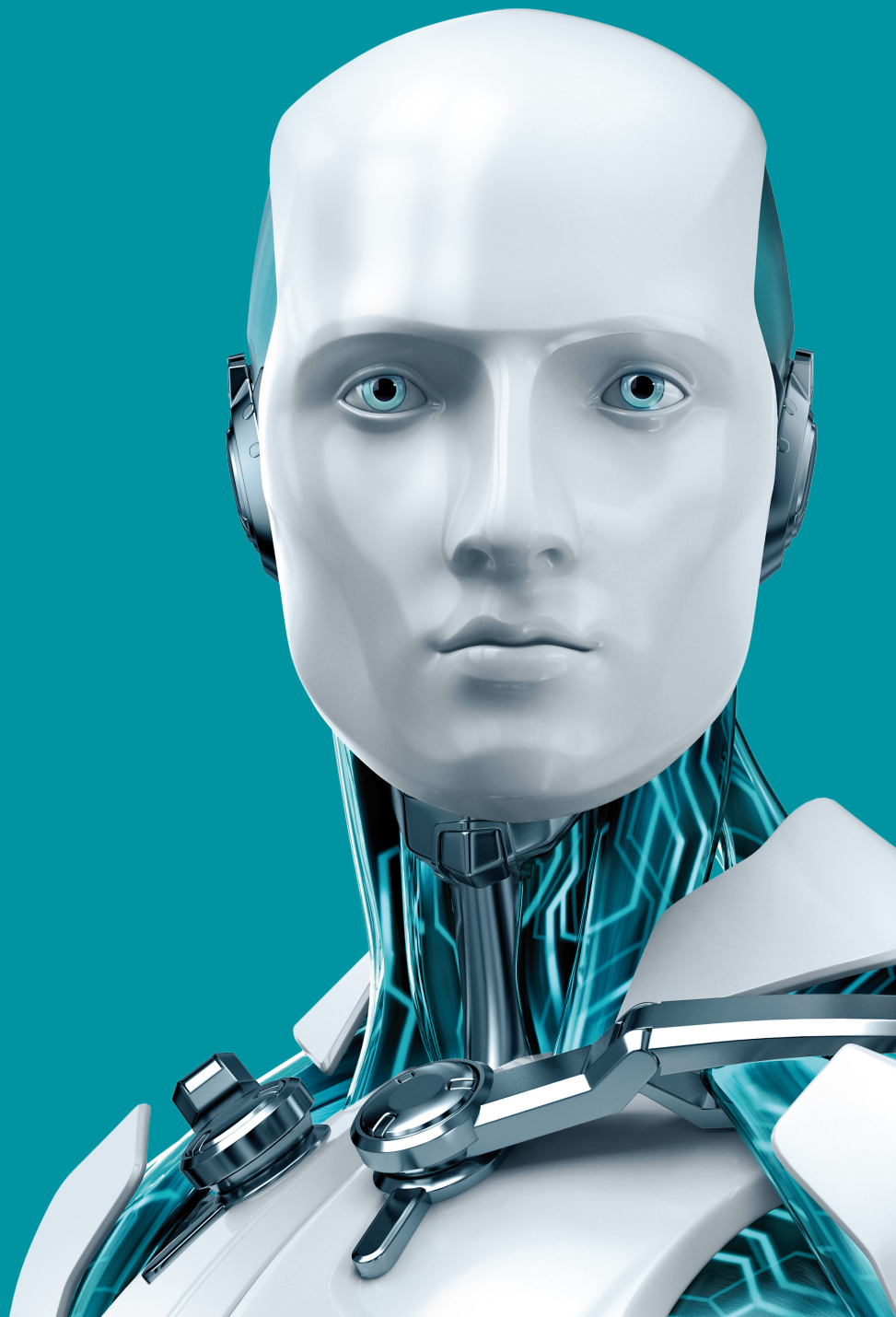
INSIDE OUT

APPROACHES TO DATA LOSS PREVENTION



CONTENTS

EXECUTIVE SUMMARY

Data breaches are one of the most significant cybersecurity issues that businesses and organizations of all sizes, ranging from large corporations to small and medium-sized companies, are facing at present. This paper – supported by a wide range of recent front-page stories and proven by statistics – offers the reader the information, reasoning and tools needed to prevent data loss.

