Interested in learning more about security?

SANS Institute InfoSec Reading Room

Preventing data leakage: A risk based approach for controlled use of the use of administrative and access privileges

Organizations invest resources to protect their confidential information and intellectual property by trying to prevent data leakage or data loss. They adopt policies and implement technical controls to stop the loss and disclosure of sensitive information by outside attackers as well as inadvertent and malicious insiders. They follow best practices like the Critical Security Controls, specifically Control 12 (Controlled Use of Administrative Privileges) and Control 17 (Data Protection), to prevent the unauthorized...

Preventing data leakage: A risk based approach for controlled use of the use of administrative and access privileges

GIAC GCCC Gold Certification

Author: Christoph Eckstein, christopheckstein.sec@gmx.net

Advisor: Richard Carbone

Accepted: August 10, 2015

Abstract

Organizations invest resources to protect their confidential information and intellectual property by trying to prevent data leakage or data loss. They adopt policies and implement technical controls to stop the loss and disclosure of sensitive information by outside attackers as well as inadvertent and malicious insiders. They follow best practices like the Critical Security Controls, specifically Control 12 ("Controlled Use of Administrative Privileges") and Control 17 ("Data Protection"), to prevent the unauthorized leakage and disclosure of sensitive information. One type of data loss or data leakage prevention controls includes endpoint protection solutions to stop file transfers to USB storage devices or file uploads to public websites. However, the larger and more complex the business and organization the more users that may be granted exceptions to these policies and controls in order for them to be able to fulfill their job related tasks. The approval of these exceptions is often solely based on the business need for the individual user. This raises the question of how an approval for an exception does influence the risk of data leakage for an organization? What is the specific data leakage risk for granting an individual user a certain exception? This paper presents a new approach to risk based exception management, which will allow organizations to grant exceptions based on inherent data leakage risk. First, this paper introduces a concept for evaluating and categorizing users based on their access to sensitive information. Then in the second step, a ruleset is defined for granting exceptions based on the categorization of users, which enables individual approvers to make informed decisions regarding exception requests. The overall objective is to lower the data leakage risk for organizations by controlling and limiting exceptions where the access and thereby potential loss of information is the highest.

1. Introduction

Over the last few years many organizations across all different sectors have seen sensitive internal information stolen, lost or purposely leaked (Garg, 2015). This data loss or leakage is, through theft or loss, intentional or unintentional, has caused organizations to lose millions, if not billions, of dollars in direct and indirect costs (Verizon, 2015). Furthermore, their reputation and brands may have suffered great damage. The majority of data leakage incidents is caused by internal users and trusted third parties, including intentional and unintentional leakage (Ernst & Young, 2011). To protect against data leakage many organizations implement various kinds of data leakage prevention (DLP) solutions (Coles, 2014). The goal is to limit and control the users' ability to transfer information or data off the organization's network to non-organization-owned devices. For example, organizations might want to block the users' ability to copy internal and potentially sensitive information to mobile storage devices or to upload data to public file sharing or storage sites. By controlling and limiting the transfer of data, organizations aim to not only reduce the risk of internal users intentionally or unintentionally disclosing sensitive information, but also to reduce the risk of external attackers using these file transfer capabilities after successfully compromising user accounts. One way to implement such technical controls is to follow the Critical Security Controls published by the Council of Cyber Security. In particular, Control 17 (i.e. "Data Protection") focuses on preventing data leakage. Additionally, Control 12 (i.e. "Controlled Use of Administrative Privileges") focuses on administrative privileges, which could be misused by users to deactivate DLP controls and should therefore be strictly limited (Council on Cyber Security).

Although DLP solutions provide the ability to limit and control the transfer of data, organizations most likely allow particular users to be excluded from a specific control on a case-by-case basis. For example, IT staff members might need to be able to use USB storage devices to be able to reinstall systems from preconfigured images. The problem is that such exceptions are often granted solely on a business need. However, limiting exception granting to the business need completely ignores possible inherent data leakage risks. For example, granting a user a USB storage device exception provides

him the technical capability to transfer information out of the organization and cause data leakage. Therefore, the decision whether to grant this USB storage device exception should include the potential risk for the user disclosing or leaking sensitive information.

This paper illustrates a new risk based approach for granting DLP exceptions and administrative privileges. The approach enables line managers to not only grant exceptions based on the business need, but also on the inherent data leakage risk. To achieve this, this paper introduces a two-step approach. In a first step, users are categorized into different risk groups based on their inherent data leakage risk, which is determined by their access to sensitive information. In a second step, rules are defined for each of these risk groups. These rules determine which risk groups are allowed to be granted which type of DLP exception or administrative privileges. Knowing the risk group of a user and the permitted DLP exceptions for that specific group thereby enables line managers to make informed decisions on whether to grant certain DLP exceptions. Furthermore, this approach creates awareness and accountability for line managers when granting exceptions with unacceptable risk (i.e. exceptions that are not allowed for a user in a specific risk group).

To demonstrate the concept for this two-step approach this paper particularly focuses on information or data leaked through file transfer via mobile storage devices and web uploads, as well as administrative privileges. However, this paper does not provide a guide for choosing or implementing a DLP solution. The concept rather serves as a template for organizations to adjust and customize the approach according to their different individual environments, requirements, and goals.

