INSIDER THREATS IN IT INFRASTRUCTURE: LANDSCAPE, SOURCES, AND TRENDS

2015-2016

Prepared by: © Ekran Systems

Contents

Introduction 3
What is insider threat? 4
Insider threats in global cybersecurity landscape 5
Identifying malicious insider 8
Behavior that enables insider attacks 12
IT assets at risk 13
Key trends for insider threats 14
Barriers to effective insider threat management 16
Detection of insider threats 17
Ekran System – effective solution to combat insider threats 21
Conclusion. Six steps toward mitigating insider threats 22

Introduction

High profile cases of recent years, such as Morgan Stanley data breach, brought insider threats into spotlight with the new force. Nowadays much more people are aware that the danger exist, but still, not a lot of them are giving it enough credit. Insider attacks can cost companies hundred thousands of dollars in damages and remediation costs, but only selected few are doing enough to sufficiently protect themselves.

Understanding insider threats is the first step in establishing effective protection. We went through a growing body of research and applied our own expertise in order to give you detailed easy-to-understand overview of insider threats. We examine what place they take in the current cybersecurity landscape, what the actual impact of such threats are on an organization and how dangerous they really are. We look at profiles of insiders, their motives, behavior and methods that they use to cause harm to your organization. And lastly, we look at how protected companies really are against insider threats and give our own advice as to how increase efficiency and effectiveness of your security.

We hope that this paper will help spread awareness of the problem and give you ideas on how you can combat it.

What is insider threat?

In order to start the conversation on insider threats, we first need to define the subject. So what exactly is an insider threat and how is it different from all other types of cyber threats?

The simplest definition you can give is that **insider threats** are the type of threat originated from within the organization. They are malicious actions, carried out by people who already have legitimate access to the sensitive data or infrastructure of the company. Malicious activity of such people is often invisible, as it is very hard to distinguish from their normal functions at the company. They can copy, modify or remove sensitive data pertaining to clients, business associates, trade secrets or digital products, plant malicious software or gain control of the critical infrastructure in order to steal or extort money or commit fraud.

Actions, caused by **malicious insiders** can result in the loss of business or clients and extremely high damage control and remediation costs. This makes insider threats very dangerous. They are costly to deal with and hard to detect and prevent, requiring completely different approach as opposed to outsider attacks.

Insider threats in global cybersecurity landscape

As the volume of research on insider threats grows, it becomes clear that they are a prominent security concern both in the US and on global scale.

Most companies in the world are vulnerable.

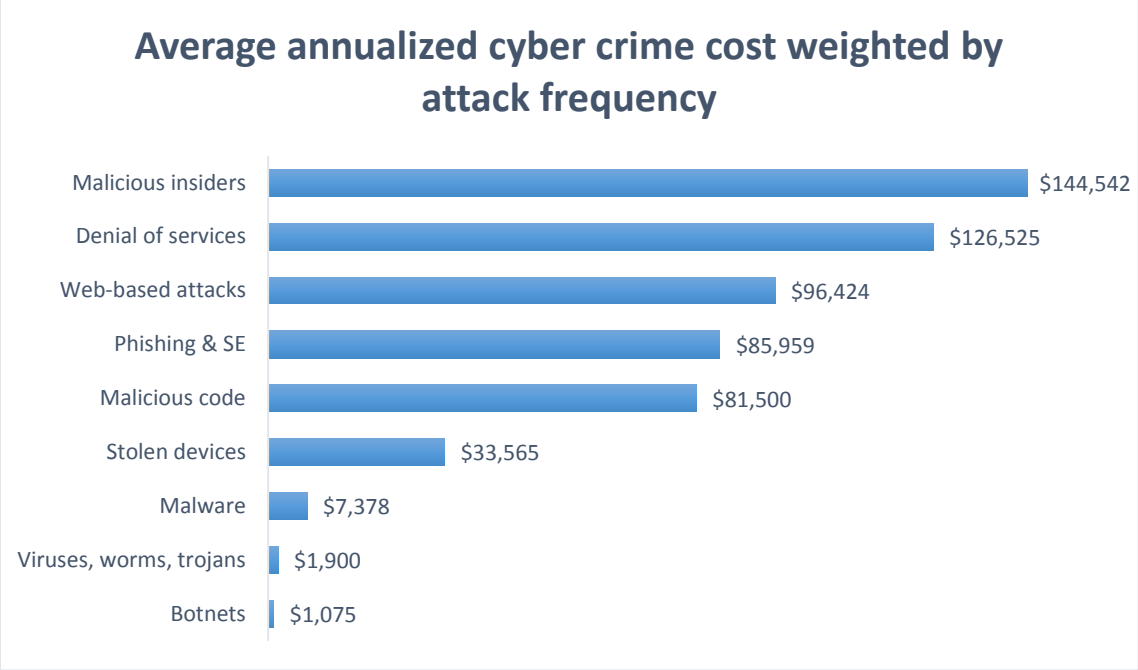
2015 Vormetric insider threat report shows (Figure 1) that most organizations in the world are vulnerable to insider threats with 34% reporting extreme vulnerability. Only 11% of organizations involved in the study reported that they have sufficient security and are not worried of the insider threat.

Figure 1. Vulnerability of organizations to insider threats

Insider crimes are the most costly.

As Ponemon 2015 cost of cyber crime global study (Figure 2) shows, crimes committed by malicious insiders on average cost much more to mitigate than other types of malicious activity. Large costs are usually associated with costly investigation, damage control, loss of clients and business.