But despite a widespread belief, incidents where information is lost or hijacked are not caused only by sophisticated hackers operating externally against the organization targeted. As quoted surveys show, insiders are the ones who often, intentionally or unintentionally (owing to poor security awareness or carelessness), cause massive leaks every year, exposing large numbers of sensitive records to unauthorized third parties.

With direct and indirect losses averaging $5.5 million per incident, prevention proves to be the better and more cost-effective strategy for any potential victim. Using encryption to protect data is a simple way that allows companies to follow regulations and not overburden their employees. This document also offers reasoning and arguments as to why and how one of the most prevalent data leak scenarios – insider threat – can and should be actively managed.

Organizations and companies can also find several general tips and advice to improve their data security, ranging from the introduction of internal policies and regular training of employees, to the use of technological means to counter the risk.

DATA LOSS BASICS

Data breach definition

A **data breach** is a cybersecurity incident that exposes sensitive, protected or confidential data to an unauthorized third party. Several types of information might be targeted, such as (medical) patient information and personally identifiable information, but also sensitive company information such as know-how or intellectual property. **Data loss**, **data spill** or **data leak** are other terms frequently used for this kind of cybersecurity incident.

Types of data loss incidents

There are multiple ways by which sensitive information can end up in the wrong hands but generally they can be divided into external and internal, depending on the cause.

For many, the first thought would be an **attack coming from the external environment**; an attack by malware, or the exploit of a vulnerability – or a large data dump – where the endangered company belongs to a group of victims targeted by the attackers.

Also, there is the obvious black hat hacker scenario, often described as an Advanced Persistent Threat (or APT). This term refers to a malicious actor using advanced tactics (often combining social engineering, advanced malware and other techniques) that is extremely persistent and aims at specific targets and their data. In some cases, hackers can spend months gearing up for such cyberattack or exploit vulnerabilities for years before their activities are spotted; this "patient behavior" has been observed in many such cases in the past.

However, statistics show that there is another threat, equally or potentially even more damaging for a firm's finances and reputation than an external attack – the so-called **insider threat**. This term refers to employees or partners of the company who have direct and legitimate access to the company's systems and are able to intentionally or unintentionally cause a data loss.

But why would anyone do such a thing? There might be several motivations behind it:

Data loss is often just a result of an **employee's mistake or carelessness**. And honestly, have you never sent an email to the wrong address; lost or forgotten one of your many USB sticks; or never had your smartphone, tablet or laptop stolen? In these ways, valuable information might land in an unintended inbox, in the hands of an unauthorized user or – even worse – it can be published online or through a social media account.

In many cases, employees do this just because they are not familiar with the appropriate way of handling data. An inexperienced user would usually pick their favorite way to share data, e.g. using a public cloud service or unencrypted drive, unaware that it's not safe.

Also, surveys have shown that as many as 60% of employees would take data from their former company and use it at their next place of work without perceiving this as misconduct, despite the fact that corporate policies are in most cases mindful of this risk and forbid such behavior.

And then there is the **intentional leak**.

Disgruntled employees might – out of frustration or revenge – voluntarily offer sensitive internal information, acquired during their employment, to a competitor. That action can diminish the competitive edge of the company, and lead to financial losses and the loss of clients. In extreme cases, stolen data might even be used to launch a competing company.

Similar scenarios can also unfold if the IT department neglects its duties by not canceling privileges and access to company systems to former employees, who could then gather information which should no longer be available to them.

In a highly competitive market, an employee with access to the firm's know-how, sensitive customer records or internal data can become a very valuable source of information. This is clear, not only to the organizations themselves, but also to their competitors, who might attempt to turn the employee into a "double agent". Nevertheless, this is yet another rare scenario.

What about the statistics?

The broader picture shows that there have been at least 5,000 confirmed breaches, exposing close to 900 million records worldwide, just in the period since 2005. Of these breaches, over 3,400 (more than 68%) were caused by insiders, unintended disclosure or a physical loss of non-electronic records, or by portable and stationary devices that were lost, stolen or discarded by employees. Of course, this is not a complete list, but rather a conservative one as other reports put the figures even higher, with more than 3,000 confirmed data breaches only in the last year.