2. Data leakage

Data leakage is the unauthorized transmission of information (or data) from within an organization to an external destination or recipient (i.e. the unauthorized removal of information out of the control of an organization). This may be by electronic or physical means. “Unauthorized” in this context does not automatically mean the data leakage by the user was intentional or malicious. Unintentional or inadvertent data leakage by internal users is also considered unauthorized (Gordon, 2007). Data leakage is

also known as data loss or data exfiltration. However, data loss also includes the loss or destruction of information due to hardware failure or destruction, which is not in scope for this paper.

Recent incidents have shown that data leakage caused by internal users is at least as much a threat as data leakage caused by external attacks. There is one incident where a single disgruntled internal user of a Swiss bank leaked bank account information of more than 2,000 prominent individuals (Ernst & Young, 2011). New studies even state that data leakage by internal users has the potential to cause greater financial losses than external attacks. Furthermore, 39 percent of IT professionals are more concerned about internally caused data leakage than the threat of external attackers (Cisco Systems, Inc., 2008). The financial damage or cost caused by data leakage incidents may range from 90$ up to 300$ per record lost in high-profile cases in regulated industries according to research (Forrester Research, Inc., 2010). Costs may include direct losses due to tangible damage that is measurable or quantifiable, as well as indirect losses. Direct losses, for example, are fines resulting from violations of regulations (such as protecting customer privacy) or costs for investigations and disaster recovery. Indirect losses are much harder to quantify and may have a much broader impact. These may include reduced share price because of negative publicity; damage to an organization's reputation and resulting loss of business; or exposure of intellectual property to competitors (Shabtai, Elovici, & Rokach, 2012).

In addition to reducing or mitigating data leakage incidents for financial and business reasons, organizations may be obliged to adhere to various regulatory requirements enforcing the prevention of data leakage. Depending on the industry, examples of such regulations are the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), California's data-breach disclosure notification law SB 1386, the Payment Card Industry Data Security Standard (PCI-DSS) and the Sarbanes–Oxley Act (SOX) (Shabtai, Elovici, & Rokach, 2012).

3. Data leakage prevention and exception management

3.1. Data leakage prevention

According to the Critical Security Controls (Control 17) "data loss (i.e. leakage) prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework" (Council on Cyber Security).

To effectively implement such a comprehensive approach to prevent data leakage, organizations should consider implementing multiple elements, which include data governance, risk assessment, regulatory and privacy compliance (Brun & Faske, 2010), data or information classification, policies, standards, procedures, data discovery, remediation processes and training and awareness (Hamilton). The ultimate goal to prevent data leakage, however, is to stop sensitive information from leaving the organization unauthorized (i.e. being leaked). There are numerous possible vectors through which information or data could potentially be leaked. Some common vectors for data leakage are email, instant messaging, social media, file transfer, web pages (e.g. blogs, wikis, forums and personal file storage sites), mobile storage devices (e.g. USB sticks) and hard copies (e.g. printouts) (Ernst & Young, 2011).

For example, internal users posting sensitive information on social media poses great danger for organizations (Friedel, 2014). Referring especially to social media, organizations want to prevent intentional and unintentional data leakage. Consider that users might not always be aware of the possible damage caused by posting apparently insensitive information on social media sites. The greater danger, however, is with intentional leakage. In one case, an internal user stole nearly 2 million customer data records over a period of 2 years. The user used a USB stick to transfer the data, 20,000 records each week (Utter, 2008).

The basis for data leakage prevention is to implement an information classification scheme that identifies sensitive information organizations want to protect (Furness, 2004). For example, an information classification scheme might define classes

like “internal”, “confidential” and “highly confidential,” while highly confidential information poses the greatest financial and reputational risk if leaked. Furthermore, a robust policy framework and user awareness training are integral parts of data leakage prevention. However, ultimately organizations need to deploy DLP solutions to enforce their policies and effectively prevent data from leaving the organization (Mehta, 2014)., DLP solutions installed on a user workstation can for block users from transferring files out of the control of the organization (Info-Tech Research Group, 2011).

3.2. Exception management

By implementing policies and DLP solutions, organizations aim to prevent data leakage through controlling information or data transfer. Ideally, organizations want to block all file transfer capabilities for all users on all devices. However, in reality, there are situations in which there is a valid business need for excluding specific users from DLP controls. For example, in situations where information needs to be exchanged with external third parties, an exception might have to be granted for the DLP solution to allow certain data transfers (e.g. file transfer to a USB storage device). Such a situation might include information provisioning to external auditors, law enforcement, and government agencies. Additionally, internal teams for incident response, cyber investigations, software development or IT support may rely on certain capabilities like mobile storage devices to fulfill their job tasks.

