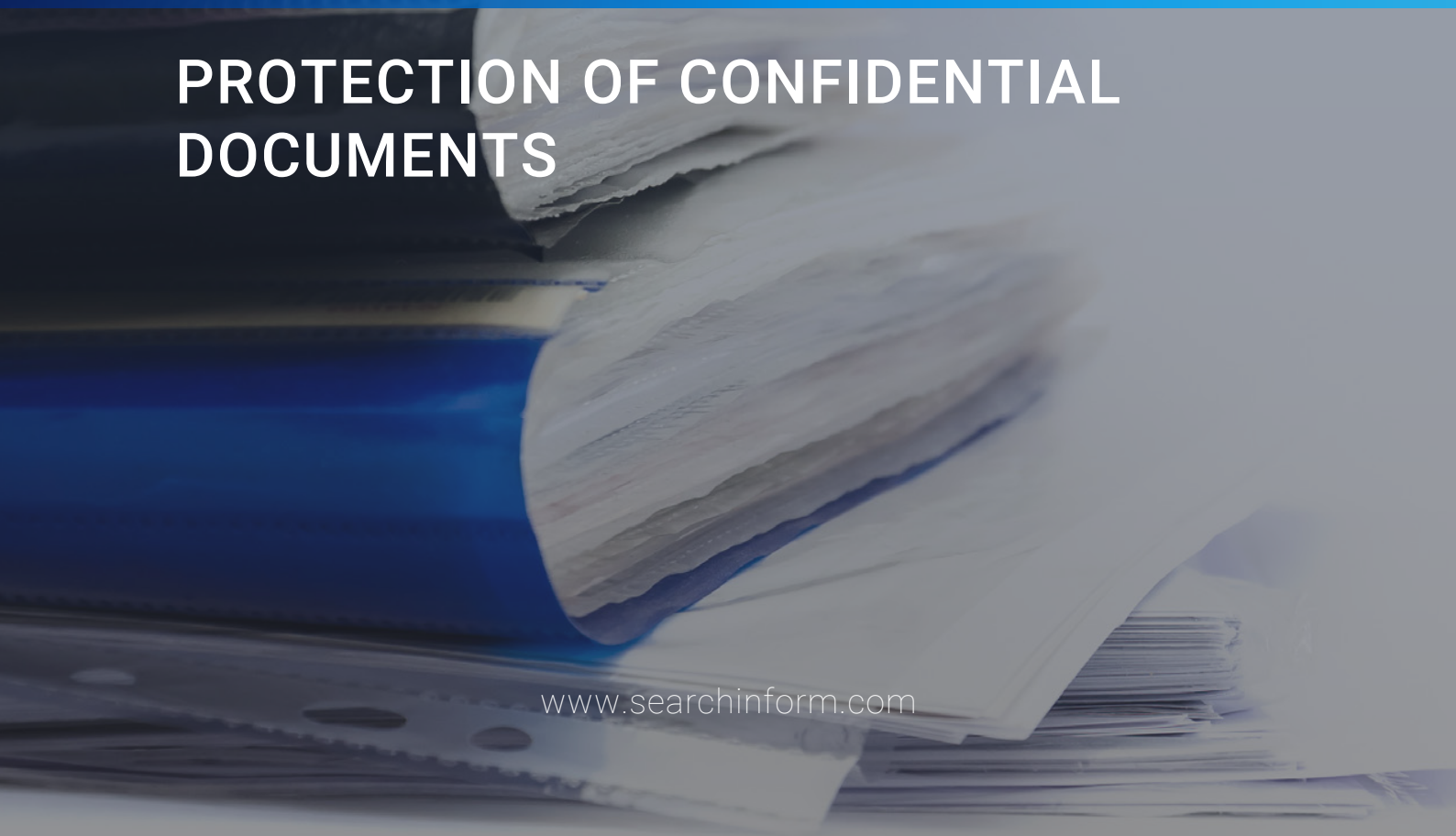
SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

INFORMATION SECURITY

[INTERNAL THREAT PREVENTION GUIDE]

PROTECTION OF CONFIDENTIAL DOCUMENTS



www.searchinform.com

WHAT IS THIS DOCUMENT ABOUT

According to the IBM and the Ponemon Institute study, in 2019 the average volume of losses from data leaks all over the world reached $11.45 million. Furthermore, leaks began to occur more often: if in 2016, companies faced an average of 1 leak per year, then by 2019 they have already recorded 3.2 leaks of data in a company per year. This data includes know-how, research results and business plans of companies, financial documents, information about customers and partners.

Today, such information is one of the main assets of any company, and therefore needs careful protection.

In this book, we:

- Systematized the experience of SearchInform clients
- Highlighted the typical and non-obvious threats associated with the leakage of confidential documents
- Outlined the protection methods that you can implement using the DLP system
- Provided recommendations with real examples from information security practices of companies

LOCAL NETWORK TOPOLOGY

Knowing the topology of your local network, fraudsters can use malware in no time and undermine the company's network or find a loophole in the equipment and steal company secrets. Therefore, do not underestimate the importance of such information.