The ESET 2015 B2B Survey has confirmed that data loss is one of companies' main concerns: it ranked number one among the cybersecurity risks that respondents had dealt with in the past, and which they considered it important to handle (60%).

The EY Global Information Security Survey 2015 offers similar figures. 56% of participants saw data loss prevention as the area of cybersecurity with the highest priority for the next 12 months. Interestingly, an equal number of respondents (56%) labeled their own employees as the second most likely source of an attack, putting them closely behind criminal syndicates (59%).

PwC's The Global State of Information Security Survey 2016, also marked current and former employees (63%) as the most common originators of cybersecurity incidents.

A large number of breaches go unnoticed

Despite the high frequency of data loss incidents documented in the statistics, it's important to mention that a number of breaches go unnoticed for months, or years, and the volume of data lost is unclear. And some of them are never even discovered.

Also, the majority of lost or stolen USB sticks, mobile devices and notebooks don't even make it into the statistics. Just ask yourself, how often do such incidents occur in your company?

In cases of targeted attacks, if the organization is among the more fortunate ones it stumbles upon the data loss in a cybersecurity audit or receives a warning from security researchers. In such cases, there is still a decent chance of avoiding devastating fallout.

In worse cases – often seen in the breaches reported by the media – data loss incidents are brought to the organization's attention by the cybercriminals themselves, bragging about it online, showing the incompetence of the victim (mostly in case of database hacks targeting state institutions), trying to sell the data or demanding a ransom. At that point, it's much harder for the victim to ameliorate the damage, and it's immeasurably more expensive than a reliable preventive solution.

Costs of breaches

What is the cost of every lost or stolen record containing sensitive and confidential information that an organization has in its databases? It varies from sector to sector, and per country, but, generally, Ponemon Institute's 2016 Cost of Data Breach Study shows that the average record is worth $158, setting the price tag for an average breach at up to $4 million.

However, data loss has more consequences than just financial costs. Secondary losses, caused by business disturbance, damaged reputation or a loss of dissatisfied clients, have their own price, which averages around $1.5 million per incident.

These sums can grow or fall considerably, depending on the country in which the organization operates. Among the 12 countries scrutinized in the aforementioned study, the highest average cost paid per lost or stolen record was in the USA ($221 per record) and Germany ($213), while the lowest was in India ($61).

According to the report, patient data has the greatest value – as high as $355/record – because of its long-lasting character. Information is also high-value in the field of education ($246), followed by pharmaceuticals ($221) and financial data ($208). At the bottom of the ranking is public sector data, with $80 per record.

The current landscape

In today's interconnected world, information has become a powerful commodity, able to affect human lives, send economies into wild fluctuations and bring down the value of company stock in a matter of moments. The combination of this power and the quantity of systems and technologies which organizations use to store sensitive information creates a significant possibility of intentional or unintentional data loss.

While data loss prevention was for a long time the domain of large corporations, the environment is changing. With the growing volume of digitally stored sensitive data in small and medium-sized businesses, the need for appropriate technological tools that are able to control its movement and use has become ever more apparent. And with the advent of industry 4.0, in which electronic documents are preferred over their offline printed versions, this trend is likely to continue in the foreseeable future.

Digitization of government services, as well as the rising popularity of e-banking and e-commerce, are all contributing to this development, producing volumes of public and private data that need protection which no guards at the front door can offer.

However, in the current (and growing) data landscape, we can see that massive breaches aren't as rare as organizations of all sizes would want. Many data loss cases attract attention thanks to the sheer volume of the compromised records, with numbers going as high as tens of millions, occasionally even hundreds of millions, of lost data files.

Others are interesting because it's the public sector that is affected. The public expects its institutions to safely store vast quantities of sensitive citizen/voter information. But the leaks of 50 million records from the Turkish citizenship database, 191 million records from the US voter database, or the entire 55-million voter database of Philippine's Commission on Elections, prove that this doesn't always happen.