While organizations might not be able to block all file transfer for all users, they should control, audit, review and recertify exceptions (i.e. they should employ exceptions management). To establish processes for requesting, granting, tracking, recertifying, and revoking exceptions, organizations need to limit exceptions, monitor and log activities of users with known exceptions. However, granting exceptions is often based solely on a business need. A user’s line manager usually approves an exception request based on the user’s need to perform a specific job task. Even if other technical solutions might be available or easily deployed, users and line managers typically opt for an exception as the most convenient solution. But how can organizations manage exceptions more effectively? How can they create an approval process that enables and encourages line managers to make better decisions? How to enable line manager to approve exceptions

based not only on the business need, but also on the inherent risk of data leakage for the organization? Organizations should primarily create awareness for the actual data leakage risk involved with DLP exceptions. Secondly, ensuring transparency for existing and potential data leakage risks across business units and teams enables their users to take necessary means to protect sensitive information.

This risk based approach to exception management presents a concept which enhances traditional "business need" approval processes to include data leakage risk; thereby not only making line managers aware of the inherent data leakage risk, but enforcing non-deniability. Because line managers are being made aware of the inherent data leakage risk, they can be made accountable in case of an incident. In addition to enhancing the approval process, organizations are able to focus their risk mitigation efforts on areas with most data leakage risk. They can specifically target and remove DLP exceptions that pose the highest risk of data leakage.

4. Risk based approach to exception management

4.1. Concept

The risk-based approach introduced in this paper is a new concept developed to enhance exception management to effectively reduce the data leakage risk. The idea behind the risk-based approach to exception management is to create transparency by introducing a concept that assesses and transpires the risk of data leakage on an individual user basis. Furthermore, by creating that transparency organizations are able to actively reduce the risk of data leakage by enforcing rules that prohibit DLP exceptions for high-risk users. High-risk users are categorized by their access to sensitive information. Additionally, transparency creates accountability for line managers and organizational units regarding the risk they are accepting by granting exceptions to their users. This is because line managers and organizational units cannot deny knowledge of inherent data leakage risks. Regular reporting informs all stakeholders of data leakage risks and existing exceptions. If a data leakage incident for a reported risk occurs, the responsible manager would have to justify why he did not remove a certain exception that led to the incident, although he was made aware of the inherent risk.

This risk-based approach supplements or extends an existing DLP exception granting process. It does not replace it. Even if it would be considered very low data leakage risk to grant a specific exception to a certain user, it does not substitute the need for a valid business need for example. This means that just because there is no apparent data leakage risk, it does not mean exceptions should be granted. Exceptions are still an exception to a policy and should be treated as a last resort. In other words, data leakage risk might just be one of many criteria organizations define in their policies regarding granting of exceptions.

4.2. Requirements and assumptions

To be able to implement this risk-based approach, organizations have to meet certain preconditions. The assessment of the data leakage risk is based on the availability of certain information within the organization. The actual information needed depends on the individual scope an organization might define for implementing this risk-based approach.

The first step and most crucial requirement for this risk-based approach should be the classification of information within the organization, as mentioned earlier. Without knowing what sensitive information an organization owns and where it is stored, the risk of leakage of that sensitive data cannot be assessed (ISACA, 2010). Additionally, organizations must have some kind of access management system or repository that lists all access to all of sensitive information for each user. As exceptions to the DLP solution are granted on individual user basis, organizations must know the individual user's access to sensitive information to be able to assess the risk with granting exceptions.

4.3. Scoping

This paper does not present a complete or holistic approach ready to be deployed, but an initial guidance and some first steps that can be employed in managing data leakage. As every organization has its own environment and challenges, each has to adjust and customize this approach to meet their specific requirements, needs, and goals. The concept presented in this paper can be adapted and extended, and it needs to be said that this can also create more complexity.

For the purpose of this paper and for simplicity, the following exceptions have been selected to provide some practical examples to demonstrate a risk based approach.

4.3.1. Mobile storage device exception (authorized and encrypted USB mobile storage devices)

Many businesses today require storage and transportation of data via mobile storage devices. For example, an organization might be obliged to provide large amounts of documents to external auditors. A system administrator might need to transport data from and to a crucial system not connected to the network. In such cases, organizations might allow a user to request and use authorized and encrypted USB mobile storage devices provided by the organization. The user is granted an exception to write on these authorized storage devices only. Devices are encrypted and can only be accessed with a security passcode. With the respective passcode, the mobile storage devices can be read from every system. Although the information is encrypted and therefore protected while transferred on the authorized mobile storage device, the data is out of control of the organization as soon as it is copied off the device to a third party system (Silowash & Lewellen, 2013). This means there is a data leakage risk.

4.3.2. Unrestricted USB

Although there already is an exception for authorized USB mobile storage devices, there might be the need for unrestricted USB connectivity. For example, organizations might operate business critical and highly sophisticated printing machinery, which is controlled via a USB connection. Ideally, the IT department would be able to install and allow just this specific machinery to be able to be connected to a specific workstation. However, this might not always be possible. In such special cases, an unrestricted USB might be granted to allow business operations. However, the exception would also allow the user to connect any unauthorized USB devices, including mobile storage devices. In this case, the user would be able to copy any data or information off the organization's network.

