SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

MANAGING SECURITY RISKS

[INTERNAL THREAT PREVENTION GUIDE]

DATA PROTECTION AND INVESTIGATION SERVICES FOR BUSINESS

www.searchinform.com

WHAT THIS DOCUMENT IS ABOUT

According to Computer Economics, in 2019 companies' expenses covering demand for risk management and security services grew from 9,4% up to 12,7% taken out of a total budget and allocated for IT infrastructure. This trend has been observed for 5 years already.

Small and medium-sized companies avidly look for an SaaS or MSSP: it is difficult to maintain IT infrastructure relying only on a limited staff, allocate budget for software license and hardware purchase as well as hire or assign employees to only deploy and work with the risk management software.

Often there are not enough people to ensure information security within a company. This is why 48% of organisations are ready to pay for security as a service or turn to MSSP.

In this whitepaper we:

- Tell when and why companies should consider applying for security services.
- Explain the way internal risk management services work.
- Advise on how to cooperate efficiently with the services provider.
- Show real numbers and case studies shared by businesses all over the world.

INFORMATION SECURITY AND RISK MANAGEMENT SOLUTIONS FOR BUSINESS

1. SEARCHING TO HIRE A FULL-TIME ONSITE RISK MANAGER OR CYBERSECURITY SPECIALIST

If a company wants to find an experienced specialist working with internal security threats, it will face some difficulties. Many companies claim that a good specialist can be found but it takes a lot of time. Besides, large businesses might require more than one employee to mitigate internal risks. The more time gets spent on searching for a professional, the bigger payroll expenses are.

2. STAFF TRAINING

If a company faces difficulties finding a professional, it can choose a simpler way – send a staffer to complete a training program. A comprehensive retraining conducted in a college or provided by a proficient training center can take up to 700 hours (nearly 17 work weeks), and it is usually a full-time education format. Such a type of studying can be beneficial for companies which expand their risk respond departments, when a senior specialist needs a team.

PAY ATTENTION: Both cases require a company to allocate extra budget for purchasing data protection software which a specialist will work with. After the system is purchased the budget should also be allocated for a training program to deploy the solution efficiently.

3. OPTING FOR SERVICES

When solving of internal risk mitigation tasks by in-house specialists is delayed in time and leads to large one-time costs, the company is ready to consider the third option – risk management services.

PAY ATTENTION: According to SearchInform, if a company has less than 100 PCs, the cost of services doesn’t exceed the costs of a full-time specialist and the purchase of the system, even in the long term. If the company has more than 200 PCs, services become more expensive than having an in-house information security department only during the fifth year of subscription.

Hereinafter, under services, we mean internal threat mitigation services (prevention of corporate fraud, data breach, workflow sabotage, etc.).

WHEN DOES A COMPANY NEED SERVICES?

Data protection can become crucial for businesses in case:

- The number of PC users is more than 50 employees, and current internal activity monitoring measures are not sufficient.
- Business processes comprise collection and processing of large amounts of personal data (there are risks of losing customer details, limitations and penalties from regulators).
- A company conducts business in a competitive market, is involved in the production of complex unique products, owns know-how and patents, which means it risks becoming a victim of industrial espionage.

WHICH THREAT PREVENTION SOLUTIONS CAN BE DELEGATED TO A CONTRACTOR?

Tasks covered by internal threat mitigation services include:

- confidential information protection;
- discovery of fraud, scheming, implicit issues within a team (employees who might undermine the team spirit and working atmosphere, sabotage or conspire);
- foreseeing risks and preventing incidents;
- time tracking and employee performance evaluation;
- mood and attitude within a team analysis and loyalty assessment;
- detailed incident reports creation for a company’s management.

A specialist uses the monitoring solution to solve these tasks.

The services provider ensures:

DEPLOYMENT OF THE SOLUTION

Specialists working at the services provider conduct technical audit of a client's IT infrastructure and deploy the solution at the customer's facilities or in the cloud.

SUPPORT AND MAINTENANCE

A specialist monitors activity within a client's corporate network remotely maintaining the system's processes: installs updates, solves problems together with technical support.

CONFIGURING OF THE SOLUTION

The provider's specialists configure the system, set the security policies in accordance with the needs of a client.

