



SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

RISK MANAGEMENT

[INTERNAL THREAT PROTECTION GUIDE]

COMPLETE DATA PROTECTION

www.searchinform.com

Contents

What is this white paper about?	3
Risks and consequences	4
What should be prevented?	4
From where do risks come?	5
Which costs does a company face?	6
Instruments and ways of protection	7
What constitutes risk management?	7
How to protect?	8
Level 1. Threat detection	8
Level 2. Incident investigation	11
Level 3. Risk control	13
How does it work?	14
Results	16

What is this white paper about?

Information about business processes, products and services, transactions, customers and employees constitutes a full-fledged business asset the loss of which is critical for any modern organisation. Therefore, data protection becomes synonymous with business protection.

Companies are constantly losing data, regardless of industry or size. And this happens more and more often: according to a study by IBM and the Ponemon Institute, in 2019, organisations recorded an average of 3.2 leaks per year against 1 incident in 2016.

The situation can be corrected if you build information protection and risk management framework properly and use different information security tools. This will allow you to effectively identify and investigate incidents, avoid violators' impact in future.

We systematised the experience of SearchInform clients and highlighted the best practices, on the basis of which we derived a comprehensive data protection strategy.

3,2
leaks per year
organisations recorded
in **2019**

1
incident per year
organisations recorded
in **2016**

**IBM and the Ponemon Institute*

In this white paper we will:

- analyse what the causes of security incidents are and what consequences they can lead to.
- give recommendations on how to protect information at all levels using specialised solutions.
- emphasise the signs by which it is possible to recognise a threat before an incident occurs, quickly fix the incident "in real time" and establish its circumstances with the help of retrospective investigation.
- show real examples of combining the advantages of different tools to achieve the best possible results.



RISKS AND CONSEQUENCES

What should be prevented?

According to international regulations, an information security incident is an undesirable event that can affect a company's business processes, compromise them or violate the degree of protection of information in software and hardware storages.

The main types of incidents include:

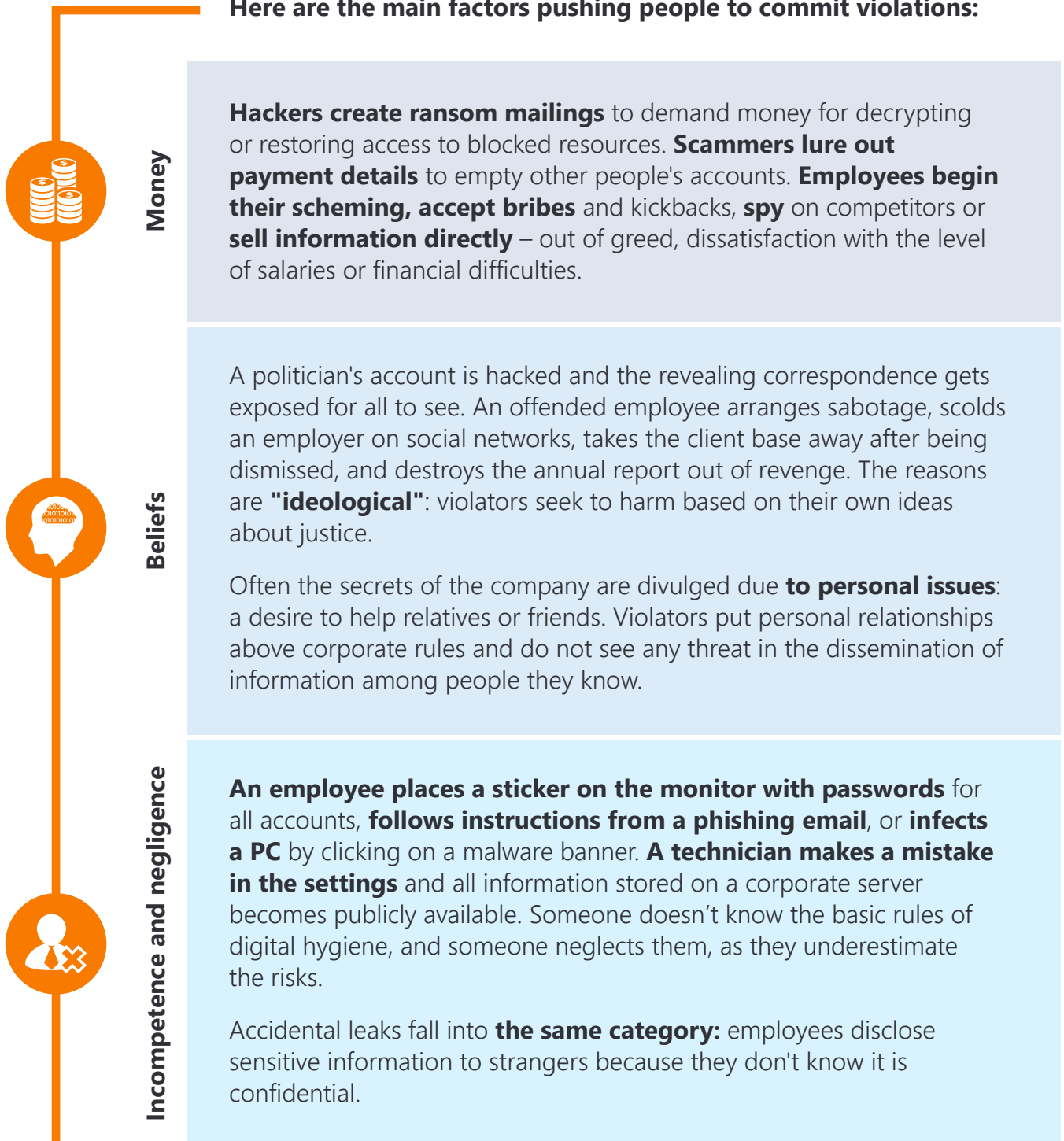
- violation of access to the Internet, hosting, email, cloud and other services;
- equipment failure due to technical or software errors;
- software deficiency;
- violation of any rules for processing, storing, transferring papers and electronic documents;
- unauthorised, third-party or illegal access to information resources;
- attempts to monitor corporate resources outside the perimeter;
- installing malware on corporate PCs;
- any system sabotage, for example, password leakage.

