The Eighth International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbia

PREVENTIVE MODEL OF DATA LEAK PROTECTION IN CRITICAL INFRASTRUCTURE FROM INTERNAL RISK FACTORS

VIKTOR KANIŽAI, PH.D.
OTP Bank, Serbia, viktor.kanizai@otpbanka.rs

Abstract: *The use of information technologies in the critical infrastructure carries a high degree of risk, and therefore there should be payed special attention to the nature of the confidentiality, integrity and availability of the data that information systems of these institutions manage. Unauthorized outflow of information may cause financial and reputational damage, which in the current market may lead to permanent termination of business. It is necessary to establish an adequate model of preventive data leak protection in critical infrastructure from internal risk factors, for the protection to be comprehensive and effective. Risks cannot be completely eliminated, but can be reduced to acceptable levels. The author of this paper presented the three main pillars of the established model.*

Keywords: *data leak, data protection model, business information security, IT security, protection of critical infrastructure*

1. INTRODUCTION

The basis of modern business represents the infrastructure of Information Technology (IT) - databases, communication flows, prompt data processing are necessary and also continuous access to services and products of the company. Taking into consideration the fact that the extraordinary events in the functioning of IT can lead to direct financial and reputational losses, the use of IT infrastructure in the critical infrastructure carries a high degree of risk.

It is necessary to pay special attention to the nature of the confidentiality, integrity, and availability of data which is managed by information systems of these institutions, as well as the dangers that threaten their functionality.

2. INTEGRATED MODEL OF DATA PROTECTION IN INFORMATION SYSTEMS OF CRITICAL INFRASTRUCTURE

The primary focus of protection should be the data, not a computer, computer network or computer system. The ultimate goal is to protect the data itself, regardless of where they are stored or where they are processed.

The most basic division of protection includes preventive and repressive protection. Repressive aims to establish the actual facts of the case of an extraordinary event that has already occurred or whose execution is threatening the security of data, and to propose measures so that such and similar events in the future would not be repeated. Preventive protection aims to prevent the occurrence of an incident and always has priority over repressive protection - it is always "better safe than sorry".

Data protection should cover all forms of data: voice, paper and electronic. It is necessary to pay attention to business talks with other parties, on the environment of the conversation, unauthorized persons not to hear the contents of the conversation and thus obtain access to the data of which the person is not authorized by his/her working position. Also, it is necessary to apply the "clean desk policy", i.e. not to leave documents on the desk after working hours so that unauthorized persons couldn’t get hold of the information contained in the printed material. The data in electronic form is the most difficult to guard, defining their protection requires a lot of expertise in the complex field of cybercrime. There is a noticeable increasing trend of high-tech espionage and warfare, as well as targeted attacks on "plain users" (i.e. ransomware virus - hides (encrypts) files on the user's computer and requires payment of a sum of money for the data to be returned).

Data protection should cover not only technology, but also human resources and business processes.

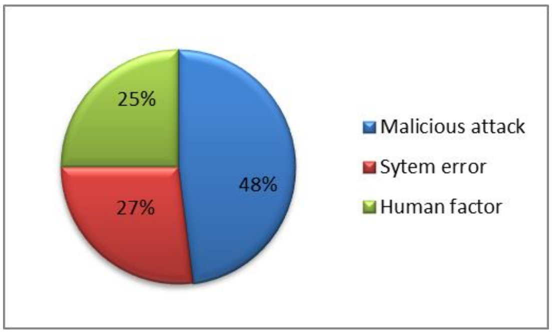


Image 1: Cause of security breach of data [1]

In addition to well-known headlines regarding unauthorized outflow of government information via WikiLeaks and Edward Snowden, we have also witnessed headlines about data leak events in companies (eg. JP Morgan [2], Citigroup [3]), at social networks (eg, Facebook [4]), on online services (eg. iCloud [5]), etc. It is necessary to pay special attention to the establishment of an adequate model to detect and prevent unauthorized outflow of information, especially in the critical infrastructure, because they handle sensitive and particularly sensitive data.

Unauthorized outflow of information can cause material and reputational damage to the critical infrastructure, which in the current market can lead to permanent closure of business.

To establish an adequate model of protection from unauthorized outflow of information it is necessary to answer the following questions:

- Where are we now?
- Where do we want to get?
- How do we want to reach the goal?