4.3.3. Web filter and web upload

Data leakage via web application or web traffic is a common vector (Ashford, 2014). Although organizations should deploy network based intrusion prevention systems for egress filtering, blocking certain websites as well as the ability to upload files adds an additional layer of protection. Furthermore, organizations may not only want to block websites with inappropriate and undesired content, but also websites that provide the ability to share potentially sensitive information (Leyden, 2003). Some examples include social media sites, blogs, forums, and public file storage sites. By blocking access to such sites, organizations can reduce the risk of users posting sensitive information (e.g. a software developer posting program code of internally developed software). However, organizations are not able to block every site used for file sharing. Blocking web uploads or file uploads to websites at least reduces the risk of users transferring whole documents or files (Chitchyan, 2014).

Web filtering and blocking web uploads are two different controls (i.e. web filtering is usually implemented through an internet proxy server, web uploads are blocked via a DLP solution on workstations). However, one exception might not work without the other. For example, if a user wants to upload a file to a public file storage site, he would need both a web filter exception to be able to browse to that site as well as a web upload exception to be able to upload files.

4.3.4. Administrative privileges

Controlling administrative privileges is an essential part to secure the organization's network and systems (Council on Cyber Security). Although administrative privileges are not directly controlled or managed via a DLP solution, they have a potential impact on the operation of a DLP solution. Administrative privileges might not be directly a source of data leakage. However, a user with administrative privileges might potentially be able to disable any DLP solution installed on the user's workstation. Furthermore, a user with administrative privileges might circumvent end-point protection mechanisms. For example, a user could potentially install file transfer applications which would enable them to transfer files via protocols like FTP or SSH. A user may change the system configuration to be able to connect to insecure networks, like

unauthorized public wireless networks. Furthermore, a user could install a new printer or printing service on their workstation to be able to print physical copies of sensitive information. Therefore, administrative privileged should be strictly monitored by organizations, as they should grant users the ability to potentially alter the system in a way that can disable or circumvent data leakage controls in place.

4.4. Approach

4.4.1. Overview

The concept introduced in this paper for implementing a risk-based approach to exception management is a two-step approach as shown in Figure 1: Risk based approach overview. Firstly, all users are categorized in different groups depending on their level of data leakage risk. The categorization is based on the users' access to sensitive information. Secondly, a ruleset is defined which specifies the exceptions acceptable for each of the groups of categorized users. Rules for lower risk groups also apply to higher risks groups, i.e. a user in the very high risk group is also subject to rules for the high risk and low risk groups. One rule, for example, would be that high risk users are not allowed to have unrestricted USB access.

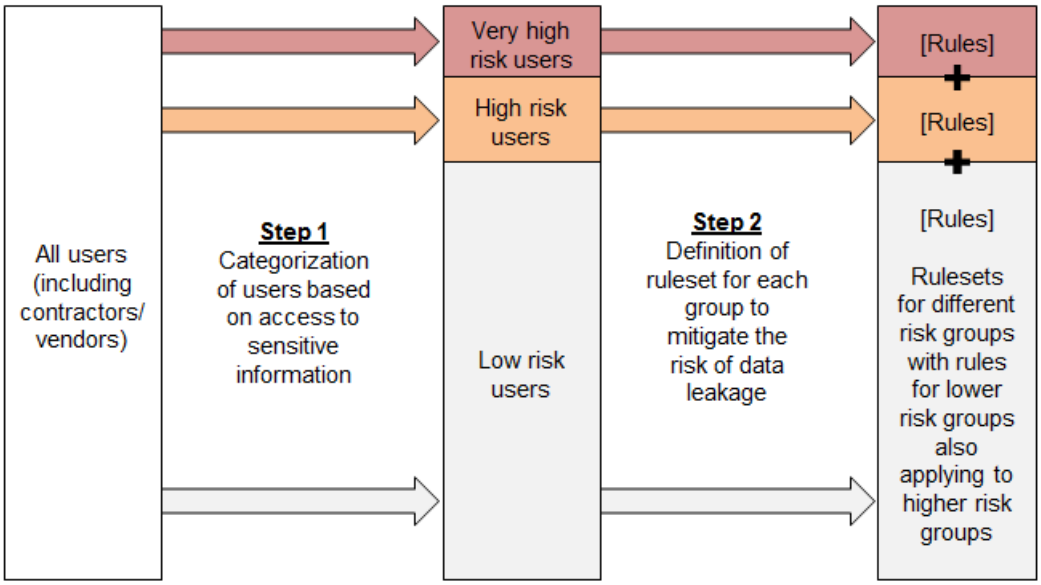

Figure 1: Risk based approach overview.

Based on the categorization of users and the ruleset defined for each group, line managers are thus empowered to grant or deny DLP exceptions based on the data leakage risk of the user. For example, a user that is categorized to be in the low risk group might be allowed to have an Unlimited USB exception. Of course, assuming other valid business criteria is met. However, a user that is considered to be in the high-risk group is denied an Unlimited USB exception. Being in that high-risk group indicates that there is a higher risk for the organization regarding data leakage if that user has an Unlimited USB exception. The reason could be that this user has access to specific sensitive financial information that cannot be leaked to competitors.

The two steps are explained in more detail in the following sections. Keep in mind that this illustration is a simplistic approach to demonstrate the concept.