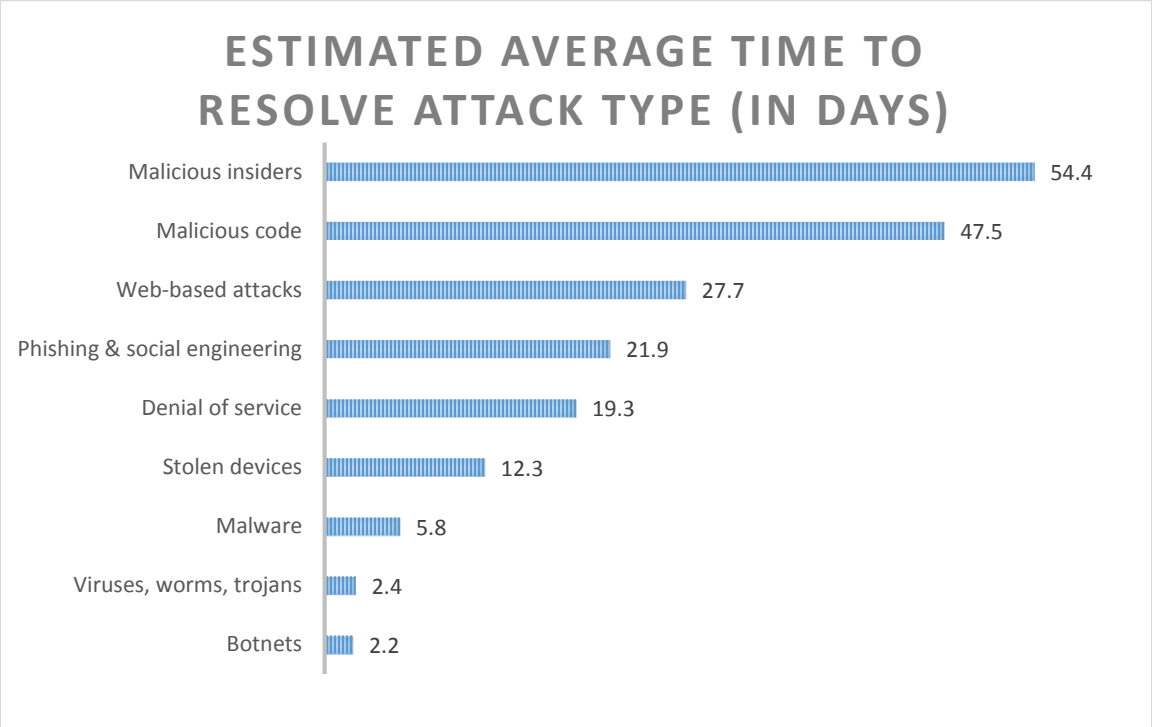
Figure 2. Average annualized cyber crime cost weighted by attack frequency



Insider crimes take the longest to deal with.

As shown by Ponemon 2015 cost of cyber crime global study (Figure 3), insider crimes take the longest to resolve. Slow resolve rate usually comes as a result of slow detection. It can be hard to fully restore events of the crime in order to detect and fix vulnerability. Most security professionals agree, that a lot of insider crimes go undetected and thus unresolved, making this statistic even more severe in reality.

Figure 3. Estimated average time to resolve attack type (in days)



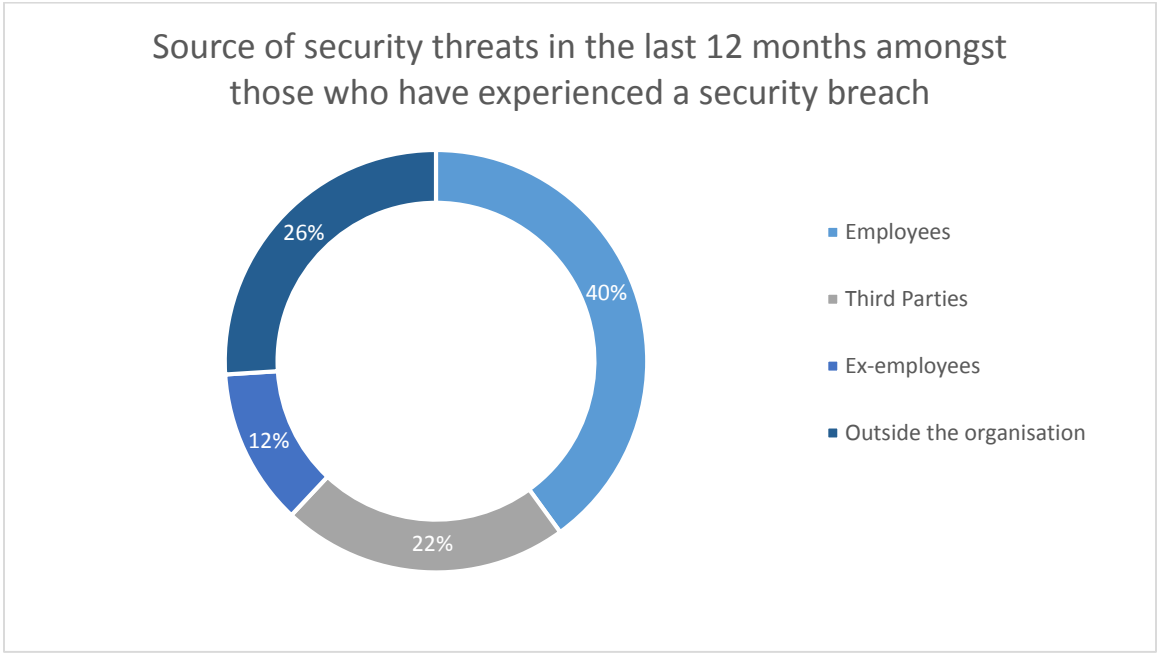
Identifying malicious insider

To fully understand the nature of insider threats we need to understand the people behind such actions. When hearing about malicious insiders, most people think about employees working in the office. However, limiting your insider threat management efforts only to current employees is a mistake that can open your organization to other types of insider threats that may fly over the radar.

> Sub-contractors, third-parties, and ex-employees are all parts of the extended enterprise and should be taken into consideration when developing your strategy of dealing with insider threats.

As shown by Clearswift Insider Threat Index (CITI) (Figure 4), most security threats comes from employees, with 40% of reported security breaches attributed to people currently working at the company. However, sub-contractors and ex-employees together are responsible for almost the same number of breaches - 38%, making them an important threat to consider.