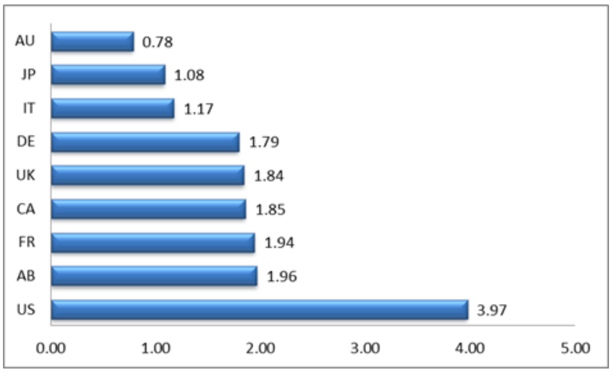


Image 2: Average operating loss due to breach of data security in nine countries in mill. US$ [1]

3. PROTECTION FROM DATA LEAK THROUGH HUMAN RESOURCES

When it comes to unauthorized outflow of data, employees and external partners who have access to data pose the greatest threat.

Often data leak happens because of high-risk steps of employees who are not aware of the possible consequences of their actions.

Typical examples of behaviour of employees indicating the lack of diligence with regard to the safeguarding of sensitive data include loud talk about confidential information in public places, not logging off from workstations, leaving passwords in sight or unprotected, and access to unauthorized web pages. Especially big threat in this area comes from employees who are losing corporate devices such as laptop computers, mobile phones, and storage devices, or the devices have been stolen because of inadequate storage. Employees who are dissatisfied or who are trying to illegally obtain material gain for themselves or for another, represent a particular challenge in the fight against unauthorized outflow of information.

Legitimate network access and mobile devices enable disloyal employees to allow the outflow of corporate data. Some workers simply do not return company devices when they leave their job. This can be expensive and dangerous for the company, because it adds another path for data loss.

Even if only 5 percent of employees who leave the workplace takes the device with him, in the company of 1,000 employees this means 50 such workers. For larger organizations risk and financial losses are far more significant [6].

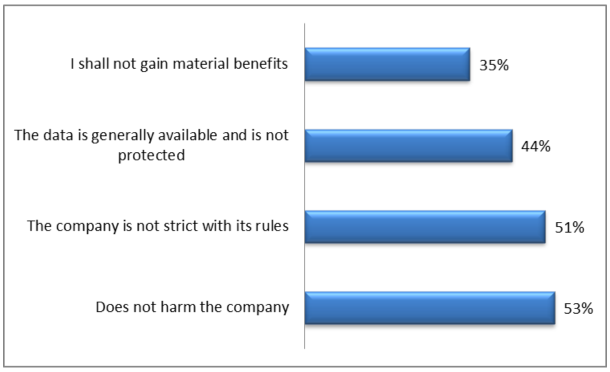


Image 3: The most common reasons due to which employees believe it is acceptable to take business data[7]

4. IT SECURITY TRAINING OF EMPLOYEES FOR DATA LEAK PREVENTION

Safety training of employees in critical infrastructure should primarily be aimed at raising awareness on the protection of data and IT during business. In order for training to be effective and successful it is necessary to previously examine the following aspects:

- The sensitivity (vulnerability) of IT that are of particular importance for the business,
- The effect of new technologies onto the protection of right to privacy, protection of trade secrets, personal data, etc.,
- The role of government and legislation in protecting data and IT,
- The application of standards in the field of IT security in corporate environment and in society in general.

In order for training to be successful people should be aware of the need for training.

Safety training on protection against unauthorized outflow of information should be aimed at raising awareness of employees about the need for security which is equal to business success. Through training it is needed to give clear answers to the following questions:

- What should be protected?
  The answer to this question involves determining the objects of protection. Protection of an object can involve: data on employees, customer data, business data, databases, etc. This is essentially the first and crucial step in training and clarifying the problems of protection in the field of IT in the critical infrastructure. People need to be especially aware of what to protect and what the values that should be protected are.
- What and who should protect data and IT in the critical infrastructure?
  The answer to this question involves the identification of risks, threats that more or less can compromise data and IT in critical infrastructure. These can include the following threats: force

majeure (earthquake, flood, fire, etc.), hardware and software shortcomings (hardware failure, software bugs, etc.), human-factor unintentional mistakes (negligence, carelessness, poor organization, incompetence, fatigue, etc.), human factor with intention (theft, sabotage, revenge, revealing business secrets, hacking, phishing, creating and distributing viruses, etc.), sources of threats from the environment (extended loss of electricity, air pollution, etc.). Through security training employees must be aware of the threats and risks to better protect data and IT in critical infrastructure.

- Why should data and IT be protected in critical infrastructure?
  Possible consequences should be determined of the loss, or damage that critical infrastructure may have from exploiting one of the threats. Here we establish the damage, consequences or loss for the critical infrastructure that may arise due to the realization of threats to objects of protection. These consequences may include partial or complete physical damage (hardware, software, data, etc.), theft (hardware, software, data, reports, information, etc.) and modification (hardware, software, data, reports, information, etc.). Generally speaking, the consequences are breaching: integrity, availability and confidentiality.