4.4.2. User risk categorization

The risk of data leakage is assessed on an individual basis by evaluating the user's access to sensitive information. The approach or user categorization is therefore information centric and focuses on sensitive information and who has access to it. Of course, all users might have access to some kind of sensitive or internal information. However, limited resources force organizations to focus on the most significant risks. In this example, organizations concentrate on preventing the leakage of the most confidential information. This does not mean, however, that organizations can customize this approach to the level they feel is appropriate to fulfill their requirements. Organizations have to define their own information classification scheme and adjust this approach accordingly. Organizations may choose to define more or less risk groups when implementing this approach to meet their requirements and goals.

To illustrate the approach Figure 2: Categorization of users into risk groups shows was being split into three risk groups. Assuming the information classification scheme defines two types of sensitive information (e.g. "confidential" and "highly confidential"), users with access to confidential information are in the high risk group. Users with access to highly confidential information are in the very high-risk group. All other users with no access to these two types of sensitive information are in the low risk group. Other types of information might for example include information classified as "internal" or "public."

Although other internal information might also be worth protecting, the idea here is to focus on most sensitive information to effectively use available resources. However, organizations will have to define their own scope.

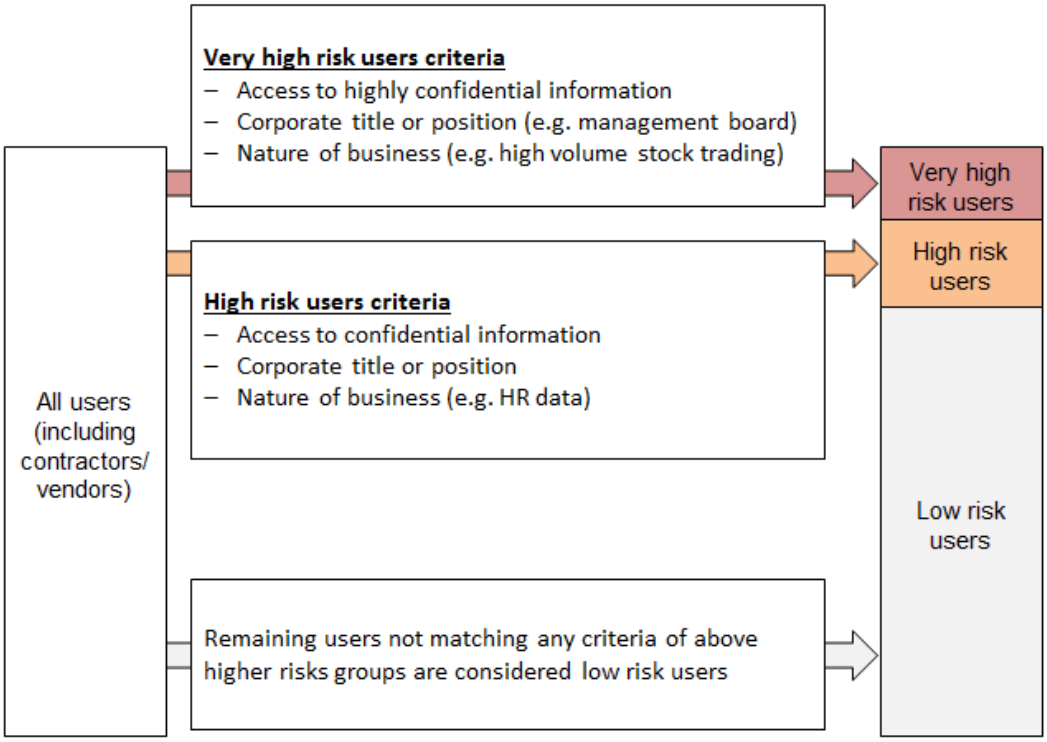

Figure 2: Categorization of users into risk groups.

Additionally, other criteria like a user's position or corporate title and the nature of their business can be added to the categorization. For example, in many organizations it can be assumed that senior executives or board members have access to more sensitive information than IT developers do. Likewise, high volume stock traders in a bank or HR staff have inevitably access to more sensitive information due to the nature of their business. For example, in the figure shown above, a stock trader, even though he is not an executive, is categorized as "high risk user." This is because the stock trader has access to highly confidential market transactions, which may cause financial and business losses if leaked, but also due to the potential breach of regulations and resulting lawsuits and regulatory fines.

Another example is a user working in HR who is categorized as a high-risk user. Leaking confidential employee information might still cause financial loss due to

breaching data privacy regulations and again resulting in regulatory fines, but the amount in this case may be less. Again, organizations have to assess and specify their individual financial and business risks and thresholds.

4.4.3. Definition of ruleset

In general, every user is allowed to have any exception if there is a valid business need. If a user is considered to be in a higher risk group as shown in Figure 3: Definition of ruleset for different risk groups, certain types of exceptions are prohibited. Equally, it does not mean that a user is allowed any exception if he is not in one the high-risk groups – there still has to be a valid business need.