This can be a data leak, fraud, industrial espionage, sabotage. There is a human behind every cyberattack or technical failure that cause leakage of sensitive information. Therefore, control of those who work with data is paramount with regard to ensuring information security.

From where do risks come?

Information that is critical for the organisation can be stolen, altered, or deleted. There are many possible scenarios, but all threats have the same source – a person. It is important to understand the psychology of potential security violators in order to make human factor control effective.

Here are the main factors pushing people to commit violations:



Which costs does a company face?

According to a 2019 IBM Security [report](#), the average price tag for data breaches and hacking of corporate databases in the SMB segment reached \$3.9 million. And this is just a clear financial loss. The consequences of cybersecurity incidents can be much broader.

This is what companies typically face:

Direct losses

For example, equipment fails due to an incident – a company needs to spend money on its repair or replacement. An important study, which the company orders from a researching company, gets leaked – the study's value is lost.

Here is the cost of unavoidable downtime, in case an incident leads to a serious disruption of business processes – for example, access to the payment system, CRM or other operational resources is lost, or the regulator suspended the license allowing a company to carry out its activities. Some of these damages, except for those fines imposed due to violations, can be recovered from the perpetrators in court.

Intellectual property theft or know-how leakage – financial loss equals the cost of technology creation.

Indirect losses

This is a lost profit due to the customer churn, the disruption of transactions or trades.

Also among the implicit negative consequences there is market reduction, loss of strategic partners, counterparties, or competitive advantage – depending on what is impacted by a data breach.

Accounting, financial, and legal documents are leaked by employees every 2 weeks.

Customers, employees and transactions data is breached every two months.*

Reputational damage

The most unpredictable among losses, which can appear as financial (for example, a drop in the value of a company's shares), or as long-term internal consequence.

Among them, for example, loss of an employer's authority among employees, as a result – sabotage, deterioration of the quality of work, an outflow of specialists.

**According to the [SearchInform Internal Security Incidents research](#)*

INSTRUMENTS AND WAYS OF PROTECTION

What constitutes risk management?

In theory business information security should always incorporate:

ensuring the confidentiality of proprietary information and its responsible usage

elimination of risks that arise during data collection, processing and storage

access rights management and **user roles assignment** depending on the level of their authority when working with different categories of data

analysis of the typical behaviour of users who work with confidential information, **the creation of rules** for such work and **the prompt detection of suspicious activities**

study and manage newly created and active **accounts** to detect incidents as early as possible

preventive work with a risk group, because the best incident is the one that doesn't happen

thorough **investigation of incidents** to identify weaknesses in the existing business processes of the company and their further optimisation

In theory, the strategy looks simple: we start by organizing the data, take minimal preventive measures (set permissions and prohibitions), monitor and eliminate violations.

