16. Distribution of personal data leaks by organization size, 2014

The total number of personal data leaks at medium-sized companies (up to 500 PCs) is substantially higher than at large companies. Medium-sized companies get 71% of all leaks and the share of large companies is 24%.

The distribution according to the data amount is quite different: 45% of personal data records at medium-sized companies and 55% — at large companies (see Fig. 17).

Fig. 17. Distribution of leaks by organization size, 2014

More detailed analysis implies that medium-sized organizations accumulate, depending on the industry, 49% to 80% of data leaks.
In many vertical structures, the amount of personal data leaked from medium-sized organizations was equal to that of large companies. Medium-sized trade and healthcare organizations lost even more than large companies of these domains.

**Conclusion:**

The situation concerning personal data protection in companies leaves much to be desired. It mostly concerns medium-sized businesses, where leaks are more frequent than at large companies. Most leaks in medium-sized business are accidental. In 2014, medium-sized companies have been the main “suppliers” of confidential information. Internet services, educational and health care institution have been leaders in this respect. These are the organizations possessing the greatest amount of personal data and unwilling to protect it, since they do not suffer from direct financial damage.

The reason of such a sad situation for small and medium-sized companies is the lack of efficient and cheap data security tools developed for small and medium-sized businesses.
Conclusions and expectations

2014 was marked by a number of major leaks of personal and payment data. The attack against Target retail chain was debated most, but it was not the only example. 14 megaleaks compromised over 683 mn records, i.e. 89% of the total amount of the leaked personal data. There were over 30 cases registered when the compromised data amount exceeded 1 mn records.

Almost three fourths of the personal data leaks were related to identity theft. The stolen information was used in fraud schemes. The criminals got loans and tax deductions for other people's credentials.

The massive attacks damaged the banks accumulating the information about individual accounts, bank card details etc., i.e. the most "marketable" data. Meanwhile, outside the bank information systems, there has been a real hunt for that very kind of data. For instance, criminals used malware to steal payment data from payment terminals of retailer chains. The big Internet service providers, transport companies, and public agencies were under attack.

The growth rates of leaked data amounts have outpaced the rate of leaks. The amount of compromised data per leak has grown. There has been a bigger share of leak caused by intruders. In other words, there have been more hacker attacks to steal personal data and other valuable information.

Malicious insiders have also been in good shape. 12% of all the leaks have been related to misuse information legitimately available to an employee. Usually, such cases dealt with financial fraud by bank employees. 8% of leaks have been related to unauthorized data access. Insiders hardly used such transfer channels as mobile devices, removable media, e-mails, and paper documents. "Advanced" malefactors know that the modern monitoring tools can successfully intercept leaks through these channels, so it is not worth the risk.

How did the companies react? The study shows that in 2014 many organizations had difficulties even with the relatively simple task — personal data security. It mostly concerns medium-sized businesses, where leaks were even more frequent than at large companies. Moreover, most leaks in medium-sized business are accidental. Medium-sized companies were the principal "suppliers" of confidential information. In this view, Internet services, educational and health care institution were the leaders.
Leak Monitoring on InfoWatch's website

InfoWatch Analytical Center's website regularly publishes reports on information leaks and the most significant incidents, supplemented with comments by InfoWatch experts. Additionally, the site provides statistical data concerning leaks during the recent years presented as dynamic graphs.

Follow the news on leaks, new reports, and analytical and popular articles on our channels:

- Mailing
- Facebook
- Twitter
- RSS

InfoWatch Analytical Center
www.infowatch.com/analytics
Glossary

An information (data) leak is an act or omission by someone who has legitimate access to confidential information, when such an act entails a loss of control over information or a breach of confidentiality of that information, as well as a breach of confidential information as a result of an external attack.

Confidential information — (here) information accessed by a strictly limited and known group of people with the provision that the information shall not be passed to third parties without the consent of the information owner. In this report, the category of confidential information includes information falling under the definition of personal data.

Intentional leaks — information leak cases when a user working with information anticipated possible negative consequences of their actions, understood their unlawful nature, was warned about liability and acted with selfish motives for personal gain. As a result, the user’s actions resulted in conditions for loss of control over information and/or a breach of confidentiality. It does not matter whether the user’s actions really had negative consequences, or whether the company suffered losses associated with the user’s actions.

Unintentional leaks — these include cases of information leaks when a user did not anticipate possible negative consequences of their actions and did not pursue personal gain. It does not matter whether the user’s actions actually had negative consequences, or whether the company suffered losses associated with the user’s actions.

Leak channel — a complex scenario (actions of a user of a corporate information system aimed at equipment or software services) resulting in loss of control over information or breach of confidentiality. Currently we differentiate 8 separate leak channels:

- Theft/loss of equipment (a server, data storage system, notebook, PC), — compromise of information during maintenance or because of loss of equipment.
- Mobile devices — information leak as a result of illegitimate usage of a mobile device/theft of a mobile device (smartphones, tablets). The use of data on devices is regarded within the framework of the BYOD paradigm.
- Removable media — loss/theft of removable media (CDs, memory cards).
- Network — leak through the browser (sending data to a personal e-mail, input forms in the browser), illegitimate use of internal network resources, FTP, cloud services, unauthorized publication of information on a web service.
- E-mail — data leak through a corporate e-mail.
- Paper documents — information leak resulting from improper storage/utilization of paper documentation, through printing devices (sending for printing and theft/removal of confidential information).
- IM — messengers, instant messaging services (information leak when transferred by voice, text, video or instant messaging services).
- Unspecified — the category used when information about an incident in mass media does not determine the leak channel.