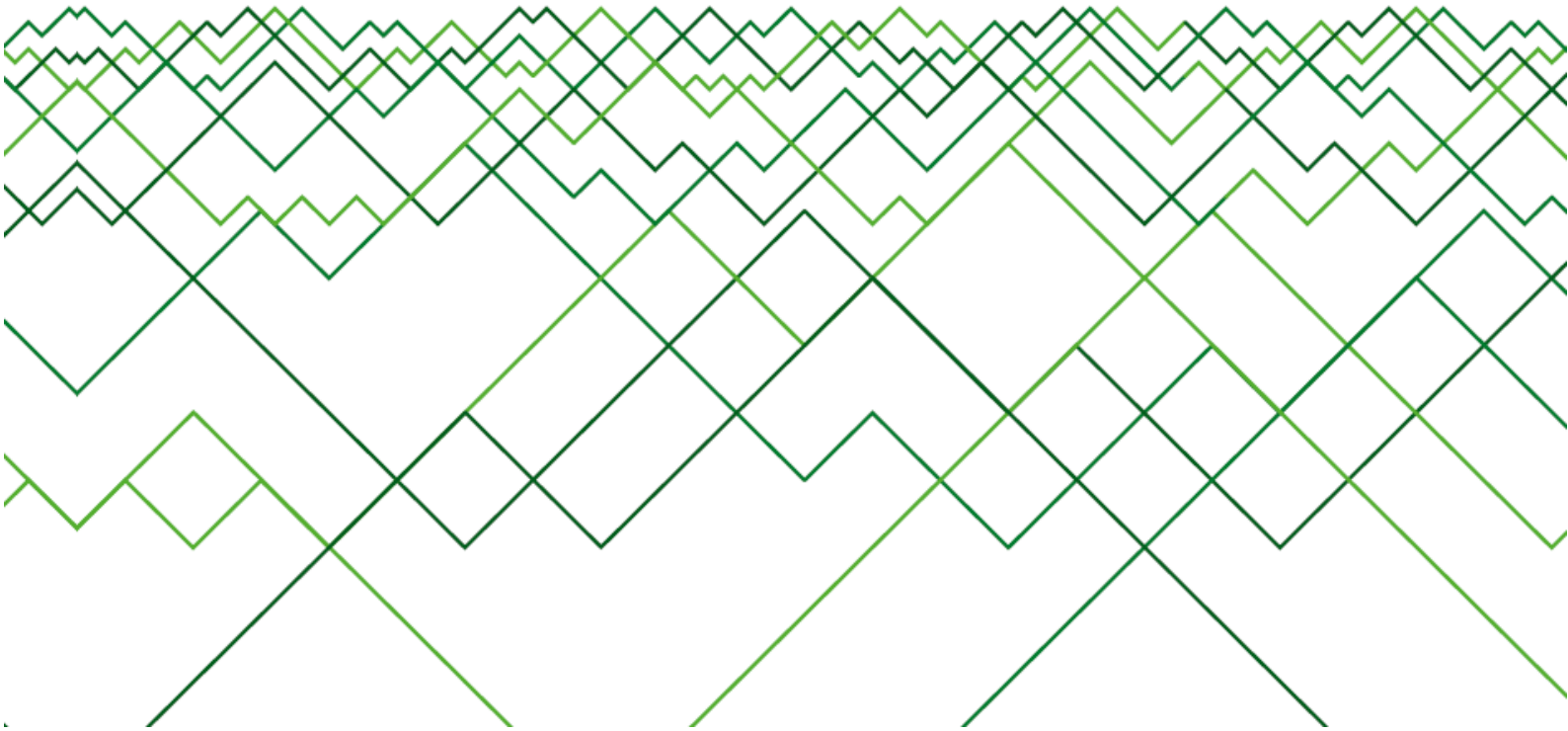
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

InfoWatch Analytical Center

10 Most Widespread Staff Errors behind Data Leakage

Prepared by: Andrey Prozorov, Lead Information Security Expert



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Table of contents

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Introduction

InfoWatch Analytical Center regularly prepares reports on sensitive data leakage in Russia and worldwide, as well as other analytical materials and leakage prevention recommendations.

According to our findings, one of the critical conclusions is that **the number of accidental and intentional data leaks is approximately the same**. However, the approaches to prevent accidental and intentional data leakage are dramatically different. Thus, in case of accidental leakage, organizations should focus on the personnel awareness raising and training and implement tools notifying users of their attempts to violate security policies. In case of intentional leakage, it is important to minimize user access rights, reduce the number of possible data leakage channels, leverage data transfer monitoring and control tools, and keep a security event archive.