But in reality control should be implemented at three levels at once.

The optimal defense strategy is to record an incident **in the present**, thoroughly investigate its **past**, and develop measures to prevent such incidents **in the future**.

How to protect?

Level 1. Threat detection

The main task at the moment is to detect an incident promptly in order to avoid possible damage. Therefore, it is important that the security professional has complete information about the volume of confidential data, the state of storage and user actions at hand – and online.

Daily monitoring of corporate networks is effective when risk managers have the tools to answer these questions:

Where is sensitive data stored and who has access to it?

First, you need to conduct a **full audit of the file system** and select the information which should be protected in the general workflow. **It is useful to put the data into categories** (financial information, know-how, personal data, etc.).

Depending on the value, **different rules for access and usage should be set** for categories. It is necessary to determine where the vulnerable documents are located: on which PCs, file servers and in which network folders. And monitor who interacts with them.



DCAP solutions

(Data-centric audit and protection) allow you to detect, classify and control files that contain sensitive data, track changes in them (created, modified, "shared", moved, deleted) and save modified versions. The systems show which of the users performed these actions and detect access violations.

How do users interact with corporate databases?

A significant part of the operations that employees perform in the corporate network are related to requests sent to the database. A critical amount of service information is stored there.

Therefore, **it is necessary to monitor the frequency and nature of such requests** (adding, deletion or altering), record attempts of unauthorised access and potentially dangerous actions (execution of malicious scripts, SQL injection).



DAM solutions

*(Database activity monitoring) keep records of all requests to and responses from the database 24/7 and alert to suspicious activity: **loading or unloading large amounts of information, unregulated content changes, attempts to download restricted information.***

Where and for what purpose do users transfer data?

It is necessary to control the data going to the Internet and monitor what is happening on the computers of employees.

First, **it will be necessary to make a clear procedure for working with information** so that employees know: internal documents should be transferred only to colleagues, work correspondence should be carried out via corporate email or instant messengers, and documents should not be copied uncontrollably to removable devices. Secondly, **this procedure or corporate rules should be abided and violations identified.**



DLP systems control data transfer channels, prevent information leaks and report suspicious user activity, which indicates other security breaches: **fraud, sabotage.** Configuring security policies allows you to automate the search and incident analysis.

What is happening within the corporate network right now?

To complete the picture, you need to be aware of the status of all elements of the IT infrastructure: activity on PCs and servers, in the file system and database, take into account security system signals.

Data needs to be processed quickly violations are discovered promptly and the response time is minimised.



SIEM systems identify attacks and problems in the IT infrastructure in real time by correlating events from hardware and software. **This helps to detect security incidents in a chain of events that seem harmless when they happen not successively but randomly.**

How to act in case of incident detection is determined by the internal regulations created by specialists responsible for risk mitigation.

For example, you can block the transfer of confidential data outside the company. Some information security tools allow you to neutralise the consequences – for example, with the help of shadow copies of files which are made by audit systems, you can restore information in case of its deletion or distortion.

However, simply eliminating the threat is not enough: you have to figure out what led to it.

Level 2. Incident investigation

If incidents are not analyzed, they will repeat themselves. Each case should be carefully analyzed, at least to assess the real scale of the problem.

You will need to find out:

What exactly happened?

It is possible to establish all the circumstances of the violation by examining the data with the help of the monitoring and control systems.

For example, confirm the fact of unloading the client base from the server (DAM) and correlate this event with the appearance of an archive with similar content on the employee's PC (DCAP). Then track its movement within the corporate network by building a content route to the point where an attempt to transfer the archive to an external address (DLP) was recorded.

Who is the culprit?

Security systems automatically record under which account unauthorised actions are performed and on which devices illegally obtained data is stored (DAM, DCAP).

Sometimes there are several violators, and they act together: in order to identify all those involved, it is useful to study user connections (DLP). And if there are no leads, the analysis of the behaviour and personal characteristics of possible culprits helps to narrow the search.



Automated profiling allows you to compose psychological portraits of users based on a psycholinguistic analysis of their correspondence, to determine the strengths and weaknesses of the employee, his beliefs, basic values and a tendency to violate certain safety rules.

Why did this happen?

It is important to study the context: the actions of the violator on the PC, communication with colleagues, searches and actions in programs and on websites. This information becomes available via the DLP system. As a rule, one of the basic risk factors will be found: conflict as an excuse for revenge, debts as a motivation to make unfair money, etc.