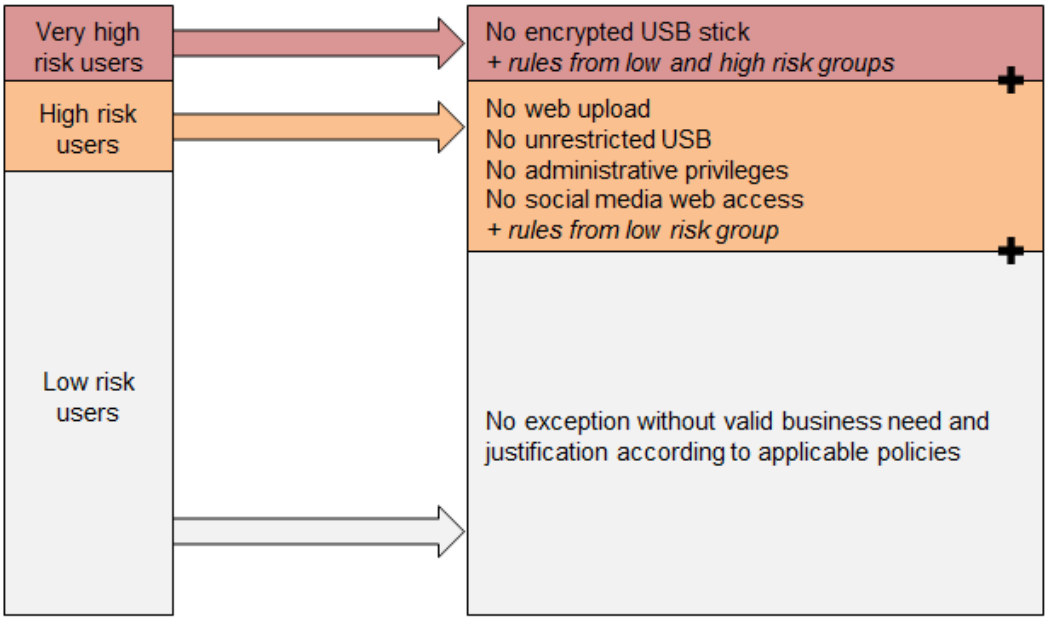

Figure 3: Definition of ruleset for different risk groups.

Rules are complementary in the way that rules defined for lower risk categories are also applicable for all higher risk categories as well. For example, rules defined for high-risk users also apply to users in the very high-risk category. The specific rules vary based on their individual requirements and risk appetite for each organization, as well as the respective exceptions in scope. In the figure shown above, users in the high-risk group are denied administrative privileges, web upload, and unrestricted USB access. In addition to that, users in the very high-risk group are denied the use of encrypted USB sticks and social media sites are blocked for their Internet connectivity.

However, this does not mean that there cannot be an exception that does not comply with these rules. In such cases there should be a strict escalation processes. Any exceptions to these rules should be documented and approved by senior management. For example, a line manager approving an Unlimited USB exception for a high-risk user could trigger an additionally necessary step for approval by his line manager or senior management.

4.4.4. Special cases

There are certain cases that do not match the defined rules. For example, domain administrators would most definitely be categorized as high risk because they potentially have access to confidential information. However, a domain administrator is not able to perform his job tasks if not granted administrative privileges. Another example is software developers. They might need administrative privileges. However, software developers usually do not need access to sensitive information to perform their job function. In such cases, other technical solutions have to be implemented to prevent data leakage.

The most crucial element is the implementation of extensive monitoring and logging capabilities. Active monitoring and logging enables organizations to know where and when sensitive data is transferred (Shinder, 2010). Other technical solutions include putting users in such cases on segregated network segments, on which no confidential information resides. Especially in the case of software developers, it is very common for organizations to set up a dedicated development environment separate from the internal network. Moreover, to follow best practices, the internal network should even be segregated according to the different categories of information that organizations own (Kostadinov, 2015).

4.5. Implementation

The implementation of this risk based approach concept will depend on the individual organizational environment. Based on solutions, systems and processes already in place, organizations could add or introduce the following elements to effectively apply this risk-based approach.

Policies and procedures are essential to create the framework and are the basis on which to build the risk-based approach. Therefore, organizations need to update all affected policies and procedures. For example, the exception policy, approval and recertification process for exceptions, reporting and escalation processes. If no applicable policy for a topic exists, the organization needs to draft a new policy. To enforce the policies a DLP solution has to be deployed. The solution needs to be able to grant selected exceptions to individual users. Furthermore, the solution needs capabilities to actively manage and report on existing exceptions. Depending on the individual implementation of the risk-based approach, organizations have to evaluate their specific requirements for a DLP solution. If a DLP solution is already in place, it has to be evaluated regarding the new requirements (Info-Tech Research Group, 2011).

On top of the reporting capabilities of the DLP solution organizations need reporting processes and tools that allow for the collecting, processing and provisioning of data. Information generated by the risk based approach needs to be processed. Up-to-date risk categorization of users must be available to line managers so they can make an informed decision. Any non-compliant exceptions according to the risk based approach ruleset (e.g. a high-risk categorized user should not have an Unlimited USB exception) should be reported to respective managers and business units on a regular basis.

Ideally, an organization would be able to provide and assess the information and create the report in real-time. However, depending on the individual implementation, the complexity and number of different systems involved, this most likely will be a challenge. Organizations may want to set up a regular cycle, e.g. weekly, by which to perform and update the user categorization and reporting.