Figure 4. Source of security threats in the last 12 months amongst those who have experienced a security breach

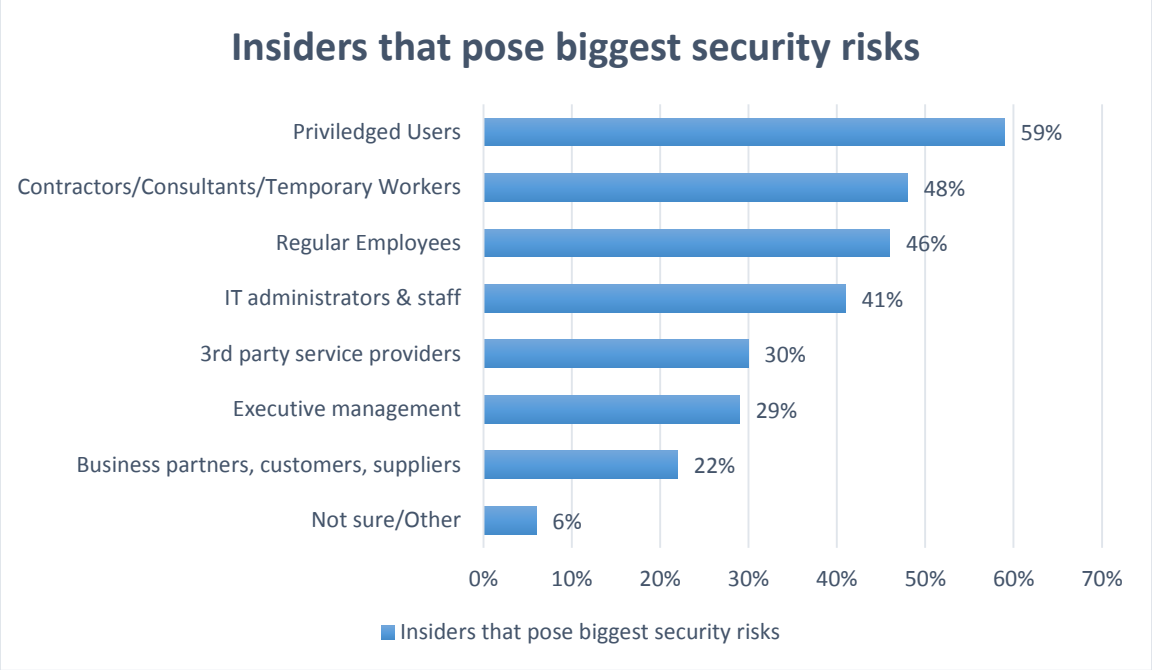


Within the extended enterprise, various types of users pose various degrees of risk to an organization. As shown by 2015 Insider Threats Spotlight Report (Figure 5), both privileged users and sub-contractors pose much bigger threat than regular employees.

> Privileged users often possess the highest level of access and considered trusted, and therefore are subjects to less strict control than the normal employee would.

In practice, this often allows them to abuse their status in order to conduct malicious actions.

Figure 5. Insiders that pose biggest security risks



Reasons for committing such malicious actions can vary. Security expert Bruce Schneier in his book Beyond Fear distinguishes several attacker profiles:

Opportunists. This type of attacker sees the opportunity and seizes it. Opportunists attack when they are convinced that they are safe and will not be caught. Basic security measures and user awareness can easily stop this kind of attacker.

Emotional Attackers. This is usually a disgruntled employee set out to make a statement. Such attacker is willing to take high risks and will usually not be discouraged by basic security measures. In fact, emotional attackers may even seek to get caught as a way of bringing attention to their issue.

Cold Intellectual Attackers. This is a skilled, knowledgeable technically sophisticated attacker that plans their action beforehand. This type of attacker usually targets specific data and will not be deterred by basic security measures.

Terrorists. This type of attacker is all about making a statement. They can even be encouraged by high risk and additional security measures, feeling that the difficulty of an attack further validates their accomplishment in the name of a goal.

Friends and Relations. Sometimes employee can also be a victim to his or her own circle of contacts. Friends or family can use employee credentials to commit fraud or data theft without them knowing about it.

End goal of malicious actions can also vary. Researcher from CERT program singled out four main types of insider threats based on goals and motives of the attacker.

IT sabotage. This a technically sophisticated attack that is usually committed by person with the direct privileged access to informational technology of the company. System administrators, programmers and knowledgeable privileged users can use their access to infrastructure in order to install backdoors, place time bombs into the software code, change system settings or otherwise compromise company's IT infrastructure. Such attacks are usually carried out by unsatisfied employee before termination.

Fraud. Employee that already has or gains access to sensitive personal data can use it to carry out one of the many types of fraudulent actions for personal gain. They can delete or modify data to steal business or clients, carry out identity theft, make illegal purchases, engage in social engineering, obtain illegal drugs, etc.

Theft of Intellectual Property. This type of attack is aimed at stealing important digital products and trade secrets such as technology, source code or content. It is usually committed by people with direct access to intellectual property, including engineers, programmers and content creators.

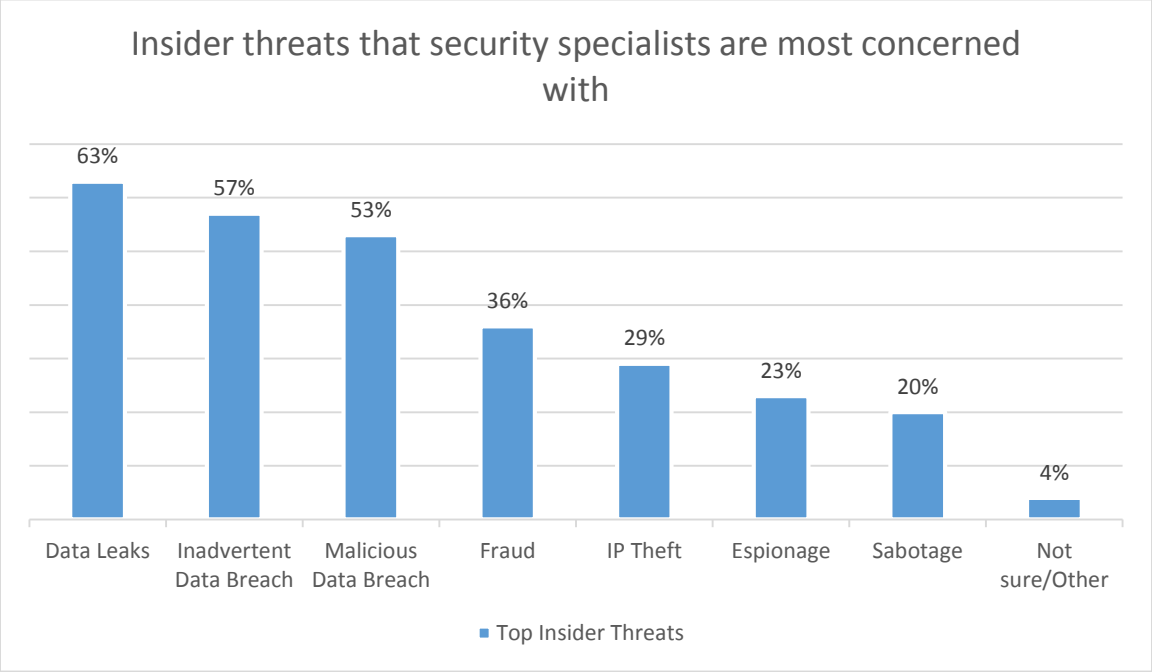
Espionage. Industry espionage and sabotage are usually highly coordinated and involve employees with privileged access, making these types of attacks especially dangerous and hard to deal with.