This document contains typical scenarios of data leakage occurring due to enterprise staff errors and/or negligence while operating data media, data processing tools and systems, as well as real life incidents and security recommendations.

10 most widespread staff errors behind data leakage:

- ✓ Loss of removable media
- ✓ Loss of mobile devices (including theft)
- ✓ Negligent use of paper documents (including loss)
- ✓ Wrong email sending
- ✓ Wrong mailing and fax sending
- ✓ Wrong access granting, sensitive information disclosure to the public
- ✓ Negligent disposal of paper documents
- ✓ Negligent disposal of equipment
- ✓ Failure to wipe out sensitive information before equipment transfer for outsourced maintenance
- ✓ Security policy breach (illegal transfer and copying of information) upon requests of other employees and third persons (social engineering)

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Data leakage scenarios and incidents

1. Loss of removable media

Removable media (for example, memory cards, USB flash, CD/DVD, and tape drives) are popular and generally available tools to transfer (exchange) information and store backup copies. A small size of such media makes it easy both to take beyond the controlled zone and to lose.

Real life incident:

> [1] *An employee of the Governor's Office of Information Technology (Colorado) lost a USB drive containing personal data of almost 19,000 public authority employees. The e-document, which was stored on the flash drive, contained first and last names as well as social security numbers (SSN) of both current and former employees. The removable drive was not encrypted despite the relevant requirements adopted by the organization.*

More data leakage incidents: [1], [2], [3]

2. Loss of mobile devices (including theft)

Currently, more and more employees use corporate and personal mobile devices (laptops, tablets, smartphones, etc.) to process sensitive information. Similar to removable drives, such devices are easy to take beyond the controlled zone and people usually do it. Moreover, mobile devices are a natural target of robbers and thieves, and therefore losses or more likely thefts of laptops and other devices are rather common.

Real life incidents:

> [4] *A corporate laptop, which contained personal data of several thousands of US citizens, including SSNs and driver license numbers, was stolen from the car of the King County Sheriff (Washington, USA), with data not being encrypted.*
>
> [5] *According to the VAIO Digital Business report by Sony, over 1 million laptops with valuable corporate information were stolen over the past 12 months. The respondents included representatives of 600 UK companies.*
>
> [6] *Credant Technologies conducted a survey in seven US airports, including Chicago, San Francisco, Douglas, Miami, Orlando, Minneapolis, and Denver, and was depressed by the results, since during the period from June 2011 to June 2012 passengers left 8,016 devices in the airports, including smartphones, tablets, laptops, and flash drives.*

More data leakage incidents: [4], [5], [6], [7], [8], [9], [10], [11]

3. Negligent use of paper documents (including loss)

Printed documents containing sensitive information are often stored without any control, left near printers, or even lost outside the organization.

Real life incident:

> [12] *Dental clinic staff in Langepasa, a town in the Tyumen Region, took patient medical records outside the clinic. When one medical record was left in the taxi, the information about the patient's health was disclosed to the public.*

More data leakage incidents: [12], [13], [14], [15]

4. Wrong email sending

Employees usually send wrong emails because of careless addressee entering/selecting or when trying to simplify the process by sending the same information to all correspondence participants.

Real life incident:

> [16] During the bulk emailing on changes in a medical insurance program, accountants at *the University of Mississippi wrongly sent a table containing personal data of 2,281 students, including social security numbers, average graduate score, sex, race, date of birth, addresses, phone numbers, etc.*

More data leakage incidents: [16], [17], [18], [19], [20]

5. Wrong mailing and fax sending

It is absolutely the same as described in the previous paragraph, only a sending method is different.

Real life incident:

> [21] *UK Information Commissioner's Office has served the Bank of Scotland with a fine of £75,000 for sending confidential information to wrong fax numbers. According to the findings, the bank employees were sending payroll records, bank statements and mortgage applications, which contained client names and contacts, to wrong fax numbers during the period from February 2009 to 2012.*

More data leakage incidents: [21], [22]

6. Wrong access granting, sensitive information disclosure to the public

This type of error covers a range of wrong actions such as granting excessive access to information and services, accidental errors during access configuration, information disclosure due to the misunderstanding of relevant confidentiality requirements, abuse of power in the course of disclosure, etc.