4.6. DLP and data privacy

When implementing a DLP solution data privacy issues need to be addressed and solved. As a DLP needs to access and analyze data being stored or transferred, this may have privacy implications for users. Therefore, organizations, especially those operating in different countries, should consult with professionals specializing in local law and regulations to ensure compliance when implementing a DLP solution (Ernst & Young, 2011). This also applies for adding this risk-based approach on top of the DLP solutions.

Extensive monitoring and logging of user activity as well as categorizing users into different risk groups might conflict with local laws or regulations. Additionally, organizations might have to get approval from internal work committees.

In any case, an organization should clearly define policies, rules, and procedures that outline the expected user behavior and the possible extent of monitoring and logging activities. For example, a request for administrative privileges should clearly state and inform users about the monitoring they are subject to. Expectancy of privacy should be well defined.

4.7. Benefits

The intended immediate benefit of this risk-based approach is to enhance the exceptions approval process. The approach provides information to enable approvers, e.g. line manager, to grant or deny DLP exception not only based on a valid business need, but also on the actual risk of data leakage involve. By doing so, an organization can enable approvers to effectively reduce the data leakage risk. By identifying users with access to sensitive information, organizations can focus their controls and exception management to where they can best protect their information. Furthermore, the risk-based approach can be adapted and enhanced to meet the individual environment and requirements for an organization. The risk categorization of users as well as the rule setting can be modified to meet many different objectives organizations wish to achieve.

Additionally, such a risk based approach to data leakage and exception management creates transparency throughout the organization. Individual user categorization can be aggregated on team or business unit level. By doing so, organizations can identify areas and units where most sensitive information is processed. Subsequently, organizations can then focus their risk management or risk mitigation activity on these areas to significantly reduce their data leakage risk. For line managers this approach creates awareness, but also introduces accountability. By granting exceptions to users in high-risk categories, they undeniably accept risk on behalf of the organization. Organizations might therefore even modify the approval process for exceptions to be escalated to senior management for the final approval of high-risk groups.

However, the benefits, the output of the user risk categorization represents is highly sensitive. If an attacker could gain access to this information, it would allow them to choose the most valuable targets within an organization. For example, users in the high-risk category have access to the most confidential information, so an attacker would know whom to target. The information reveals top targets for social engineering; therefore, it should be well protected.

5. Enhancements and additional applications

The risk-based approach presented in this paper is neither comprehensive nor a complete approach. Instead, it is a practical concept to enhance an already existing exception management approach to more effectively focus on the risk of data leakage. Individual implementation will vary by organizational environments and requirements. However, the principle idea remains. Exceptions to DLP should not only be granted based on a business need, but should be granted or denied based on the actual risk of data leakage in each individual situation.

Other criteria to consider when categorizing users into different risk groups might be personal factors, organizational factors, or behavioral indicators (U.S. Department of Justice - Federal Bureau of Investigation, n.d.). However, organizations should be aware of legal and regulatory requirements when thinking about including this information. In addition, factors like organizational affiliation and country might be considered. For example, organizations might assume a higher risk of data leakage if a user is working for an external contractor. Likewise, organizations might assume a higher risk of data leakage if a user is working or living in certain countries. Thus, the level of corruption in a country the organization operates in might be a factor.

In additions, organizations might think about extending the ruleset to include other vectors for possible data leakage. For example, granting users remote access to their email accounts or remote access to the organizations network might be based on the users risk categorization. Assuming organizations have internal software or application management solutions that control and manage installed applications on end user devices,

the installation of certain application with file transfer capabilities like SSH or FTP could be prohibited.

6. Conclusion

The risk-based approach to exception management is a practical method to enlarge decision making from a simple business need to a risk aware decision. Approval of exceptions to data leakage prevention controls should not only consider the business need, but the actual risk of data leakage associated with granting certain users certain exceptions. Although the concept outlined in this paper is basic, it serves as foundation for organizations to build their own customized solution. A customized solution will be inevitable in order to account for the individual prerequisites and requirements each organization will have. The main idea, however, remains the same; users are categorized according to their access to sensitive information. Furthermore, organizations define rules for each category of users to limit their ability to transfer or leak the information they have access to. Based on these rules, line managers or exception approvers are enabled to make risk aware decision. Regular reporting creates transparency and accountability for line manager and business units over actual data leakage risks by identifying existing non-compliances to these defined rules. Furthermore, by specifically targeting and mitigating identified non-compliances, organizations can effectively reduce their data leakage risk.

Additionally, this basic approach or concept offers possibilities for enhancements and further applications (e.g. including personal factors in the risk categorization of users). However, implementation takes time and is not always easy, (e.g. overcoming challenges like local data privacy regulations). Over time, creating transparency hopefully promotes a more risk aware culture. In conclusion, this risk based approach to exception management presents an alternative to a more common “business need” approach, thereby enabling organizations to effectively control, report and reduce their data leakage risk.