It is also worth mentioning, that not every insider attack comes from users with malicious intent.

> Often uneducated employee can cause data leaks or give malicious outsiders access to sensitive data inadvertently.

Authors of 2015 Insider Threats Spotlight Report (Figure 6) asked lead security specialists what type of insider threat they are most concerned about. Data leaks and inadvertent data breaches took the first two places, showing how big of a factor human errors are in a current insider threat landscape.

Figure 6. Insider threats that security specialists are most concerned with



Behavior that enables insider attacks

Certain technology and behavior that insiders engage in by going about their daily routines are inherently unsafe. If employee carries malicious motives, they can use these factors to carry out an insider attack. User errors committed in an environment where these factors are present can also result in a serious data leaks and security breaches. Authors of Clearswift Insider Threat Index (CITI) (Figure 7) examined such factors and determined the level of risk they possess among US organizations.

Removable storage devices. 49% of companies called removable USB storage devices the biggest internal security threat that they are facing. Such devices are small, inconspicuous, easy to use and carry. They can be used to copy large amounts of sensitive data and also can carry malicious code that automatically activates on connection. Policies and solutions for managing such devices are imperative for implementing reliable successful security.

Users not following data protection policy. Uneducated users that are unaware of why certain practices exist, pose a great risk to the security of the company. Negligence of corporate security policies by such users can cause unintentional data leaks and losses resulting in hundred thousand dollars of damages. Failure to report a fellow co-worker that breaches company security policy can also result in malicious insider attack going undetected.

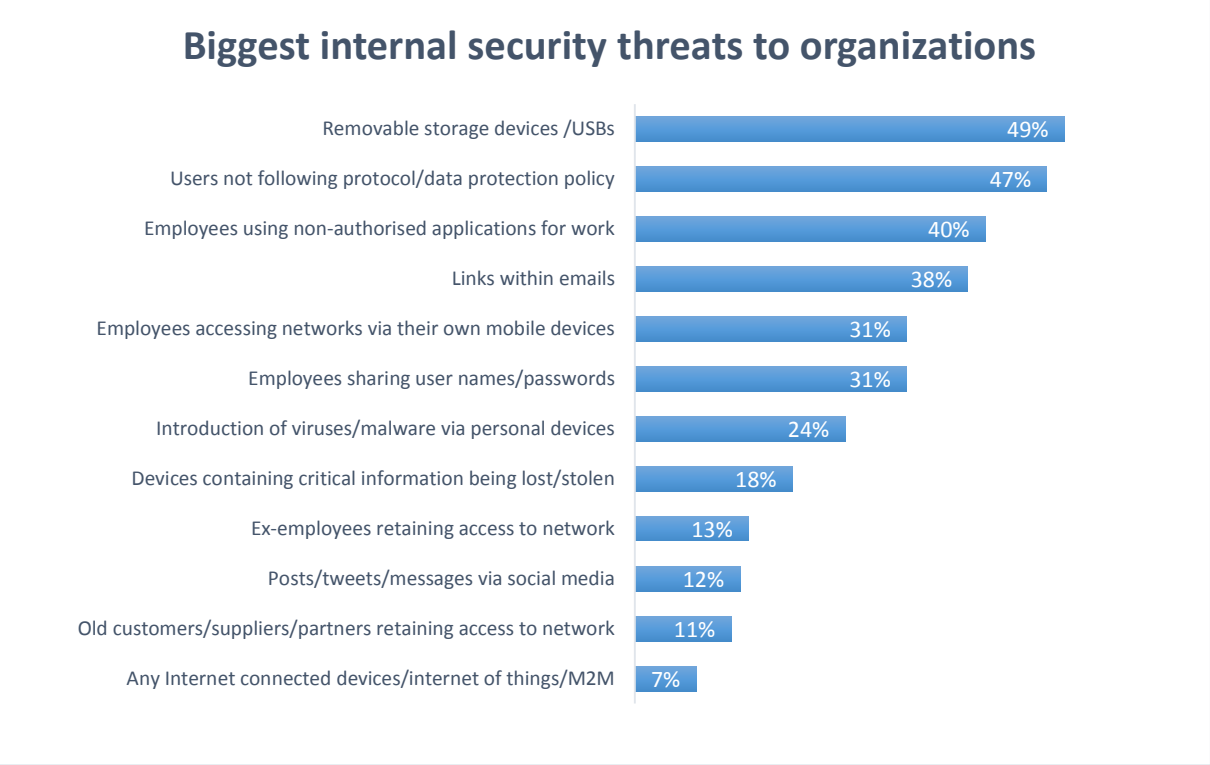
Use of non-authorized applications for work. By using an insecure data channels, employee opens organization to potential data leaks and malicious attacks. Unauthorized applications can also be used by malicious employees to quickly copy or damage data, get access to the infrastructure, or cover their tracks.

Links within emails. Spam by itself is usually not considered a high priority problem. However, uneducated user clicking on a malicious link may give full access to the company infrastructure and resources to perpetrators.

Increase use of mobile devices. Use of mobile devices in corporate space constantly grows, but such devices do not possess corporate level of security. Mobile devices of employees can be used both by them and by perpetrators outside of the organization to gain access to critical data and infrastructure.