Real life incidents:

> [23] *During the inspection, the Tambov Region prosecutors found out that from December 1, 2012, to August 6, 2013, the regional State Labor Inspectorate published the legal entity and individual entrepreneur review plan for 2013 on its official website, with tax registration numbers (INN) and residential addresses of some entrepreneurs being disclosed there.*
>
> [24] *The Tyumen Justice Court fined Tyumen Central Air Traffic Agency for passengers' personal data publication on its website, including passenger full name, date of birth, residential address, passport details, flight routes, etc. The above data was easily available to any website visitor.*

More data leakage incidents: [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]

7. Negligent disposal of paper documents

Negligent disposal of paper documents is surprisingly widespread. Documents containing restricted information are not destroyed properly but just thrown away.

Real life incidents:

> [34] *A woman in Abakan, a town in the Khakassia Republic, found three packets left near the garbage can in the yard and containing papers with personal data of Kedr Bank clients, including client first and last name, passport details and even the existence of their dependent persons.*
>
> [35] *A Kansas clinic chief physician and owner had to discontinue his medical practice due to the negligent usage of confidential documents related to his clients—women who procured an abortion. In mid-March, passers-by found out thousands of medical records left in the garbage can in the school territory near the chief physician's house, with names, addresses, phone numbers, SSNs and medical details being easily retrievable*

More data leakage incidents: [34], [35], [36], [37], [38]

8. Negligent disposal of equipment

In addition to incidents when computers and storages with sensitive information are just thrown away without data wiping out, this type of errors also includes the transfer and resale of such hardware for repeated use.

Real life incident:

> [39] *A Wales man accidentally threw away an HDD containing the file of more than 7,500 bitcoins. Today, one bitcoin costs over $1,000 which makes the man's total loss exceed $7.5 million.*

More data leakage incidents: [39], [40]

9. Failure to wipe out sensitive information before equipment transfer for outsourced maintenance

Organizations often outsource computing equipment repairs and maintenance to specialized centers instead of doing it themselves. However, sometimes the transferred media are not checked for sensitive content, or such checks are not always possible due to device malfunction. Eventually, repairs/maintenance personnel may gain access to all the information stored on the device.

Real life incident:

> [41] *Virginia Tech suffered from data leakage after outsourcing the maintenance of a server containing personal data of 145,000 people*.

More data leakage incidents: [41]

10. Security policy breach (illegal transfer and copying of information) upon requests of other employees and third persons (social engineering)

Such errors occur when somebody (including unknown persons holding themselves as company employees) requests or directly instructs (in case of a boss) an employee to save or transfer sensitive information using any method. And a deliberate desire to steal this information can be behind the request.

Real life incident:

> [42] *Standard Chartered Bank* and Citi Bank Korea suffered from the leakage of confidential information on 130,000 clients*. A Citi Bank employee printed personal and contact details of more than 30,000 people, while Standard Chartered Bank employee, acting upon fake senior's request, copied the information to a USB drive. These leaked data contained client names, phone numbers, addresses, their financial standing details. The corrupted employees received a total of approximately KRW300 million (some $300,000). The data was later used to solicit clients by phone with loan offerings and advertisements.*

More data leakage incidents: [42]

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Security measures

№	Staff Error	Security Measures
1.	Loss of removable media	- Staff awareness raising and training - Mandatory media encryption - Monitoring and control of connected devices, filtering the information transferred to removable devices - DLP systems - Tools for guaranteed information destruction - Tagging of removable media - Device case labels and/or recorded text files containing the owner's contact details
2.	Loss of mobile devices (including theft)	- Staff awareness raising and training - Encrypting information stored on mobile devices - A ban to store information on mobile devices, terminal access to information - Cable locks for laptops - Software and/For hardware to track (control the movement of) mobile devices - Remote wipe out tools - Tools for guaranteed information destruction - Mobile device tags, device case labels and/or screen saver with the owner's contact details
3.	Negligent use of paper documents (including loss)	- Staff awareness raising and training - Marking of documents - Folders and/or enclosures containing the owner's contact details - Printing control
4.	Wrong email sending	- Staff awareness raising and training - DLP systems
5.	Wrong mailing and fax sending	- Staff awareness raising and training
6.	Wrong access granting, sensitive information disclosure to the public	- Staff awareness raising and training - More complicated access granting procedure and additional approval steps, regular access analysis and review - Tools to monitor and control the access granting

7.	Negligent disposal of paper documents	- Staff awareness raising and training - Shredders or other tools to destroy paper documents - Printing control
8.	Negligent disposal of equipment	- Staff awareness raising and training - Tools for guaranteed destruction of information and/or data media
9.	Failure to wipe out sensitive information before equipment transfer for outsourced maintenance	- Staff awareness raising and training - Tools for guaranteed destruction of information and/or data media - Non-disclosure agreement concluded with third parties
10.	Security policy breach (illegal transfer and copying of information) upon requests of other employees and third persons (social engineering)	- Staff awareness raising and training

Instead of conclusion

Accidental data leakages in organizations can have various scenarios. Since there is no single and universal approach to combat such leaks, the protection requires a systematic and comprehensive approach.