Data leaks also grab media attention if the organization operates in a very sensitive industry, such as healthcare. Since January 2015, multiple major breaches have been reported, hitting different US insurers Anthem, Premera Blue Cross, Excellus Blue Cross and CareFirst. According to news reports, more than 90 million patient records were hijacked.

But as mentioned before, the risks do not originate solely from external sources. A report by the Identity Theft Resource Centre mentions several examples of data loss cases involving an insider.

In November 2015, almost 15,000 records were mistakenly leaked from a dermatologist's practice. A spreadsheet containing demographic patient information was sent to a number of patients instead of a customer satisfaction survey. The attachment included sensitive personal data such as name, social security number, date of birth, gender, occupation, contact information and date of last and next appointment.

In the same year, a similar number of records (16,000) was stolen from Children Medical Clinics of East Texas. A disgruntled employee took the business documentation and failed to return it even after being requested to do so by his employer. Further investigation showed that the same worker accessed patients' medical records without authorization as well. He/she took a copy of the data and handed it over to another former employee of the clinic.

But even large banks contain bad seeds. In May 2015, Morgan Stanley had to fire an employee who stole 350,000 records of its wealth-management clients and posted some of the information online. The bank alerted law

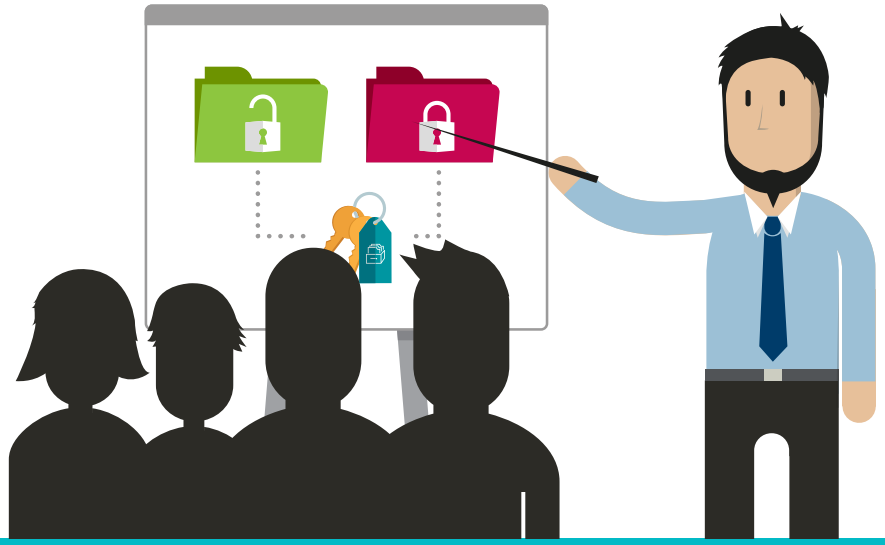
enforcement authorities but found no evidence that customers had suffered any financial loss. The data of about 900 clients was published, but was "promptly" removed, according to the company.

Czech branch of a telecommunications giant T-Mobile has also confirmed an employee attempt to steal and sell its customer marketing data. It probably involved all of its 1.5 million clients, making it the largest known data breach in country's history.

Even careless employees can pose a data loss risk for companies. As documented by an ESET survey in the United Kingdom, around 22,000 USB sticks are lost or forgotten in the laundry every year, together with 970 mobile phones and tablets. Despite the fact that these devices can contain sensitive business information and internal documents, half of them are never returned to their owners.

HOW CAN AN ORGANIZATION PROTECT ITS DATA?

There are several general steps which can be taken by an organization to increase its data security. These can be applied in any case, whether it's in a private company, a public institution or a healthcare facility:



1. **Introduce internal policies and directives**, setting detailed rules for data security and protection. These documents should be clear and easy to understand, stating proper means and processes when handling the data, specifying who is allowed to access particular company systems, databases or sensitive records, and what are the roles and responsibilities for individual employees and departments.
2. Each organization should perform **data classification**, determining which data doesn't require strict regulations, and which data is in need of some level of protection. It's also very important to mark high value data – the so-called "crown jewels" – whose leakage could severely damage the company. Of course, company's data classification can be broader, depending on its specific needs.
3. **Data encryption** is one of the basic precautions, every company should implement to keep its sensitive information safe. ESET DESlock+ Data Encryption is a simple and powerful way to protect data on virtual as well as hard drives, on removable media and in emails. Thanks to minimal user interaction required, it is much easier to achieve employee compliance.
4. **Data responsibility** should be specified in contracts, both with internal staff (either directly in their employment contracts or appendices) and external partners (e.g. as non-disclosure agreements).
5. Trust is good, but control is better. It's advisable to use a reliable data loss prevention solution that audits whether rules are being followed and detects any unusual activities which could result in a future security incident. The same solution can also enforce the rules, giving employees no option other than to use a secure method for handling the data – e.g. using an encrypted external device or the company's private cloud for transferring the data.
6. As mentioned earlier in this whitepaper, many data security incidents are caused by poorly informed employees. **Regular security awareness training** for staff, offering information, advice on best practice and tools for handling internal – and, in particular, sensitive – data, might help mitigate the risk.

7. **Employee motivation and appreciation** is another vital part of breach prevention programs. Building up a respectful and pleasant company culture not only helps to improve staff performance, but also lowers the risk of future damage caused by disgruntled employees.
8. Organizations can also prevent possible insider threats by performing **detailed background checks on all jobseekers and their references**. In case there are any uncertainties or negative findings, the company should, depending on their severity, think twice before employing such a candidate.

What factors should your organization pay attention to?

All the measures mentioned above are essentially worthless without meaningful control. An employer should, therefore, perform regular internal audits with the focus on handling sensitive data, and implement a data encryption such as ESET DESLock+ Data Encryption or use proactive solution to monitor employees' compliance with the rules on data protection, to prevent future incidents.

1. The organization should be aware of how its sensitive data is being handled, and when and where it's being moved or copied. The tools and systems put in place should be able to detect and prevent any attempt by unauthorized personnel to share sensitive data without it being properly encrypted or to send it via public cloud storage facilities.
2. The use of company resources, such as desktop and mobile devices, printers or costly software (e.g. AutoCAD, etc.) should be monitored and optimized, if necessary.

Who deserves increased attention in your organization?

New employees during their probation period are just getting introduced to the company culture and values. Despite this, they already have access to databases and systems that contain valuable internal data and know-how. The risks of intentional or unintentional data loss incident increase even more in combination with low experience and possibly low awareness level of these employees'.

Employees working out their notice period, and employees who are considering leaving company are classified as high-risk subjects in many surveys focused on cybersecurity incidents. With no technological countermeasures applied, they are in a position to steal valuable insider data which can give an advantage to competitors or even allow the establishment of a new competitor. As already shown in statistics, 60% of the employees would take the data from their former company and use it in the future.

However, failure in security can occur at any level, including the highest levels of an organization. Thus, a **basic security audit** focusing on data handling should encompass **all employees**, no matter their rank or the time they have spent in their current position.

HOW CAN ESET HELP?

ESET as a pioneer in the cybersecurity field with almost 30 years of experience, offers a variety of comprehensive solutions targeting data security. Some of them are part of the main portfolio others coming from members of ESET Technology Alliance.

Data encryption

Sensitive data can fall into unauthorized hands by mistake or via loss or theft. To protect it, ESET DESlock+ Data Encryption offers strong encryption for desktop computers, notebooks and other data-storing devices, as well as for cloud or emails.

Data loss prevention

Safetica 7 is a data loss prevention that reveals not only the incident itself, but its wider context as well. With the help of the solution, the client is able to backtrack events before the attack, show how the incident unfolded, and also detect any subsequent actions, thus helping to clarify its causes and consequences. By obtaining this information this solution helps to prevent damaging scenarios in the future.On top of this, the client organization gains a detailed overview and control over its sensitive data. By setting up Safetica Zones mirroring the company environment, the client is able to create rules for handling and sharing of specific data and select which restrictions to apply, and where.

Device management

Using the same tools clients are able to take full control over removable media in the company network, allowing data to come in but not go out on employee devices. This enables customers to eliminate the security threats presented by BYOD (Bring Your Own Device) and build device policies for your entire company.