Password sharing. Often even when company has a policy in place to prevent password sharing, employees will do it anyway for their own convenience. Password sharing makes it difficult to determine who accessed the sensitive data. It also allows insider with insufficient entitlement level to access data that he or she is not supposed to have access to.

Figure 7. What US businesses believe to be the biggest internal security threats to organizations.



IT assets at risk

When it comes to insider threat, every electronic asset and application can become a target. However, building your defenses around everything may not be financially reasonable, forcing you to prioritize assets that are most likely to be the target of an attack or the ones that have the biggest security weaknesses.

57% of respondents of 2015 Insider Threats Spotlight Report (Figure 8) named **databases** as the IT asset most vulnerable to insider attack. Database contains all important data in a single easy to access place, making it a convenient tool allowing for productive workflow, but also an easy target for malicious insiders. **File servers** where named most vulnerable assets by 55% of respondents. By getting access to actual files on the sever, insider can easily copy or modify them. Such access can also be used to install backdoors, plant viruses or change system settings, affecting whole network infrastructure. Servers and databases are two crucial IT assets that host and govern the most important data, affecting the workflow of the whole organization. If those assets are compromised, it may cost company valuable time short-term and hundreds of thousands of dollars in damages long-term.

Figure 8. IT assets at risk

Key trends for insider threats

Understanding recent changes and the current state of things within the insider threat landscape will help us channel resources in the right direction in order to employ the most effective counter measures. Insider Threats Spotlight Report identifies five biggest current trends associated with insider threats, which show us that insider threats become more prominent and dangerous, while most companies still do not put enough efforts to fight them:

Privileged users are the ones posing the most risk. According to the report, 59% of security specialists consider that privileged users pose the biggest risk to an organization. Such users are often considered well trusted and most companies do not take the necessary security measures to control their actions. Moreover, such users have direct access to critical infrastructure and most sensitive data, making malicious insider attacks, committed by them much more dangerous and hard to detect.

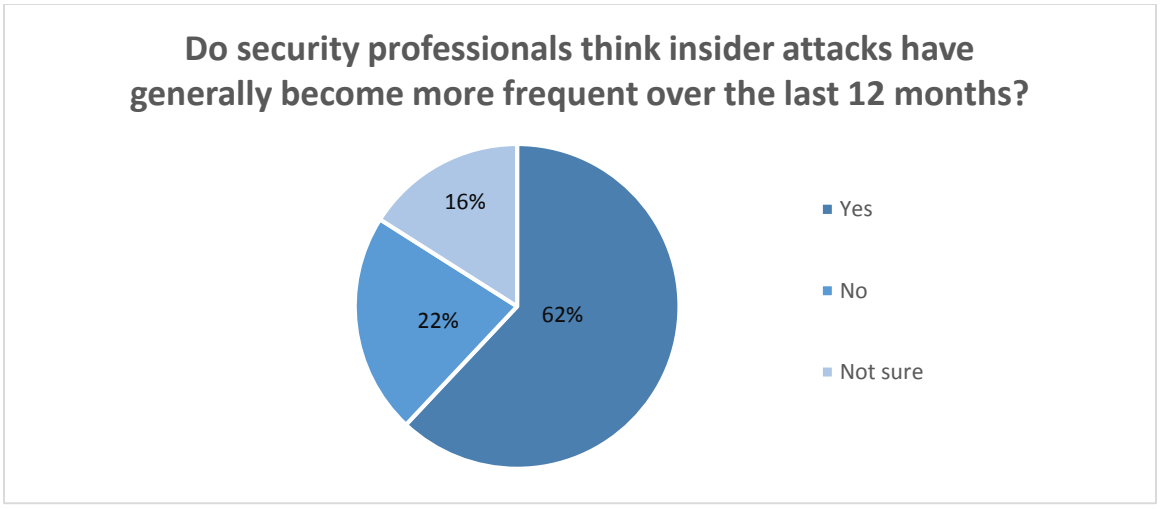
Frequency of insider threats are constantly rises. Insider Threats Spotlight Report (Figure 9) found, that when asked whether they saw a rise in frequency of insider attacks over the last 12 month, 62% of security professionals agreed that insider threats are becoming more frequent. There are a number of factors contributing to this, with the lack of data protection solutions, spread of insecure mobile devices and low user awareness being the most prominent among them.

Lack of preventive measures. Most organizations do not employ sufficient preventive measures to prevent insider threats from ever becoming full-fledged attacks. Prevention measures include not only the use of specific software solutions, but also employment of efficient and effectively enforced security policy and cultivation of high level of user awareness. According to same report, more than 50% of all companies do not have those measures in place.

Insider attacks are hard to detect. Insider threat detection is a major weak point in security for many organizations. Speed of detection is fairly slow with 40% of organizations struggling to estimate how long they will need to detect malicious insider actions. Main reason for this is not only inherent difficulty coming from the fact that insider has access to corporate infrastructure and can cover his or her tracks more effectively, but also insufficient security measures. Effective tools for detecting insider attacks, like user monitoring are still not employed by many organizations.

Scope of damages are escalating. As mentioned above, insider attacks are the most costly to deal with. Cumulative cost of all actions needed to resolve an insider attack can add up to several millions of dollars. According to the same report, 34% of companies are estimating remediation cost of more than $500 000 on average. With attacks becoming more frequent, while security budget are staying the same, scope of damages and cost of dealing with insider attacks are escalating across the board. What also worrying is that many companies are struggling to estimate average damages or remediation costs from potential insider attacks. With costs constantly escalating, companies are left unprepared for the amount of spending they may need to do in case of a successful insider attack.

Figure 9. Do security professionals think insider attacks have generally become more frequent over the last 12 months?



Barriers to effective insider threat management

Statistics and key trends show how vulnerable most organizations are to this type of threats. Most of them do not employ measures needed for efficient insider threat management and even ones that do often find themselves victim to insider attacks. 2015 Insider Threats Spotlight Report (Figure 10) examined various reasons preventing companies from better managing their insider threats:

Lack of training and expertise.