As a part of consulting services, InfoWatch specialists can help select necessary security measures, develop policies and procedures, conduct staff training, and much more.

Please feel free to contact us!

Phone/Fax: +7 495 22-900-22

E-mails:

- General information: info@infowatch.ru
- Sales team: sales@infowatch.ru
- Support team: support@infowatch.ru
- Public relations: pr@infowatch.ru

Address: 13 build. 41, 2nd Zvenigorodskaya St., Moscow, 123022, Russia

Official website: www.infowatch.ru

Follow us:

- https://www.facebook.com/InfoWatch
- https://twitter.com/InfoWatchNews

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Annex A.
The referenced incidents

[1] http://www.infowatch.ru/analytics/leaks_monitoring/5059
[2] http://www.infowatch.ru/analytics/leaks_monitoring/4040
[3] http://www.infowatch.ru/analytics/leaks_monitoring/2604
[4] http://www.infowatch.ru/analytics/leaks_monitoring/3129
[5] http://www.infowatch.ru/analytics/leaks_monitoring/3040
[6] http://www.infowatch.ru/analytics/leaks_monitoring/2704
[7] http://www.infowatch.ru/analytics/leaks_monitoring/2768
[8] http://www.infowatch.ru/analytics/leaks_monitoring/2747
[9] http://www.infowatch.ru/analytics/leaks_monitoring/2690
[10] http://www.infowatch.ru/analytics/leaks_monitoring/2682
[11] http://www.infowatch.ru/analytics/leaks_monitoring/2602
[12] http://www.infowatch.ru/analytics/leaks_monitoring/3601
[13] http://www.infowatch.ru/analytics/leaks_monitoring/3137
[14] http://www.infowatch.ru/analytics/leaks_monitoring/2862
[15] http://www.infowatch.ru/analytics/leaks_monitoring/2653
[16] http://www.infowatch.ru/analytics/leaks_monitoring/4026
[17] http://www.infowatch.ru/analytics/leaks_monitoring/4045
[18] http://www.infowatch.ru/analytics/leaks_monitoring/3053
[19] http://www.infowatch.ru/analytics/leaks_monitoring/2746
[20] http://www.infowatch.ru/analytics/leaks_monitoring/2589
[21] http://www.infowatch.ru/analytics/leaks_monitoring/3399
[22] http://www.databreaches.net/company-responsible-for-mps-social-security-mistake-explains/
[23] http://www.infowatch.ru/analytics/leaks_monitoring/3926
[24] http://www.infowatch.ru/analytics/leaks_monitoring/3439
[25] http://www.infowatch.ru/analytics/leaks_monitoring/5064
[26] http://www.infowatch.ru/analytics/leaks_monitoring/5012
[27] http://www.infowatch.ru/analytics/leaks_monitoring/4685
[28] http://www.infowatch.ru/analytics/leaks_monitoring/4044
[29] http://www.infowatch.ru/analytics/leaks_monitoring/3575
[30] http://www.infowatch.ru/analytics/leaks_monitoring/3306
[31] http://www.infowatch.ru/analytics/leaks_monitoring/3290
[32] http://www.infowatch.ru/analytics/leaks_monitoring/3150
[33] http://www.infowatch.ru/analytics/leaks_monitoring/3092
[34] http://www.infowatch.ru/analytics/leaks_monitoring/3086
[35] http://www.infowatch.ru/analytics/leaks_monitoring/2644
[36] http://www.infowatch.ru/analytics/leaks_monitoring/5208
[37] http://www.infowatch.ru/analytics/leaks_monitoring/2643
[38] http://www.infowatch.ru/analytics/leaks_monitoring/4686
[39] http://www.ichip.ru/novosti/internet-i-seti/2013/11/zhitel-velikobritanii-vybrosil-zhestkii-disk-s-7500-bitkoinov16
[40] http://rus.delfi.lv/news/daily/abroad/major-britanskoj-armii-vybrosil-v-more-noutbuk-s- sekretnoj-informaciej.d?id=43872606
[41] http://news.idg.no/cw/art.cfm?id=30A58A5E-F281-7C65-AB08CF33CE7C4D1C
[42] http://www.infowatch.ru/analytics/leaks_monitoring/5021