- What to protect data and IT in the critical infrastructure with?
  The answer to this question involves the choice of measures and resources that will be used to protect data and IT in critical infrastructure. Data protection and IT security in critical infrastructure can be seen as: normative regulation, measures of physical-technical security, logical security, security staff training and security control – monitoring.

- How will data and IT be protected in critical infrastructure?
  This also includes a clear definition of IT security policy of the institution, IT security strategy, the development of internal normative acts, organizational structure. A clear answer to this question involves training employees on the use of modern methods and means for the protection of data and IT in critical infrastructure.

All should have the primary goal of raising awareness about the need for protection and IT security in critical infrastructure. The importance of training is enormous because employees become safer and thus more effective in their work.

The modern form of training involves the use of cyclic learning. Training should be based on the application of modern technology with involvement of highly specialized professionals in this field. Training should be active, to be based on encouraging and directing.

The training should include an analysis of experiences, both locally and globally. Training must be comprehensive, well-planned and organized in order to avoid certain types of commercial training, by offering short-term courses, one-day or half-day training often by incompetent agencies and individuals. It is necessary to have direct cooperation between scientific and educational institutions with market operators, which should be well planned and organized in order to carry out quality training in the field of data protection.

The form of training in which users play active roles is the most effective way to meet the requirements for expert training, increase knowledge and awareness of data protection.

Training is the most effective preventive measure to protect data. If users have adequate awareness and knowledge in the field of data protection, then the actual execution of activities through IT is safer, regardless of the technical - technological solutions of protection. We should not forget, the first lines of defence are the users themselves.

5. TECHNOLOGICAL SOLUTIONS FOR PREVENTING UNAUTHORIZED OUTFLOW OF DATA

Technological solutions are used for policy enforcement, monitoring and warning on violations of security provisions, as well as to ensure data protection. They manage the risk of data loss, regardless of whether the event occurred intentionally or due to human error.

Technological solutions to prevent unauthorized outflow of information include:

- Tools for encryption,
- Antivirus protection,
- Firewall protection,
- Intrusion Prevention System,
- Tools to test on vulnerabilities,
- Web filters, and so on.

To detect events, DLP solutions commonly use the following principles:

- Described data: keywords, file types, data identifiers, etc.; attributes of the sender or recipient.
- Fingerprinted data: structured data, unstructured data.

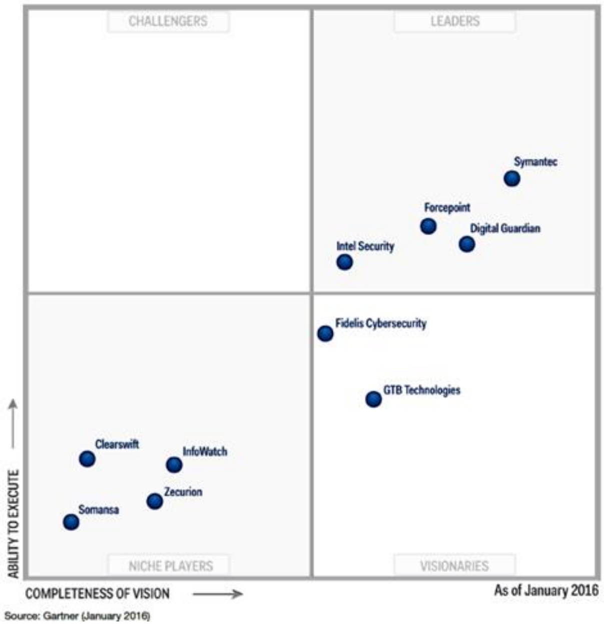
The most important element of technological solutions is a dedicated solution for preventing unauthorized outflow of data (Data Loss Prevention - DLP solution). It is defined as a product which on the basis of centralized sets of rules identifies, monitors and protects data at rest (storage - file servers, databases, web servers, etc.), motion (network - e-mail, web, FTP, instant messaging etc.), and processing (workstations - computers, printers, data carriers, etc.), through a detailed analysis of the content.

When the DLP solution detects a suspicious event, it usually applies one of the following measures:

- Notifications: sending e-mails to the sender / manager / IT Security Department; pop-up windows; syslog alerts, etc.

- Blocking: blocking the SMTP, HTTP / S, FTP, IM, etc. traffic; blocking further use of peripheral devices, such as USB / CD / DVD, printer / fax, etc.
- Modification: modifies the data traffic itself in terms of encrypting sensitive data.
- Relocation or copying stored files.

There are many dedicated DLP technological solutions on the market, and the author of this paper wouldn't favour any one of them. Instead, Gartner's estimates on these solutions are shown below, on Image 4.