63% of security specialists reporting lack of professionals as the biggest barrier to manage insider threats. This can be explained by the fact that insider threats only recently gained prominence in the field of cybersecurity, coupled with rising demand for qualified personnel, creating the situation where industry cannot train security experts fast enough.

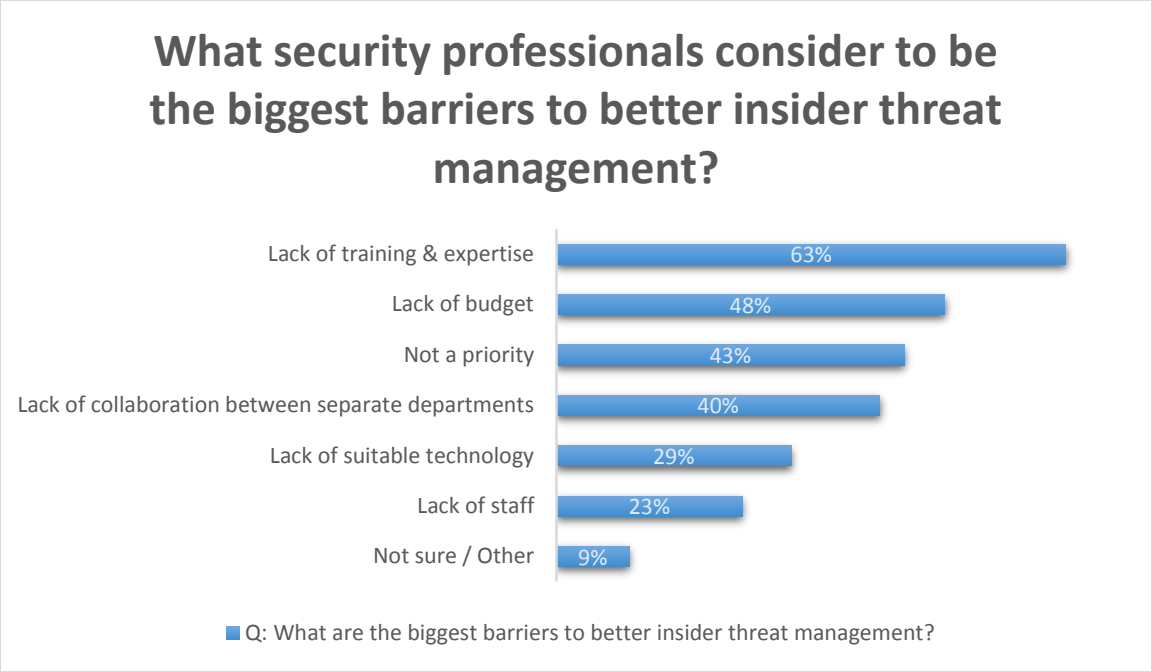
Lack of budged.

Another prominent barrier for better insider threat management is insufficient security budged. Most companies are not spending enough on security in general with prevention and detection of insider threats getting the back seat in the grand scheme of things. In 2015 -2016, 66% of security specialists expect their security budged to decrease or stay flat with only 34% expecting an increase. Insufficient funds prevent companies from hiring required professionals and getting software solutions that will allow them to effectively manage insider threats.

Not a priority.

Low level of priority was reported as the biggest barrier to better insider threat management by 43% of respondents. Despite the rising number of high profile cases, upper management of most organizations is still underestimating the severity of insider threats and potential repercussions that they carry. This leads to a number of security problems ranging from lover security budgets to inefficient security policy.

Figure 10. What security professionals consider to be the biggest barriers to better insider threat management?



Detection of insider threats

The first step in establishing efficient insider threats management is an effective detection. And as practice shows, this step can be one of the hardest for most companies. Three main factors make detection of insider threats especially difficult:

Insider already has legitimate access to critical data and infrastructure.

Employee or sub-contractor is someone who needs to perform tasks involving critical data and infrastructure. It is hard to detect instances of unauthorized access when employee needs to access certain data all the time in order to perform his or her job.

Malicious behavior of insider is indistinguishable from their normal activity.

Employee copy, change, or even remove important data all the time. Malicious behavior can be very similar to normal everyday tasks of the employee and as a result, insider attack can be very hard to detect.

False positives.

Employees often tend to cut corners and use complex behavioral patterns in order to do their job effectively. As a result, many automatic solutions, designed to detect and prevent insider threats, tend to produce large

number of false positives, often disrupting established workflow of an organization and making detection of actual insider attacks harder.

In order to overcome these obstacles, complex approach needs to be applied. One of the potential avenues to consider is the changes in day-to-day activities of employees. Security specialist should be aware of the regular behavioral patterns of their employees and be alerted by sudden suspicious changes. The following behavioral indicators described in "Combating the insider threat" publication by US-CERT, the operational arm of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC), are intended to act as a springboard for organizations to detect and deter malicious activity:

- Employee working with corporate network while taking vacation, on weekends or while staying sick.
- Employee stays in office at odd hours without specific request or authorization by their supervisor.
- Employee is noticeably enthusiastic about working overtime, at odd hours or over weekends.
- Employee makes unnecessary backups or copies of important data.
- Employee shows unusual strong interest in matters outside their immediate competence.
- Employee shows vulnerability, such as financial difficulties, gambling, health condition, alcohol or drug abuse, etc.
- Employee taking unexpected trips or vacations, suddenly acquiring wealth or repaying a large loan, etc.

By taking all of these factors into account, you often can identify potential malicious insiders and take additional security measures to prevent insider attacks. However, security specialists should be aware and mindful of employee freedom and privacy. It is important to control your employee's behavior while allowing them to work effectively and not intrude on their rights.

Other part of detecting insider threats, arguably, much more reliable and effective, is the **monitoring of user activity**. It is imperative to the company security to monitor user access to critical assets and infrastructure. In a lot of industries, such monitoring is even required by compliance regulations.

However, data from 2015 Insider Threats Spotlight Report (Figure 11) shows that more than two thirds of organizations currently do not employ such monitoring. And even ones that do conduct user monitoring are usually limited to access logging, as shown by the same report (Figure 12).

Figure 11. Does your organization monitor security configurations / controls of your applications?