Productivity measurement

Do you know what is happening in your company? Safetica 7 offers an effective tool – Central Console – providing the client with precise information on what the employees are doing, showing short-term and long-term trends in their performance. This makes it possible to anticipate security and productivity issues in advance.

Activity filtering

With the right information, you will be able to build a more productive work environment, eliminating time-wasting factors. This includes activities like browsing non-work-related websites, or using applications that are not necessary for employees' everyday job.

Is monitoring of employees in accordance with the law?

Monitoring of employees poses a clash between two legal areas – the rights and freedoms of employees and the rights of the employer to protect its own property and interests. As laws and rules in different countries may vary, Safetica provides analysis for specific countries on demand – requests are channeled either directly to Safetica or via network of Safetica's regional distributors.

(The information provided below applies only to the European Union and its member states.)

According to an advisory body of the European Commission A29WP (Article 29 Working Party), prevention is to be prioritized over detection. Therefore, rules prohibiting misuse of company resources are superior to monitoring and searching for insubordination, thus preserving employees' rights. This can be achieved by introducing blacklists of webpages or applications not allowed on the workstations.

Safetica 7 supports this approach via the restrictive functions built into its data loss prevention solution. Monitoring functions – in accordance with A29WP recommendations – should only be applied in case where compelling reasons arise. This includes misuse of company data, information, devices or other resources, and repeated attempts to violate the rules. Safetica 7 also offers option to audit admin rights, restricting their privileges only to the necessary minimum and thus protecting the collected data from misuse.

Employee should be warned about undesirable behavior by software means, such as pop-up windows or other automated warning systems. These functions are implemented in Safetica's solutions and are easy to set up via Safetica Management Console. The strictness of the settings and policies can be adjusted selectively for risk groups (new or leaving employees) and for permanent employees.

Employee monitoring in European Union states should also comply with other basic conditions flowing from EU Directive 95/46/EC:

1. Obtaining the employee's consent where the employer intends to process personal information or conduct monitoring is mandatory.
2. Monitoring should be based upon and ensue from specific events that point to misuse of company data, devices or other resources or from other information-gathering methods traditionally used for employee evaluation. Safetica allows organizations to gather this kind of information via its automated warnings, detecting deviations in employee performance. It can also be set up to notify management immediately, if such patterns emerge.
3. Personal data[1] should only be used for the purpose for which it has been gathered.
4. Transparency towards employees is recommended if monitoring is being applied. One way to handle the situation is to permanently provide each employee with access to gathered materials in the company system. Another approach is to provide detailed information on what is being gathered.
5. Conditions for legitimate and legal monitoring of employees are regulated by specific laws in each country. These are to be found in the national labor code, or its equivalents. Mostly, monitoring of staff is to be based on the employer's legitimate interest in protecting its property from threats and extraordinary circumstances.

Last but not least, personal data stored in the system needs to have a necessary level of protection that has to be maintained during the whole period of its gathering and processing. Apart from protecting this information from unauthorized access, it also has to be protected from mishandling by authorized personnel, which contradicts the rules established in legislation.

1 *EU Directive 95/46/EC: "Personal data shall mean any information relating to an identified or identifiable natural person (...)".*
A29WP (Advisory body of the European Commission): Additional to direct information about the employee, evaluation and other information containing specific elements allowing the identification of employee is also to be regarded as personal data.
In compliance with aforementioned definitions, any data evaluating activities of employees processed by functions offered in Safetica 7 is to be considered as personal data.

CONCLUSION

Statistics and specific cases described in this whitepaper prove that the **threat from insiders** is currently one of the most prominent data-loss scenarios and therefore can no longer be neglected. However, even by following best practice when setting up the internal environment and employer-employee relations, it can be hard to mitigate significant parts of the internal threat.

This, in combination with the growing volume of digitally stored sensitive data in small and medium businesses, the advent of industry 4.0 and the digitization of public services, makes it ever more apparent that appropriate and reliable technological tools able to control data movement need to be in place, in order to fully secure organization's sensitive information.

Encryption (ESET DESlock+ Data Encryption) as a cornerstone of data security combined with data loss prevention (Safetica 7), offer a solution that enables organizations to protect their interests, have full control over the sensitive data and its movement, and measure the productivity of their employees – all in compliance with local regulations.