You should control:

- **Company IP addresses and Media access control (MAC) addresses of the equipment** using a phrase search – if you keep track of a list of specific unique addresses or using a regular expression search to find references to any addresses that match a uniform pattern, such as ###. ###. ###. ### where # is the number for IP4 (group 0 to 255).

- **List of network equipment used in the company.** Knowing the weak points in the hardware of certain manufacturers will allow hackers to create exploits for vulnerabilities. Therefore, it is also worth tracking information about network equipment using a phrase search by manufacturer and model, or using a regular expression search. The search should exclude the correspondence of system administrators with each other and with suppliers so that DLP does not consider the planned work on the purchase of equipment suspicious.

- **Data for authorisation in the accounts of system administrators.** A real treasure for scammers, given the extended rights of system administrators. Specific logins and passwords can be tracked by phrases. But you can also use regular expression search if you know the sequence and other features of the credentials (for example, the first letter of the first and last name in the login, a certain number of lowercase and uppercase letters, as well as numbers in the password).

CASE: ATTEMPT TO LEAK THE LOCAL NETWORK TOPOLOGY

INTRODUCTORY: large retail chain; current security control using a DLP system.

WHAT HAPPENED: the security service discovered that one of the lawyers copied a document with diagrams of local networks and organisation of communication of the enterprise onto a personal flash drive.

INVESTIGATION: Since the DLP system automatically encrypted the data and it could not be opened on non-corporate computers, the security service continued to monitor stealthily.

It soon became clear that a recently hired lawyer deliberately ingratiated with one of the system administrators and gradually collected data on the company's local network, storing it on a computer. As for the job responsibilities, the employee's interest was absolutely irrelevant. In addition, information that fell into the hands of fraudsters could paralyse the system of operational accounting of warehouse balances. Rebuilding it would take a lot of resources, not to mention the losses concerning the downtime. The company did not risk it, and the suspicious lawyer was dismissed.

KNOW-HOW, UNIQUE DEVELOPMENTS

Know-how is the most valuable information for any business, its compromise can lead to the minimum loss of competitive advantage, maximum - to the forced drop out from the market.

You can track specific secret files using **an attribute search**. To do this, you need to set as many attributes of the file as possible: type (extension), name, size, etc. The wider the list of attributes, the more efficient the search is, for example, the system will detect the transfer of a secret file, even if the employee changes his name – in size and extension.

PLEASE NOTE: In order to hide their traces, scammers often place classified information in another, atypical file, for example, insert text, images, Excel tables or charts into an RTF file. Modern OCR technologies make it possible to expose such schemes.

You can use **phrase search**. As search queries, the system is given a unique composition of products, development technologies and other secret information. After that, matches are searched for via all channels. Only emails sent as part of the workflow to the corporate addresses of colleagues are excluded from the scan.

But it is best to use search types that deeply analyse the contents of secret files. For example, **search for similar** – when a know-how description is loaded into DLP, after which the system searches for all similar texts. If there are too many such confidential files, **a digital fingerprint search** is suitable for control. This type of monitoring will take into account the content of documents of different formats and their hash sums.

PLEASE NOTE: The best results are obtained by using a DCAP solution for file auditing in conjunction with a DLP system. DCAP will tell you on which PCs, servers, network folders confidential files are stored and who has access to them. DLP – will show if these files are being sent outside the corporate perimeter.

CASE: ATTEMPT TO LEAK UNIQUE COMPANY DESIGNS

INTRODUCTORY: a metallurgical enterprise; current security department using DLP and DCAP systems.

WHAT HAPPENED: In DCAP, the security service discovered that files with sensitive data are stored on the computer of an employee who did not have access rights to them. Moreover, at the time of the incident, this employee was on vacation.

INVESTIGATION: The DLP system revealed that this computer was regularly running remote access tools. It turned out that the network administrator was involved in the case, who temporarily stored confidential data on the victim's computer before transferring it to third parties. Thus, a respectable employee could become an innocent "accomplice" in the leakage of information, but the leak was prevented.

BUSINESS PLANS OF THE COMPANY

Competitors want to outrun you. And business plans will help them to do it.

To prevent such secrets from leaking, it is better to use several types of search:

- **Search by similar**
  In this case, the text of the secret document with the company's plans becomes the search query. Comparing the interception with it, the system finds all files similar to the original "technically" and by meaning. Moreover, the degree of "similarity" can be established. This means that you will know about the incident even if the employee copies some of the secrets and compiles them with other information.

- **Search by digital prints**
  An alternative technique that will take into account not only the contents of files, but also their hashes. It is very convenient when the company's business plans are contained in a large array of data: you do not have to make a search query for each separate document – you just need to transfer a folder with dozens of secret documents to the system. It will identify them and will track them within the captured data.

- **Search by words or phrases**
  The system will track correspondence and messages that include certain keywords, for example, "development strategy", "SWOT", "strategic planning", "dynamics", "trends", "growth", "decline", "potential", "Promotion". Search queries should be combined into rules (for example, search for messages in which A, B and C appear at the same time) – this will make the system's responses more relevant.