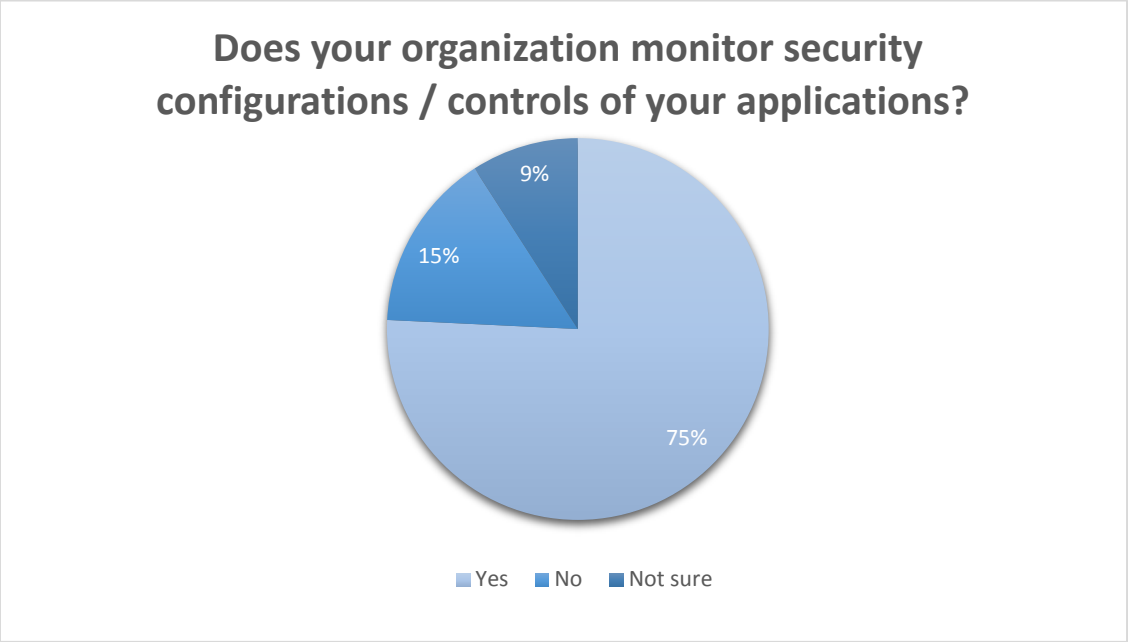
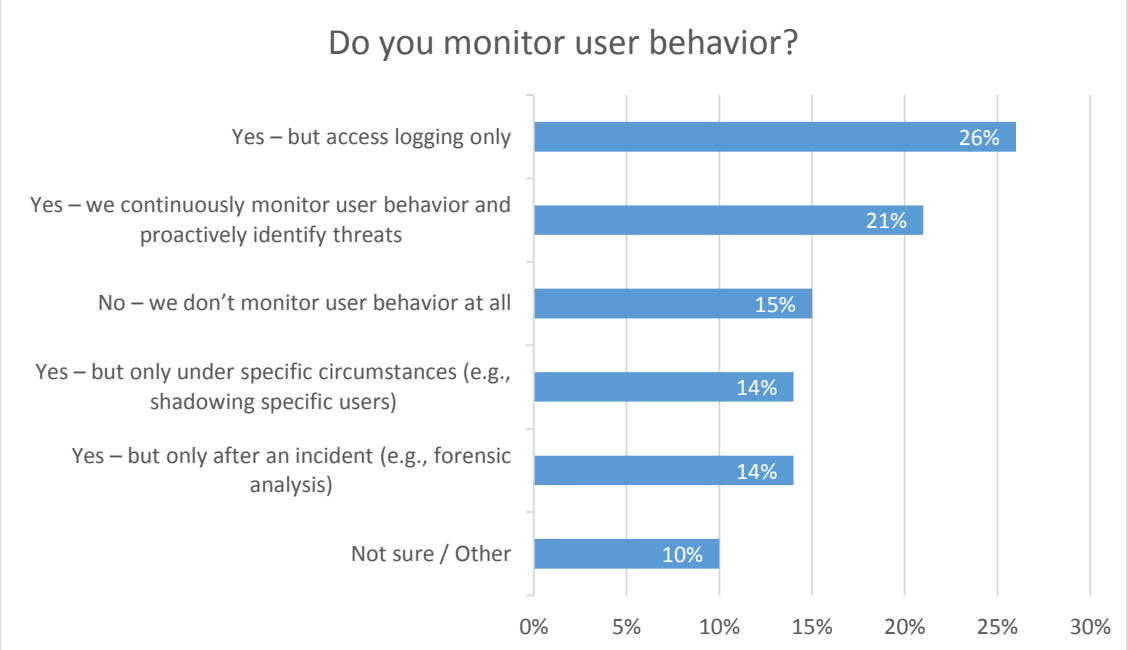


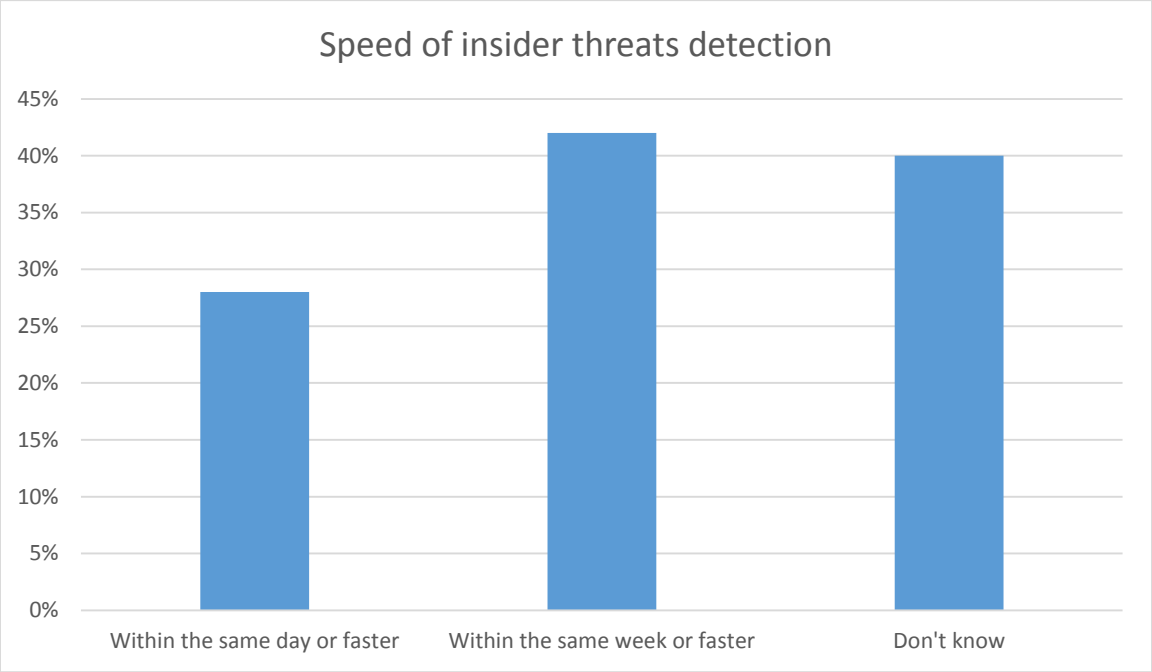
Figure 12. Do you monitor user behavior?