Profiling will show deeper reasons: it is useful to compare employee profiles in dynamics for different periods. Change may indicate burnout, stress, unfulfilled ambition.



The more you know about an incident which caused an investigation launch, the easier it will be to draw a conclusion on how to prevent similar incidents in the future.



Level 3. Risk control

Prevention of violations is based on a clear understanding of the scenarios for the development of security incidents. In addition, you need a complete overview of the "battlefield": well-functioning monitoring and control of corporate networks, storages, knowing the weak spots in the IT infrastructure (for example, outdated equipment and software that has not been updated for a long time).

Proactive work has two main directions:



Restrictive measures

Based on the company's internal regulations – business processes, job responsibilities of employees, communication channels used – **rules for access to sensitive information should be set**. And also to structure data storage, distribute user roles and block unwanted actions: for example, sending documents to the clouds or copying them to flash drives.

The work will be facilitated by **setting up automatic rules for searching for incidents according to specified criteria** (security policies in DLP, correlation rules in SIEM, data classifiers and access rules in DCAP and DAM).

Most solutions come with a set of predefined policies, but security professionals have the ability to tweak them or create their own.



Identification of risk groups

DLP security policies detect signals in user behaviour that indicate addiction (alcohol, drugs, gambling), dangerous interests (for example, extremist), **unfavorable life circumstances** (family problems, debts, illnesses, etc.). Here there are signs of disloyalty, from negative discussion of management to viewing vacancies and updating the CV.

You should also pay attention to the psychological portraits of employees.

Automated profiling, among other things, allows you to get a snapshot of the entire team: ratings of employees are compiled depending on how clearly one or another quality is expressed in them. For example, the most scandalous, non-team, overly motivated for money can potentially cause problems.

All of these factors can be a catalyst for disruption. Therefore, users who fall under suspicion after policy alerts or have low profiling ratings should be taken under control.

How does it work?

We have collected the stories from SearchInform clients, which clearly show how the usage of information security tools when bundled helps establish the details of the incident and regain control over the situation.

Case: unauthorised access to someone else's email

What happened: the **SIEM system** reported that someone else had access to the manager's mailbox.

Investigation: analysis of the logs showed that the system administrator set up mirroring of the manager's email to his mailbox. To understand why he did this, the specialists analysed his actions with **Risk Monitor**.

It turned out that the system administrator didn't leak any data. Then they studied his correspondence: he told a friend via Skype that he had lost the prize because one of his colleagues had complained about him to his superiors. It was decided to find the person who complained in the manager's letters.

As a result: the offender – system administrator – was punished again, which he refused to agree with and decided to quit. On his last day, he tried to take revenge: he remotely connected to the database in order to download a malicious script deleting information.

The DAM system confirmed the SQL-injection attempt, the information security specialists promptly blocked all actions with the help of **Risk Monitor** through the remote administration software. The incident was prevented.

Case: violation of data access rules

What happened: the **DAM system** recorded numerous data changes in the customer base.

Investigation: using shadow copies of requests to the database, it was established that several employees with the right to access the database changed the numbers of clients from remote time zones, and after a short time cancelled the changes.

The **DLP system** captured messaging in a WhatsApp chat where these employees discussed the search for "reliable people" in order to convey "instructions" to them. The file with the same name was attached within the correspondence – it comprised the scheming: when a clients were supposed to have night-time in their countries, the scammers changed their numbers to their own in order to confirm small payments on their accounts via SMS, and then returned the correct phone numbers to the database.

As a result: file audit (DCAP) revealed who else in the company had a file with criminal instructions, and it was removed from publicly accessible location. Those involved in the scheme were fired, the fraudsters were handed over to law enforcement agencies.