DATA PROTECTION

A risk manager assigned by the services provider analyses the situation in a company, prepares detailed reports on incidents (the reason for the violation, evidence). Conducts internal investigations if necessary.

HOW TO ESTABLISH EFFECTIVE COMMUNICATION WITH A SPECIALIST

The quality of the services can be impacted by a few factors.

THE QUANTITY AND QUALITY OF INPUTS – ANY INFORMATION ABOUT A COMPANY

Provide a specialist with information about a company to ensure quick introduction to a company’s internal architecture and communications:

- a general list and job descriptions of employees whose PCs will be protected by the solution (for the correct assessment of user actions in the system: for example, a managing director can access accounting documents, but a manager can’t);
- a list of employees working remotely (they should be monitored first of all, since they use corporate data, but remain out of an employer’s sight);
- a list of email domains (for monitoring messages sent and received by email);
- competitors' email domains (to track connections with employees);
- a list of the most valuable information assets: know-how, documents, databases with restricted access;
- general information about a company and description of business processes, etc.

RESPONSIBLE TRUSTEE APPOINTED BY A COMPANY

A specialist's work will be more productive if a company creates a role of a trustee for one of its employees who will be responsible for cooperation with a specialist providing services. The two can communicate and stay informed of detected incidents. A trustee will also have an access to the monitoring solution to control a specialist's activity and work with the solution instruments if needed.

Choosing a trustee requires attention. It should be a loyal staffer who the management can rely on. In case there is made a wrong choice the quality of the provided services can deteriorate. For example, a trustee can be too slow when discovering a violation, might conceal incidents which are too intricate or even awkward and ignore detected problems.

EMERGENCY CHANNEL

Information security and risk management are about promptness, that is why it is important to decide on what, where, to whom and when gets sent by a specialist. Email isn't an emergency channel. A phone and a messenger are a better choice.

CLIENT’S FEEDBACK BASED ON REPORTS

Besides alerts to incidents which require prompt intervention and assistance, a specialist sends a detailed report to a trustee in accordance with the schedule which they agreed on. All the incidents, both minor and major, are considered in it.

Usually, if a company installed the monitoring software on 100 PCs or less, the first report can be obtained within 7-10 days. If more than 500 PCs are to be protected with the solution, it can take a month to create a correct report. One month is enough for an analyst to collect information from all the departments and PCs.

An analyst is responsible for making and sending a report. This specialist can highlight the most impactful violations and give recommendations how to respond to them. But decision making is what a trustee or a CEO does.

Efficient interaction can be established only in case a feedback is sent and received on an ongoing basis between a specialist and a client.

THE FIRST MONTH OF USING THE INFORMATION SECURITY AND RISK MANAGEMENT SERVICES: STATISTICS AND CASES

The best way to check the quality of a services provider is to request a free trial. Usually a month is enough to evaluate it.

Based on the trial experience in companies from different industries, SearchInform specialists have collected general solution implementation statistics.

In the first months of using the services, 100% of organisations find at least some incidents. Almost always among them there are:

- data leakage;
- inefficient usage of work hours and resources;
- activities not related to job tasks;
- fraudulent scheming;
- spreading spiteful or undermining opinion about a company and a team;
- job search.

Among other frequent incidents there are: gossiping about management, sending confidential documents to a non-corporate email or uploading to the cloud, copying data to a USB flash drive, printing personal documents at the workplace.

All these cases were detected during the services were tested as a free trial.

ILLEGAL SIDE BUSINESS AND SENDING VALUABLE DATA OUTSIDE THE CORPORATE PERIMETER

A client (construction company) asked a specialist to focus on fraud search and prevention of data breach. Several dozen violations were detected during one month.

Among major incidents there were:

- **Launching a side business** (a lot of documents belonging to a competitor company were found in a personal email box of an employee who was a Chief Financial Officer; later it became clear that in that very company three more employees were working as senior managers).
- **Uploading corporate documents to the cloud** (employees uploaded files, project documentation, information about a public cloud investor's expenses).
- **Copying to external storage devices** (employees copied agreements, financial and accounting documents, projects, and other information to USB flash drives).