Access logging is a good start, but it does not provide you with enough data to monitor privileged users or users sharing same accounts correctly, and overall is not enough to efficiently detect insider threats.

Poor detection speeds and detection rates are the result of such poor state of user monitoring. Authors of 2015 Insider Threats Spotlight Report (Figure 13) asked security specialist how fast their organization detects insider threats. And while 42% of organizations are capable of detecting insider threat in less than a week, with 28% capable of detecting such threat in less than a day, 40% of respondents simply don't know how fast their organization can handle insider threat detection.

Figure 13. Speed of insider threats detection



Ekran System – effective solution to combat insider threats

One of the most effective ways to detect and control insider threats is to use a dedicated user monitoring software, such as Ekran System.

Ekran System is an agent-based solution that records every user session on a computer with installed Client. Users are made clearly aware of the recording, yet they cannot stop it or block the Client. Resulting recording allows you to clearly see each and every action taken by the user and easily identify any malicious or unauthorized activity.

Data from every end-point (desktops and servers) is stored in a centralized database that your security personnel can access via a convenient Web-based Management Tool.

Session video recording. Ekran System conducts video recording of everything that user sees on his or her screen complete with mouse movement. Relevant metadata is also recorded, including names of used applications and active windows, keystrokes, entered commands, visited URLs, etc. Each video is clearly associated with a specific user and indexed for easy searching.

Privileged user monitoring. Ekran System can monitor all users regardless of the level of privilege they have within the system. Administrator cannot pause the recording or block the Client. If he or she decides to run malicious code or access sensitive data without proper authorization, it will be clearly visible via video log augmented by text metadata log.

Subcontractor monitoring. Ekran System can be used to effectively monitor sub-contractors and third-party vendors. Actions of every remote user will be clearly visible and thoroughly recorded, allowing you to quickly find out the cause of potential incidents.

Alerts and notifications. With the help of customizable alerts and notifications, Ekran System can quickly inform your security personnel about potentially malicious actions. Alerts can be set to fire after certain events, sending notification with the link to the corresponding video log via email. Security then can watch the live video feed from the user screen to see exactly what said user is doing. If user conducts malicious activity, they can immediately block him or her, preventing any harm.

USB device management. As noted above, USB storage devices are often used by malicious insiders to copy and steal valuable data. Ekran System can detect such devices on connection and optionally automatically block them.

Ekran System has a powerful report generating tool that you can use to create a number of reports by pre-determined parameters. Such reports can aid in security audit and risk assessment.

Ekran System uses flexible per-Client licensing scheme, allowing you to solve insider threat detection problem in a cost-effective way no matter how large or small your company is.

Conclusion. Six steps toward mitigating insider threats

Insider threats are a very complex and widespread issue that almost every organization will face at one point or another.

Malicious insider actions can cost company huge amount of money, reputation and goodwill, are very hard to detect, and take a long time to deal with. It is best to be prepared and set up your defenses in advance, than to deal with consequences of insider attack.

As a conclusion to this paper, we present you with a set of six simple measures that you can employ to protect yourself from insider threats:

Educate users.

Educating your users about insider threats and best security practices can go a long way toward establishing reliable security for your company. Most users do not hesitate to sacrifice security for their own convenience, opening the way for both unintentional data leaks and malicious insider attacks. It is important to explain your employees why certain policies are in place and why they should follow them.

Implement and enforce security policy.

Efficient corporate security policy should take insider threats into account. Good practices include limiting users to their own devices, prohibiting password sharing, limiting work hours or session duration, prohibiting use of unsafe USB devices, etc. For the policy to be effective, users should be thoroughly informed about it. Upper management should be invested in the policy and it should be enforced from the top down.

Control or limit use of shared accounts.

Frequent use of shared accounts poses a great danger to the security of an organization. These types of accounts prevent you from knowing who exactly gained access to critical data or changed system settings, making it difficult to detect and deal with insider threats. Use of such accounts should be discouraged or secondary authentication tool, such as the one integrated into Ekran System, should be provided.

Monitor user activity.

User activity monitoring is the cornerstone of detection and control over insider threats. Solutions such as Ekran System allow you to monitor any user, including the ones with elevated level of privileges in order to analyze their behavior, detect and often prevent malicious actions. It is important to employ user monitoring solution and use it to monitor critical infrastructure and sensitive data.

Recognize and respond to suspicious employee behavior.

Often behavior of insider planning an attack contains crucial tells, allowing observant security personnel to take additional security measures to protect sensitive data from potential threat. Suspicious noticeable changes in the usual behavior of employees should be noted and investigated.

Deactivate computer access following termination.

More often than not companies do not terminate credentials of former employees immediately upon termination, allowing them to still access company infrastructure and sensitive data. Whether they want revenge for perceived injustice or conducting corporate espionage for their new employer, old employees can use their credentials to copy, alter or destroy sensitive data. Computer access of such employees should be immediately deactivated upon termination.

Insider threats are still largely overlooked. Most companies are sitting on a time bomb of sensitive data and critical infrastructure poorly protected from insiders. We hope that this paper gave you a better understanding of what insider threats are and how to effectively manage them.