PLEASE NOTE: Employees talk about the company's business plans in their daily correspondence. To prevent the system from considering this a dangerous incident, letters sent to colleagues at corporate addresses should be excluded from the scan.

CASE: DANGER OF LEAKING COMPANY BUSINESS PLANS

INTRODUCTORY: retailer; DLP system testing.

WHAT HAPPENED: the development of the security policy showed that one of the employees communicates with an unknown person on Skype about the nearest development plans of the company.

INVESTIGATION: It turned out that the account of the unknown interlocutor belonged to a former employee of the firm – a sales manager who got a job with a competitor, but continued to closely communicate with some colleagues. Using the user relations report, it was possible to establish that the ex-employee talked to several employees and tried to find out internal news, changes in company policy and future development plans. The security service cut off this "friendly communication" and put the employees at risk.

INFORMATION ABOUT PARTNERS AND CONTRACTORS

A leaked dealer list and other similar information can give a head start to competitors and seriously harm the company. To combat this threat, it is recommended to use:

- **phrasal search** – by names / names of contractors and by names of supplied goods / services, if there are few of them;
- **search by regular expressions** – addresses, article numbers of goods and any other information that appears in the databases.

Verification should be carried out by mail, instant messengers, clouds, documents printed and copied to external devices.

PAY ATTENTION: the search will be even more effective when the databases of counterparties or other documents on cooperation are fully loaded into the program. After that, it compares all traffic with the loaded template: if similar documents end up in the hands of employees without access rights to them, or go outside the company perimeter, the system will inform. Use this functionality if your security system supports it.

CASE: DRAINING THE SUPPLIER BASE

INTRODUCTORY: a retailer of car tires and spare parts; DLP system testing.

WHAT HAPPENED: the head of sales uploaded the vendor database and price list to the cloud.

INVESTIGATION: The study of user connections revealed that the employee passed information to her husband, who was in cahoots with competitors. Having lost several suppliers due to data leakage, the company transferred the results of the investigation to the operational authorities, and they launched a criminal case. The damage was estimated at almost two million dollars. The retailer managed to recover more than 70% of the losses via court – they were recovered in the form of a fine from the perpetrator of the incident.

TENDER DOCUMENTATION

The declared value, volumes of goods and services and other information of the bidders may be used by fraudsters for unseemly purposes.

To prevent such leaks, one should look for the names of the subject of the procurement and the synonymous row "tender", "deal", "auction", "purchase", "contract", "agreement", etc., which is mentioned in one of two contexts:

- “cost”, “volumes of purchase/sale”, “volume of services offered”, etc.
- "discuss", "agree", "meeting", etc.

You should check messengers and social networks, mail, Skype and other communication applications.

CASE: ATTEMPT TO DRAIN TENDER DOCUMENTATION

INTRODUCTORY: a company selling protective and insulation equipment; current security control using a DLP system.

WHAT HAPPENED: the trigger showed that one of the employees of the Moscow branch of the company sent information on the ongoing tender to the external mail of an unknown user.

INVESTIGATION: Monitoring showed that the task to send a document to this address came from the director. He explained that he was away and could not enter the corporate mailbox, so he was waiting for a letter to his personal one. The security staff had reason to believe that the director wanted to leak information. This would have resulted in the company losing the $ 9 million tender. There was no information leak, since the information security department prudently encrypted the document. However, the director of the Moscow branch was fired.

CLIENT BASES

Leaking customer data can give competitors a head start and seriously hurt the organization.

To combat this threat, you can use a **search by customer name** or **search by regular expressions**, for example, addresses, passport numbers, and almost any other information that appears in the customer base. It makes sense to set the minimum number of records that must appear in a document for it to be considered suspicious.

Searching for similar ones is also very effective: you need to load client databases into the programs, and it will compare all outgoing traffic with them and report all matches.

Verification should be carried out by mail, instant messengers, clouds, documents printed and copied to external devices.

CASE: CLIENT BASE LEAK

INTRODUCTORY: credit institution; current security control using a DLP system.

WHAT HAPPENED: the development of the security policy drew the attention of the information security service to the anomalous activity of the employee in relation to client bases (individuals).

INVESTIGATION AND PREVENTION OF THE INCIDENT: The program helped to establish that the specialist has collected several client bases and combined them into one document. After – I sent it to a colleague who did not have access rights to this data.

As a result of the analysis, it was possible to expose the collusion: the first employee had to collect the data, and the other one had to sell it to interested parties. But, anticipating the insider, the information security service using the DLP system encrypted the documents that the second specialist threw on the USB flash drive. Thanks to this, "customers" would not be able to read the information. After collecting evidence of the violation, the criminals were fired.

www.searchinform.com

+44 0 20 3808 4340
order@searchinform.com

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

ABOUT US

SearchInform is the leading developer of risk and compliance software. Our technology secures business against corporate fraud and financial losses, provides for internal risks management, and for human factor control.

Visit our blog to be updated on relevant risk management and data safety issues.

linkedin.com/company/searchinform
facebook.com/SearchInformInternational
twitter.com/SearchinformI