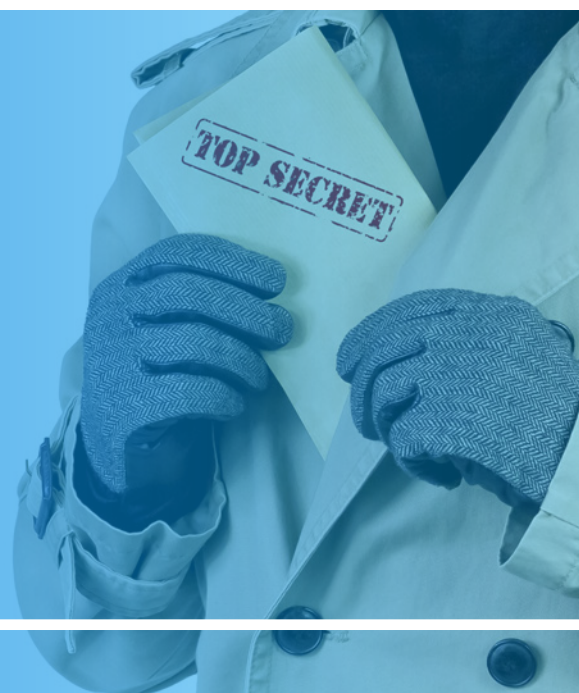
Case: anonymous blackmail

What happened: the leader received an anonymous message on Facebook with threats to spread “compromising evidence” within the team which might undermine his reputation. As a proof, there was attached a photo of the laptop screen showing a confidential document containing evidence of “wrongdoings” opened on it.

Investigation: search for the sender in Facebook finished with no outcome: the page was created only to send one private message, and then deactivated. There was no data captured with the **DLP system** that any of the employees registered a new account on the social network.

Then, in the **DCAP system**, they tried to reveal who had access to the document, the photo of which was contained in the anonymous letter. There were 28 such people. To narrow it down, specialists studied their psychological portraits in the **profiling system**. They singled out two of them who, summing up their characteristics, were potentially capable of implementing such a complex scheme.

As a result: the security service conducted an interview with each suspect and soon followed the violator’s confession.




RESULTS

Let's fix it: **the security perimeter of the company must control external and internal threats at all levels.** The combination of advanced information security tools provides:

- Constant awareness of what is happening in the company;
- Ability to respond quickly and prevent incidents;
- Reduction of losses due to the fault of personnel;
- Knowledge base for making strategic decisions.

Comprehensive monitoring reveals more than individual violations. Systemic problems are becoming noticeable: unproductive business processes, personnel decisions. This is an opportunity to see ways of optimization, find new points of growth and realise the potential for the company's development.

Therefore, we say that **security is not a “defense against”, but a “benefit to” business.**



SearchInform was founded in 1995, since then the company has been developing information security solutions for businesses as well as has been active in the ERM market for 15 years already. In 2017 SearchInform solution was recognised by Gartner and included into the Gartner Magic Quadrant. Today the company provides more than 3000 clients in 20 countries with the software and services protecting over 2 000 000 computers all over the world.

The developer conducts annual international series of conferences all over the world. SearchInform Road Show has already been held in Latin America, the Middle East and North Africa, South Africa, India and Indonesia. SearchInform products and services for comprehensive protection against internal threats include:



Risk Monitor, our key solution, is a comprehensive internal threat mitigation platform which allows a company be aware of any activity performed within the corporate perimeter. Its toolset builds up your risk management program and lets you control data in transit and data at rest, monitor internal and external user communication, conduct ongoing and retrospective investigation identifying every detail of an incident or a potential threat acting as an early warning.



DLP is part and a solid foundation of the Risk Monitor concept. It incorporates instruments for monitoring nearly each communication and data transfer channel, including messengers, email, web forms and chats, social media, external storage devices, printers and other popular means to share information.



FileAuditor classifies sensitive data identifying confidential files, conducts access rights audit, archives critical documents facilitating incident investigation and enabling recovery of information, and monitors user operations on a file system alerting to changes made to a file.



Database Monitor identifies information adding, removing or changing in a database 24/7. The software conducts automated indexing of requests to a database and makes them available for search and analysis.



ProfileCenter is an automated profiling packed into a smart easy to use instrument. It will help you to know who you work with, learn about how to appoint employees and to make sure whether a specialist is a good fit for the position and has no risky propensities and criminal tendencies.



TimeInformer tracks user activity, detects arrival and departure time, analyses work with websites and applications. The collected data gets processed by the software and is rendered as reports which let you understand who is dedicated and who is watching videos or messaging half a day.



SIEM collects information from various sources, analyzes security events in real time, records incidents and alerts to them.



SearchInform services offer on-premises and cloud-based options. The company can provide software and analytics, the customer receives all the requested information about internal activities and security events.

The solutions can be used individually or bundled. When products interact with each other, the customer gets a synergistic effect. When these are products from one vendor, they interact more successfully than when integrated with the systems developed by different solutions makers.

SearchInform products are suitable for companies in various industries – from banking to mechanical engineering. We protect the data of patients of medical institutions, we ensure the safety of know-how in manufacturing companies, we monitor the confidentiality of document flow in government organisations.

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/Searchinforml