Source: Gartner (January 2016)

Image 4: Gartner's estimates on DLP solutions [8]

6. PROTECTION FROM UNAUTHORIZED OUTFLOW OF INFORMATION THROUGH BUSINESS PROCESSES IN CRITICAL INFRASTRUCTURE

For the DLP to be complete, it is necessary to protect business processes as well in the critical infrastructure. What is important to emphasize is that protection represents supporting process in terms of business operations, and as such should not distort the expected business processes which bring profit to the institution. Protection should not be a burden for the business of institutions which would break or permanently stop the business processes, but should protect them. Of course, sometimes the easiest way is to completely shut down some processes with the excuse that they carry a high degree of risk, but in this case it is not the goal, but to be in line with business requirements and find optimal solutions for the business processes to flow as expected, and at the same time they would also be secure.

For existing processes, it is necessary to conduct comprehensive and detailed risk analysis, identify possible points of unauthorized outflow of information. The most trivial examples are Internet access and the ability to use removable data carrier. The best and easiest way would be to prohibit access to the Internet completely and prevent the use of any removable media, i.e. to close the information system of the institution in such way. But business needs impose and require constant access to the Internet and peripheral devices for storage and transfer of data. This is why in this case the protection means limiting, not abolition. And limitation means determination of who can access all content on the Internet and in what period of time, who can have the ability to use USB memory temporarily or permanently, and so on. On the other hand, there is the monitoring of those streams of data with the help of technical solutions to prevent unauthorized outflow of information, as described in the previous chapter of this paper.

In new business processes that are yet to be defined and introduced, it is necessary prior to their implementation to assess possible risks regarding the unauthorized outflow of information and mitigate identified risks by appropriate measures that will be part of the new business processes.

In this, and in all matters, the support from top management is essential. Without this support, all of the above will not function properly; it may be achieved that internal documents would cover the matter of DLP, but in practice it will not be implemented as intended. It is necessary for management, given the potential threats and losses, to invest into the protection of data from unauthorized outflow, and it shouldn't be seen as inevitable cost but as an investment into the security of business processes. On the other hand, it is also inevitable for the protection not be a disabling factor for business processes, but a factor that will make safe operation of institutions on the issue of unauthorized outflow of information.

7. CONCLUSION

The use of IT infrastructure in the critical infrastructure carries a high degree of risk, and therefore special attention should be payed to the nature of confidentiality, integrity and availability of the data that information systems of these institutions manage. Unauthorized outflow of information may cause financial and reputational damage, which in the current market can lead to permanent closure of operations.

The preventive model of data leak protection in critical infrastructure from internal risk factors, which is designed and presented in this paper, includes not only technology, but also human resources and business processes.

The greatest emphasis in this paper is on human resources, because employees in critical infrastructure constantly have access to the information that the institution stores and processes in accordance with and due to the nature of work performed, and are therefore they are the weakest link in the system of protection against unauthorized outflow of information. But from the other side, they also represent the first line of defence.

REFERENCES

[1] Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute

LLC, “2016 Cost of Data Breach Study: Global Analysis”, June 2016.

[2] “JP Morgan suffers data breach affecting 76 million customers”, http://www.itgovernanceusa.com/blog/jp-morgan-suffers-data-breach-affecting-76-million-customers/, last accessed on 10.07.2016.

[3] “Citigroup Suffers Massive Data Breach In Japan”, http://www.huffingtonpost.com/2011/08/08/citigroup-suffers-another_n_920862.html, last accessed on 09.07.2016.

[4] “Facebook Data-Leaking Bug Exposes 6 Million Users' Data”, http://www.infosecurity-magazine.com/news/facebook-data-leaking-bug-exposes-6-million-users/, last accessed on 09.07.2016.

[5] “2014 celebrity photo hack”, http://en.wikipedia.org/wiki/2014_celebrity_photo_hack, last accessed on 10.07.2016.

[6] Cisco Systems, Inc, “Data Leakage Worldwide: The High Cost of Insider Threats”, 2008.

[7] Symantec Corporation, “What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk”, 2013.

[8] Gartner, Inc., “Magic Quadrant for Enterprise Data Loss Prevention”, 28.01.2016.

[9] An Osterman Research White Paper, “Best Practices for Dealing with Phishing and Next-Generation Malware”, April 2015.

[10] Jeffrey Roman, “Morgan Stanley: Insider Stole Data – BankInfoSecurity, Employee Posted Some Client Information Online”, http://www.bankinfosecurity.com/morgan-stanley-insider-stole-data-a-7750, last accessed on 05.06.2016.

[11] Vormetric, Inc., “The Insider Threat, How Privileged Users Put Critical Data at Risk”, 2013.