PAY ATTENTION: Data transfer blocking can be enabled to protect valuable files from leaking – sending of documents to a flash drive, social media or to the cloud can be forbidden. This helps a company promptly prevent a data breach. But monitoring is preferable when it comes to massive and intricate fraudulent scheming.

EMPLOYEE CONDUCT AND WORKPLACE ETHICS VIOLATION, ACTIVITY NOT RELATED TO JOB TASKS

A CEO of a printing company wanted to get the details about employee productivity, learn whether the team worked in accordance with the timetable. A big part of the staff appeared to spend time on entertainment or working "for themselves".

Popular incidents:

- **Visiting leisure websites** (many employees spent from 30 minutes to 4 hours daily watching Youtube, playing games, messaging on social media, making purchases online, reading news).

- **Extra work** (a company's manager launched an online store selling photo albums for children and received orders during her work hours at her full-time job; a designer communicated with employees from the company he was working at).

- **Usage of non-corporate email** (managers received orders from clients using their personal emails which is usually a marker indicating accepting kickbacks and can point at client database theft).

PAY ATTENTION: Problems with work ethics and part-time extra jobs are often exacerbated by the temporary transfer of personnel to "remote work". A drop in employee productivity when working outside the office is observed by 40% of companies, a decrease in the length of a work day – by 28% of companies.

DOCUMENT FORGERY, FRAUDULENT ACTIVITY AND DATA LEAKAGE

In a food wholesale company, in addition to typical violations, a specialist discovered fraudulent schemes.

It took one month for the solution to detect:

- **Document forgery** (an employee inserted a signature and a seal in a graphic editor into commercial offers; an employee of the personnel department "drew" the employees' signatures in job descriptions implying employees' agreement with the instructions).

- **Corporate data copying** (an employee copied information about the conditions of working with suppliers, a description of business processes and a list of employees to a USB flash drive; an employee shared investment details via TeamViewer; another employee recorded a large amount of personnel data to an external hard drive).

- **Sending files belonging to a company to a non-corporate email** (an employee regularly sent documents to her private email box).

PAY ATTENTION: Remote Desktop Protocol (RDP) leaks are not uncommon. Monitoring solutions have the ability to control it. For example, you can prohibit copying any information from a PC with an active RDP connection or block the movement of documents in this mode.

USAGE OF CORPORATE RESOURCES AND MASS JOB SEARCH

Dozens of incidents were discovered in a state-owned company within a month, many of them indicated problems with work culture and ethics.

Among the key ones:

- **Active search for vacancies during work hours** (an employee repeatedly received newsletter with suitable vacancies to the corporate email, another received a notification to his email with gratitude for posting a resume on the job search site, the third one updated the resume on indeed.com).

- **Discussion of the upcoming dismissal in messengers** (several employees actively and emotionally discussed their dismissal in correspondence, many expressed dissatisfaction with the management).

- **Inappropriate usage of corporate resources** (employees regularly used work printers to print personal multi-page documents - books, textbooks, instructions, etc.).

PAY ATTENTION: Employees who are going to quit often take valuable corporate documents and data (marketing and accounting reports, customer databases, etc.) "as a keepsake". Therefore, their actions in a corporate system should be controlled strictly.

EMPLOYEE PERSONALITY, INCLINATIONS AND TRIGGERS

At a manufacturing company, a specialist found a large number of incidents involving employees with issues. They were identified with the help of policies configured to search for keywords from specialised dictionaries.

Among the incidents:

- **Gambling addiction and playing the stock market** (an employee spent a lot of time online on the stock market; another received checks from a bookmaker's office to his email).
- **Debts and loans** (employees took expensive microloans; one of the employees tried to draw a debt out threatening to a colleague and writing him aggressive messages in the messenger).
- **Large purchases** (several employees were spotted on the websites advertising expensive real estate and cars. Specialists paid attention to this as a likely sign of employee participation in kickback schemes).
- **Drug addiction** (an employee asked a friend on Facebook where to buy prohibited substances; another one received an offer to buy drugs in the messenger).

PAY ATTENTION: Employees with issues are more likely to turn into malicious insiders and commit crimes (theft and leakage of information, fraud) due to lack of money or under the influence of blackmail from competitors and bosses. Offended and disgruntled employees can sabotage or "inspire" an entire department to quit.

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