Christoph Eckstein, christopheckstein.sec@gmx.net

7. References

Ashford, W. (2014, 10 30). *Firms at serious risk of data loss through file sharing, study shows*. Retrieved 07 13, 2015, from http://www.computerweekly.com/news/2240233730/Firms-at-serious-risk-of-data-loss-through-file-sharing-study-shows

Brun, J., & Faske, D. W. (2010). *Data loss and information management.* Retrieved 07 01, 2015, from https://www2.eycom.ch/publications/items/banking/201010_data_loss/201010_EY_Data_loss_and_information_mgmt.pdf

Chitchyan, D. R. (2014, 04 11). *Detecting and Preventing Data Exfiltration.* Retrieved 07 04, 2015, from http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-de_lancaster_executive_report.pdf

Cisco Systems, Inc. (2008). *Data Leakage Worldwide White Paper: The High Cost of Insider Threats.* Retrieved 07 02, 2015, from http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.html

Coles, C. (2014, 06 05). *What are the Top Data Loss Prevention Tools?* Retrieved 07 13, 2015, from https://www.skyhighnetworks.com/cloud-security-blog/what-are-the-top-data-loss-prevention-tools/

Council on Cyber Security. (n.d.). *The Critical Security Controls for Effective Cyber Defense.* Retrieved 07 12, 2015, from http://www.counciloncybersecurity.org/critical-controls/

Ernst & Young. (2011, 10). *Data loss prevention.* Retrieved 07 02, 2015, from http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf

Forrester Research, Inc. (2010). *The Forrester Wave: Information Security and Risk Consulting Services.* Retrieved 07 01, 2015, from https://www.forrester.com/The+Forrester+Wave+Information+Security+And+Risk+Consulting+Services+Q3+2010/fulltext/-/E-res56675

Christoph Eckstein, christopheckstein.sec@gmx.net

Friedel, L. (2014, 05 08). *Social media poses grave danger to companies' confidential information*. Retrieved 07 15, 2015, from http://www.insidecounsel.com/2014/05/08/social-media-poses-grave-danger-to-companies-confi

Furness, T. (2004, 11 25). *Implementing Information Classification within the Enterprise.* Retrieved 08 02, 2015, from http://www.giac.org/paper/gsec/4198/implementing-information-classification-enterprise/106714

Garg, R. (2015, 04 22). *After the Breach – Do You Have a Proactive Response and Recovery Plan?* Retrieved 07 28, 2015, from http://zecurion.com/category/security-breaches-data-loss-incidents/

Gordon, P. (2007, 10 15). *Data Leakage - Threats and Mitigation.* Retrieved 07 10, 2015, from http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931

Hamilton, P. (n.d.). *Data Loss Prevention Program.* Retrieved 07 04, 2015, from http://www.mcafee.com/us/resources/white-papers/foundstone/wp-data-loss-prevention-program.pdf

Info-Tech Research Group. (2011). *Vendor Landscape: Data Loss Prevention.* Retrieved 07 31, 2015, from http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/rpt_infotech-research_dlp-vendor-landscape.pdf

ISACA. (2010). *Data Leak Prevention.* Retrieved 07 02, 2015, from http://www.isaca.org/Groups/Professional-English/security-trend/GroupDocuments/DLP-WP-14Sept2010-Research.pdf

Kostadinov, D. (2015, 02 23). *Data Traffic & Network Security*. Retrieved 07 13, 2015, from http://resources.infosecinstitute.com/data-traffic-network-security/

Leyden, J. (2003, 03 06). *Personal storage sites are the latest security risk*. Retrieved 07 15, 2015, from http://www.theregister.co.uk/2003/03/06/personal_storage_sites/

Mehta, L. (2014, 07 09). *Data Loss Prevention (DLP) Strategy Guide*. Retrieved 07 13, 2015, from http://resources.infosecinstitute.com/data-loss-prevention-dlp-strategy-guide/

Christoph Eckstein, christopheckstein.sec@gmx.net

Shabtai, A., Elovici, Y., & Rokach, L. (2012). *A Survey of Data Leakage Detection and Prevention Solutions* (1 Edition ed.). New York: SpringerBriefs in Computer Science.

Shinder, D. (2010, 03 29). *10 ways to make sure your data doesn't walk out the door: UPDATED*. Retrieved 07 13, 2015, from http://www.techrepublic.com/blog/10-things/10-ways-to-make-sure-your-data-doesnt-walk-out-the-door-updated/

Silowash, G. J., & Lewellen, T. B. (2013, 01). *Insider Threat Control: Using Universal Serial Bus (USB) Device Auditing to Detect Possible Data Exfiltration by Malicious Insiders.* Retrieved 07 11, 2015, from http://www.sei.cmu.edu/reports/13tn003.pdf

U.S. Department of Justice - Federal Bureau of Investigation. (n.d.). *The Insider Threat - An introduction to detecting and deterring an insider spy*. Retrieved 07 13, 2015, from https://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

Utter, D. (2008, 08 05). *Countrywide Insider Stole Data For Two Years*. Retrieved 07 13, 2015, from http://www.securitypronews.com/countrywide-insider-stole-data-for-two-years-2008-08

Verizon. (2015). *2015 Data Breach Investigations Report.* Retrieved 17 28, 2015, from http://www.verizonenterprise.com/DBIR/2015/

Last Updated: April 24th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Doha 2018	OnlineQA	Apr 28, 2018 - May 03, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced