netwrix

2017

IT Risks Report

www.netwrix.com

Introduction

Survey Coverage:

723 Organizations

30+ Industries

32% Large enterprises

68% Small and medium companies

Every year, more data breaches grab the headlines, and then new buzzwords in related cyber security pop up. It's easy to get confused about what's an isolated attack and what's actually threatening organizations on a daily basis. The shocking attacks in the spotlight do not necessarily reflect the real state of IT security in organizations or provide an accurate view of the threat landscape.

To get the true picture, we regularly survey organizations, asking what IT risks they meet on a daily basis. We learn how IT pros perceive their organizations' ability to fight IT risks, such as data compromise, system downtime that disrupts operations, and penalties for non-compliance with government and industry standards. And we check those perceptions against how they actually implement security policies and their plans for the future.

In this report, we share what we've learned. Specifically, we analyzed feedback collected between March 15 and April 15, 2017, from 723 respondents holding various positions in IT departments across all major industries worldwide. They shared their concerns, failures and successes via our online questionnaire. Some questions allowed only one answer and others allowed multiple responses. In some cases, we compare the results of this survey to a similar survey conducted in 2016.

This report would not be possible without the input from our survey participants. The Netwrix team thanks each one of you; we greatly appreciate your help.

Highlights

IT Risks: Context

- The number of organizations that have at least some controls over user activity, data access and IT changes in place grew from 62% in 2016 to 85% in 2017.
- IT auditing has become a more widespread practice, used by 84% of organizations in 2017 versus 63% in 2016. Manual IT auditing methods are still very common, but implementation of third-party software is growing steadily.
- The majority of organizations (89%) limit the range of IT security solutions in use to the basic ones, and only 13% of respondents use more advanced solutions for information security governance or risk management.
- The majority of organizations (65%) do not have dedicated personnel responsible for cyber security. The same is true for compliance — 56% of organizations subject to compliance delegate this task to the IT operations teams.

IT Controls and Practices: Perceptions

- Only 58% of respondents consider their current IT controls (or lack of them) adequate to their organization's specific needs.
- Employee activity in the IT infrastructure continues to be neglected more than the activities of IT staff and third parties; only 36% of organizations say they are fully aware of employees' actions.
- Like last year, organizations have the most visibility into activity and IT changes in endpoint protection (61%), virtual infrastructure (59%) and on-prem systems (52%). Shadow IT and BYOD are still the main pain points for about one third of the IT pros surveyed.
- Visibility into user activity across the IT infrastructure primarily benefits security initiatives, helping organizations to detect (79%) and investigate (73%) incidents, secure assets (55%), and mitigate security, compliance and system outage risks (53%). Visibility helps them avoid problems such as system unavailability, data leakage, and audit failures.

IT Risks: Operations, Security, Compliance

- Even though 47% of organizations still experience operational issues due to lack of visibility, the number of respondents who are satisfied with the time required to fix them grew from 49% in 2016 to 81% in 2017.
- 65% of respondents admitted to having security incidents in 2016; the most common reasons cited were malware and human errors.
- 48% of organizations that have to comply with any cyber security standard still struggle to ensure continuous compliance and provide complete evidence of it to auditors. In addition, passing IT audits requires extra effort from the IT team.
- 66% of organizations perceive employees as the biggest threat to system availability and security.

Threat Resistance and Next Steps

- Just 26% of organizations claim to be well prepared to beat IT risks.
- For those who are not prepared, lack of budget (57%) and time (54%) are the main obstacles.
- Organizations are planning to focus their future investments on securing sensitive data, since they cannot foresee every possible threat.

PART 1

IT Risks: Context

Before we dive deeper and talk about IT risks organizations are dealing with and whether they are successful or not, it is important that we look at what controls, practices, solutions and human resources organizations have in the background to deal with issues of any nature.

We are also going to analyze, where possible, tendencies over the past year and see if organizations continue to gravitate toward fuller IT controls, as they previously did.

1.1 IT and Security Controls in Place

> *The number of organizations that have at least some controls over user activity, data access and IT changes in place grew from 62% in 2016 to 85% in 2017.*

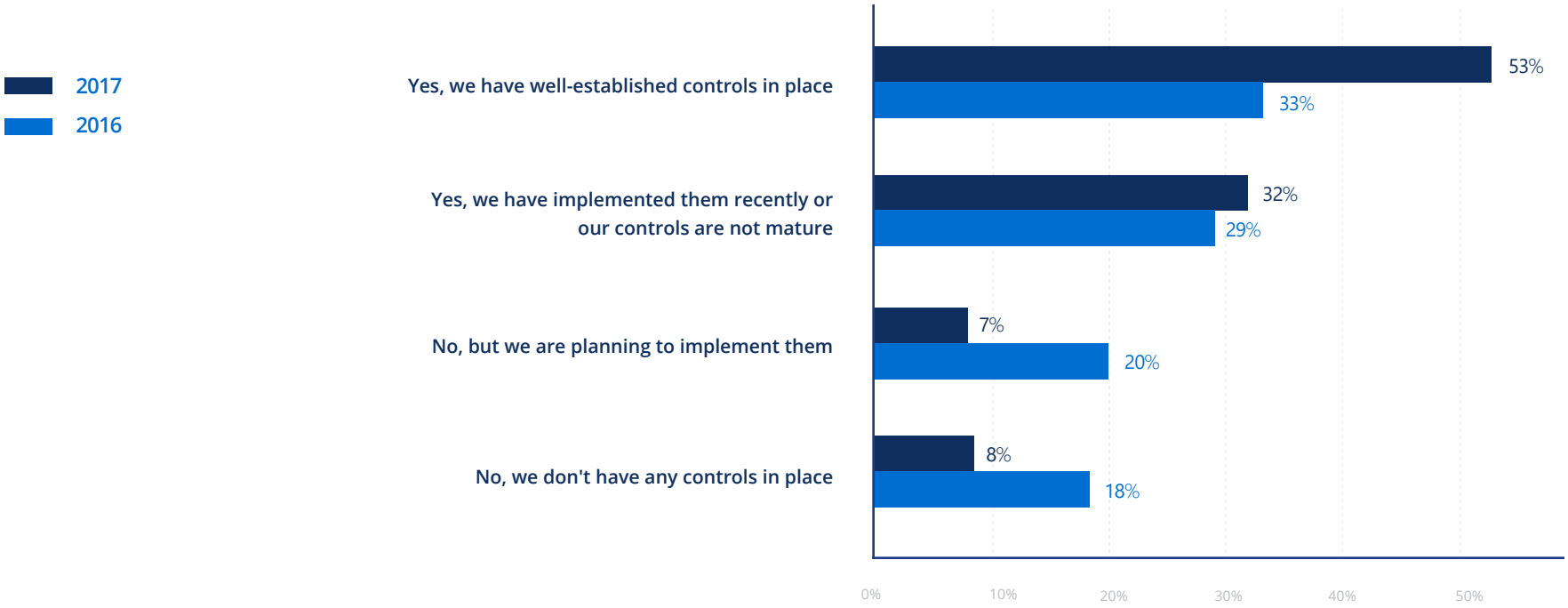
This year, we observed a great increase in the number of organizations that have at least some IT and security controls in place: 85% this year vs. 62% in 2016[1]. Overall, more than half of organizations already have mature controls in place vs. one third last year. While every fifth organization last year admitted they didn't have and didn't plan to implement any IT controls, this year, only 8% of respondents fall into this category.

[1]Here and further on in this report, we refer to the data revealed in the 2016 Netwrix IT Risks Report and the 2016 Netwrix Visibility Report.

This leads us to conclude that regardless of industry, size and sensitivity of stored data, organizations have gradually come to realize that they need to have a stronger hold on activity in their IT environment.

We will reveal the reasons for these changes in organizations' tactics further in the report.

Availability of any controls over user activity, data access and IT changes in organizations



1.2 Established IT Auditing Processes

> *The need to establish IT auditing processes has increased over the year; organizations mostly prefer to use third-party software.*

Despite the general automatization trend, the share of organizations that use manual IT auditing to gain visibility into activity in their IT infrastructures is still very high. About 67% of all respondents said they had manual processes of IT auditing for at least some systems.

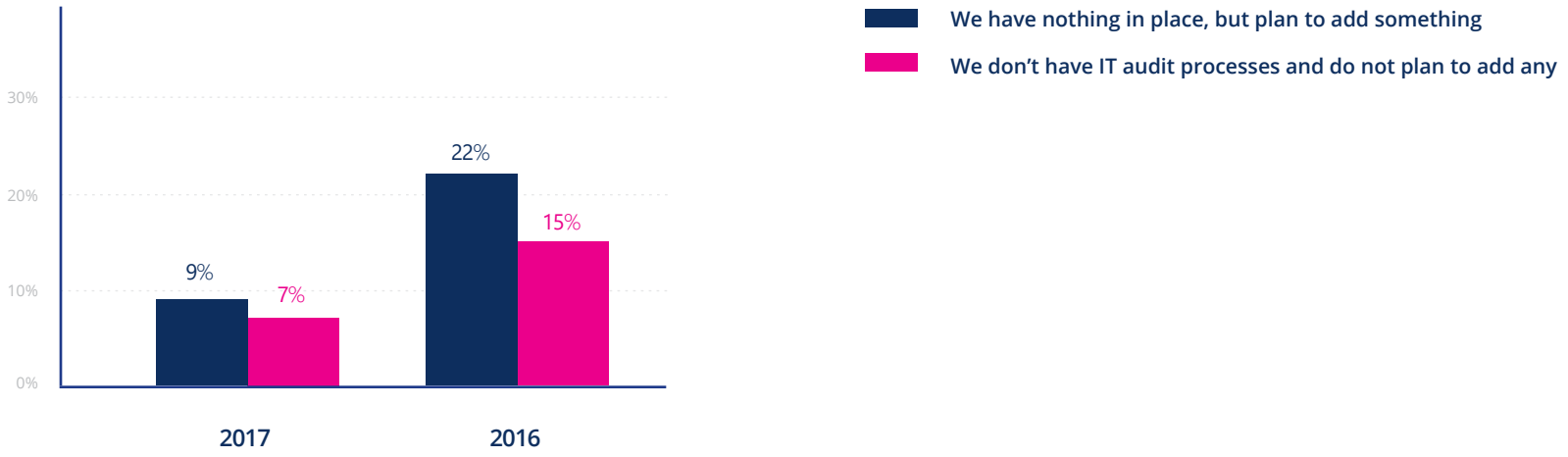
With that said, there is definitely a continuing tendency toward wider adoption of IT auditing processes: The number of organizations that still don't use any IT auditing methods decreased from 37% in 2016 to 16% in 2017.

More organizations have begun to use either third-party software (63%) or homegrown scripted solutions (25%) at least partially. Since the majority of respondents prefer to have direct control over the IT environment for better security, compliance and troubleshooting, quite expectedly, the number of organizations that entrust their IT auditing processes to MSPs remained unchanged from the last year (6%).

Various methods to gain visibility into data and IT environment. Choose all that apply

- 67% System native logs (manual IT auditing)
- 63% Third-party software
- 25% Homegrown scripted solution
- 9% We have nothing in place, but plan to add something
- 7% We don't have IT audit processes and do not plan to add any
- 6% This process is outsourced

Organizations that do not have any IT auditing processes in place



1.3 Availability of IT Security Solutions

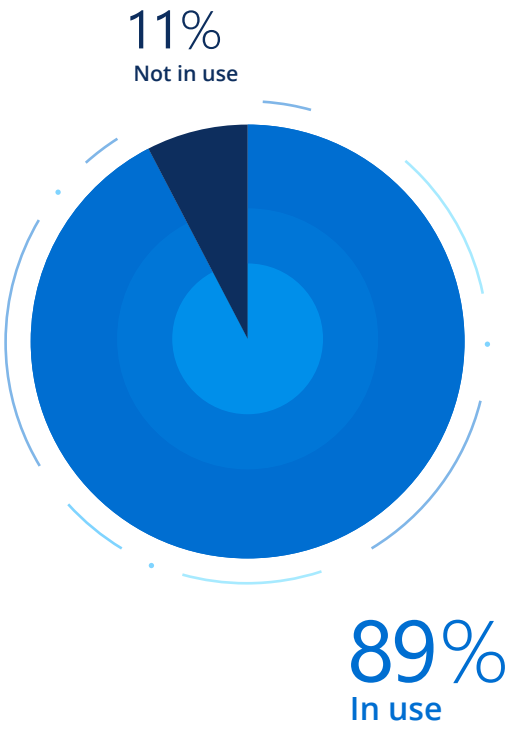
89% of organizations use basic IT security solutions, while only 13% leverage more advanced solutions for information security governance or risk management.

We asked our respondents to tell us more about the cyber security software they use. Organizations attempt to protect their IT environment at least at the basic level. The absolute majority of organizations (89%) use some kind of security software. However, the share of organizations that have advanced security strategies is significantly smaller: Only 13% of respondents use information security governance or risk management solutions.

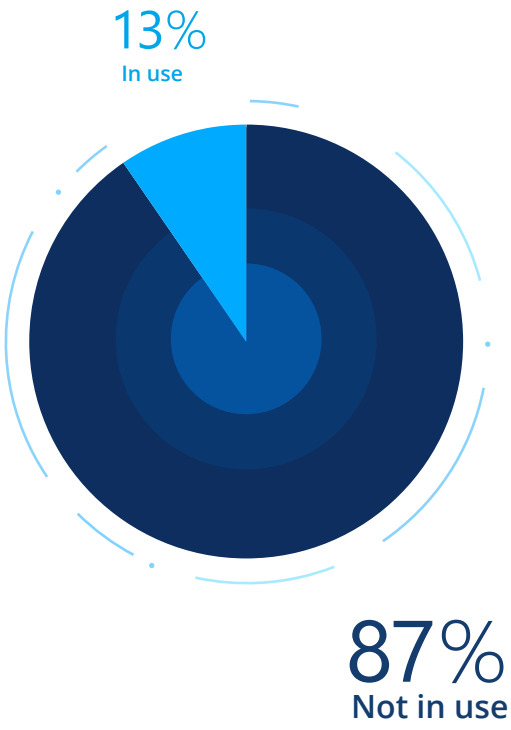
Here, the results for SMBs and large enterprises vary, as the latter tend to have fewer obstacles and greater needs for IT security solutions.

Thus, 100% of enterprises and 86% of SMBs have IT security solutions in place; however, not all of them have opted for advanced protection. Only 21% of enterprises and 12% of SMBs have software for information security governance or risk management.

Availability of any IT security solutions



Availability of software for information security governance or risk management



1.4 Availability of Dedicated Human Resources

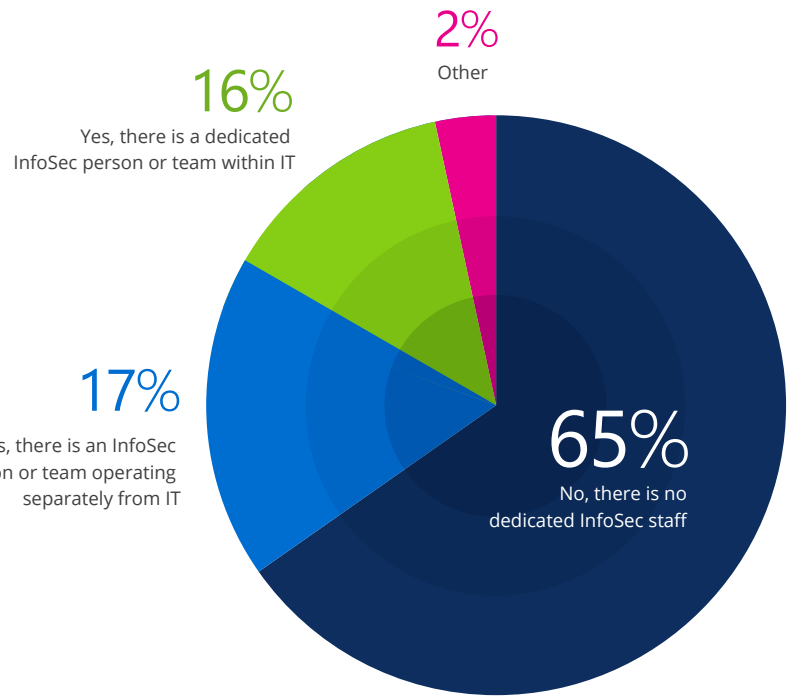
> *The majority of the organizations do not have dedicated personnel responsible for cyber security and compliance.*

In the majority of organizations, IT operations teams have to take responsibility for cyber security and compliance as an additional task. For a deeper understanding of the organizations' attitude toward IT risks, we also asked if there are dedicated personnel responsible for security in general, security monitoring and incident response in particular. The findings confirmed what we often hear from the IT community: IT operations teams bear the burden of the IT tasks, be it maintenance, troubleshooting, security, compliance, user support or anything else.

First, 65% of the surveyed organizations have no dedicated informational security personnel. Another 33% of respondents said they have an InfoSec person, or even a security team, which can be either a part of the IT department or a separate department.

The rest of the organizations prefer or can afford to have security personnel only for certain functions, such as, for example, risk management.

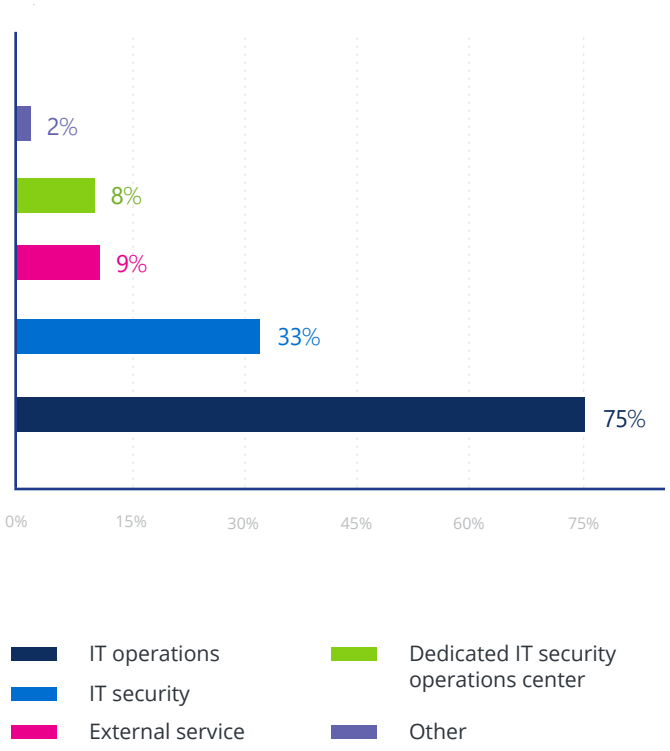
Availability of a separate information security function



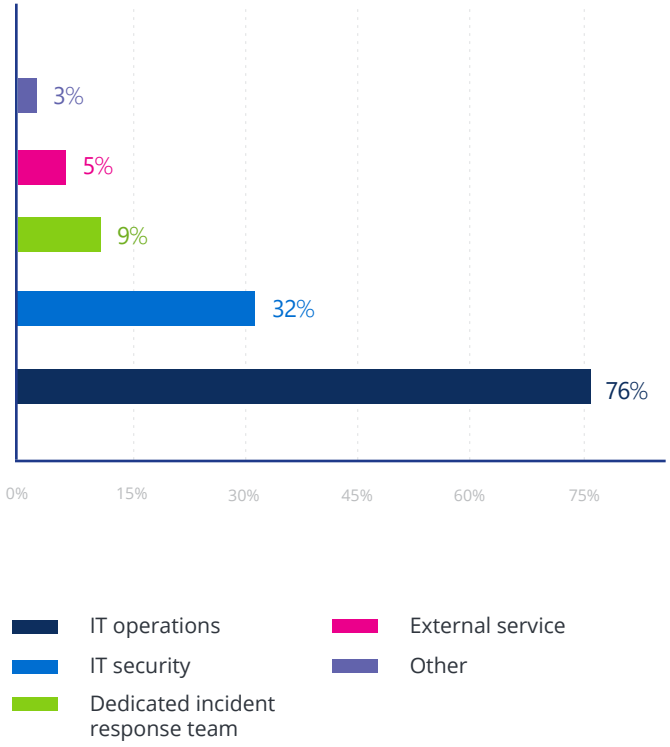
Second, in about 75% of the surveyed organizations, IT operations teams are partially or wholly responsible for security incident monitoring and response.

Some organizations outsource the tasks of monitoring (9%) and response (5%) to third parties.

Department responsible for security incident monitoring. Choose all that apply



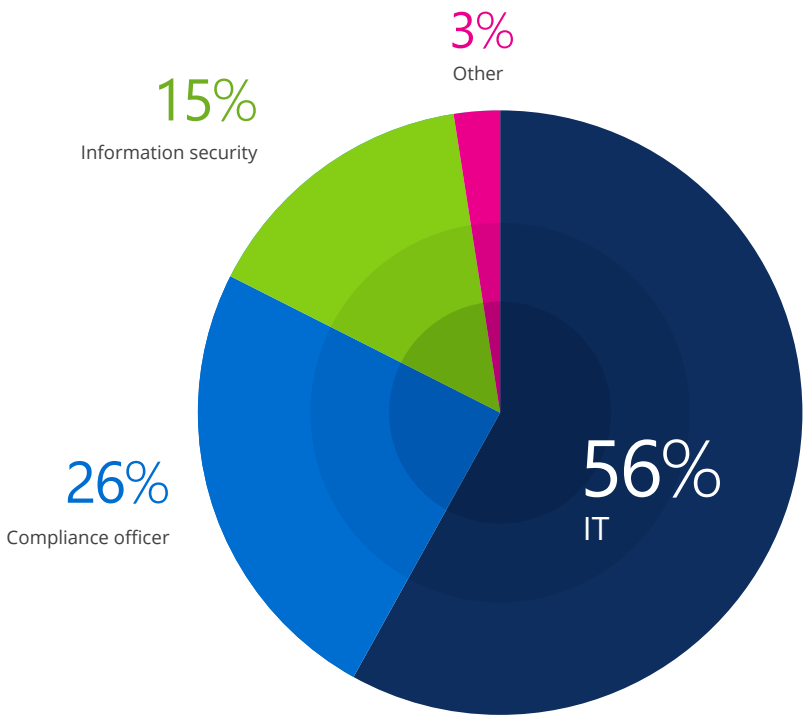
Teams responsible for the security incident response process. Choose all that apply



Similar to cyber security, the majority (56%) of organizations that comply with internal or external regulations (75% of all surveyed organizations) delegate to IT operations teams the responsibility for both ensuring that the organization meets its compliance obligations and passing compliance audits.

Only a quarter of organizations have a separate compliance officer or team that is fully responsible for this task.

Team / person primarily responsible for ensuring compliance



Part 1. **Summary**

Organizations have definitely been trying hard to tame the chaos caused by the generally growing complexity of their IT infrastructures and inability to control user activity and IT changes occurring in the IT environment.

It is interesting to note that while we see more and more respondents establishing IT controls, these controls are mostly basic, and only a very small number of organizations take a comprehensive approach and dive into risk management. Lack of dedicated security and compliance roles in the majority of organizations further confirms the fact that organizations for the most part do not have a full-fledged risk mitigation strategy.

Thus, despite the positive tendencies, it is still too early to state that organizations have overcome the barriers to establishing full control over the IT environment, which is necessary to minimize the impact of IT risks.

PART 2

IT Controls and Practices: Perceptions

Since we have a basic understanding of how organizations are trying to establish security controls, let us talk about perceptions respondents have about their effectiveness. Perceptions are not always rational and may be hard to analyze with diagrams. However, we find it important to get feedback from IT pros who deal with IT issues about whether the practices they have in place are adequate to the business specifics and their everyday challenges.

One of the main questions we are trying to find the answer to is whether respondents have enough understanding of what their users are doing and what is happening in general in the various parts and layers of the IT environment to timely detect, investigate and remediate a potential issue or an actual threat.

2.1 Adequacy of IT and Security Controls

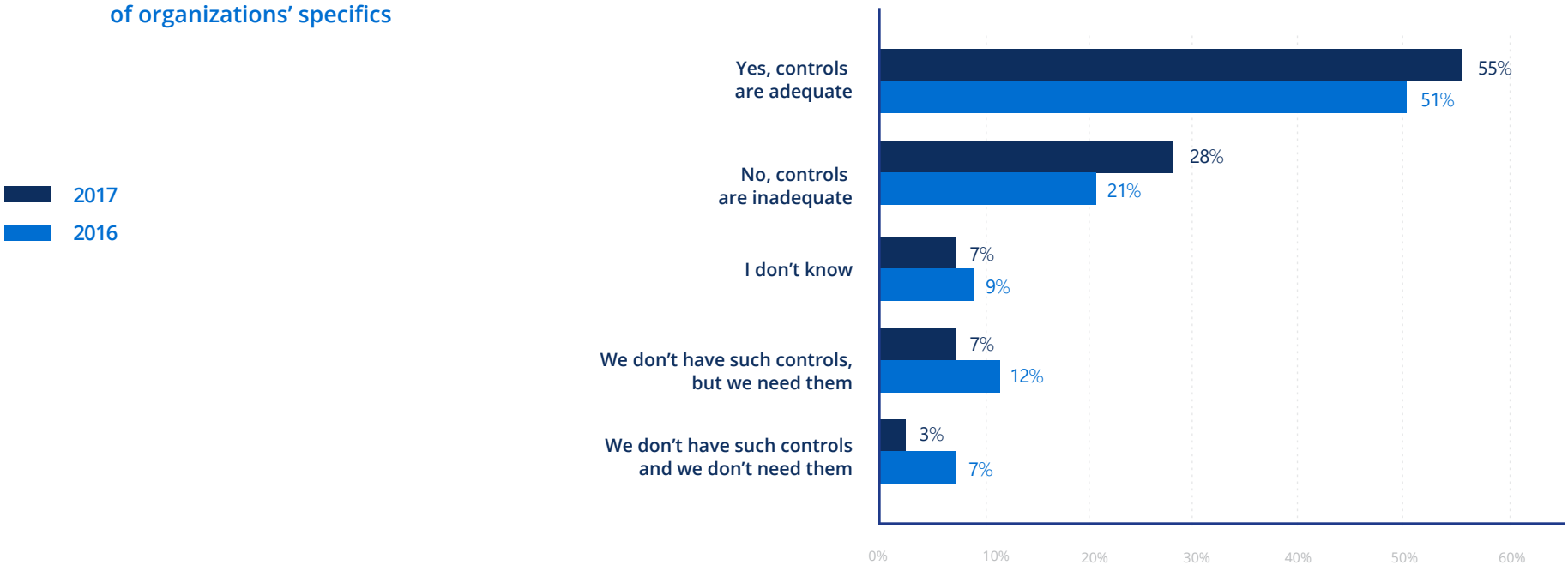
> *35% of respondents admit that established IT controls or the lack of them is inadequate in terms of their organization's specifics.*

Having at least some IT and security controls in place is definitely very important. However, it is critical that implemented controls are adequate in terms of the organization's size, complexity of infrastructure, business specifics, etc.

Having asked this question, we received interesting results. While the number of organizations that have implemented some controls or enhanced the existing controls has grown, at the same time, the percentage of both satisfied and unsatisfied organizations has grown as well. Thus, 55% of respondents consider the controls adequate in 2017 vs. 51% in 2016. At the same time, 28% of organizations in 2017 see the controls as inadequate vs. 21% in 2016, as respondents have realized that established controls are not enough to be fully prepared to fight cyber risks.

Overall, organizations tend to implement more controls and tighten the existing ones. On the way to a more manageable and secure IT infrastructure, they understand that a basic set of controls in the context of a great variety of IT risks is no longer enough.

Adequacy of IT and security controls in terms of organizations' specifics



2.2 Depth of Visibility into User Activity

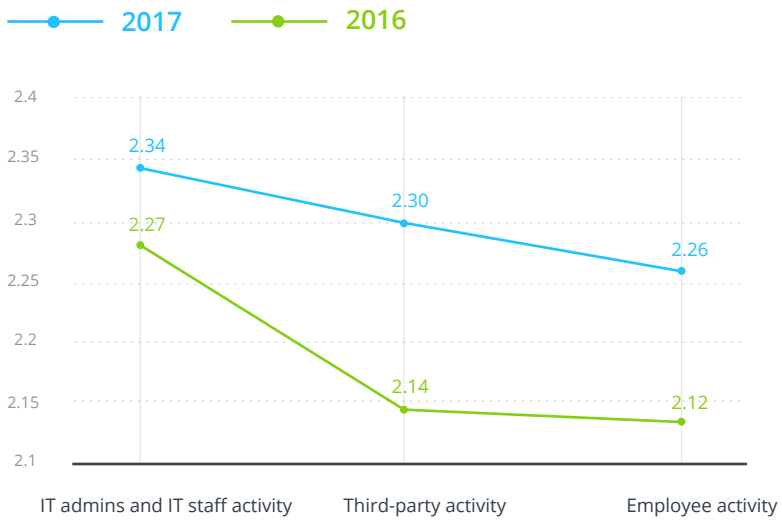
> *Activity of regular employees bothers organizations less than activity of IT staff or third parties.*

To decrease the number of IT incidents or their impact on business processes, organizations need to be aware of what activity is happening across their IT infrastructure. We asked respondents to evaluate the level of visibility they have into activity of different types of users: IT personnel, employees and third parties, including vendors, contractors, partners, etc.

Almost every tenth company doesn't have visibility into any of those aspects. The activity of IT staff is monitored by 43% of organizations. Third parties' activity is fully controlled by 41% of organizations. Meanwhile, only 36% of respondents claim they have complete visibility into the activity of regular employees.

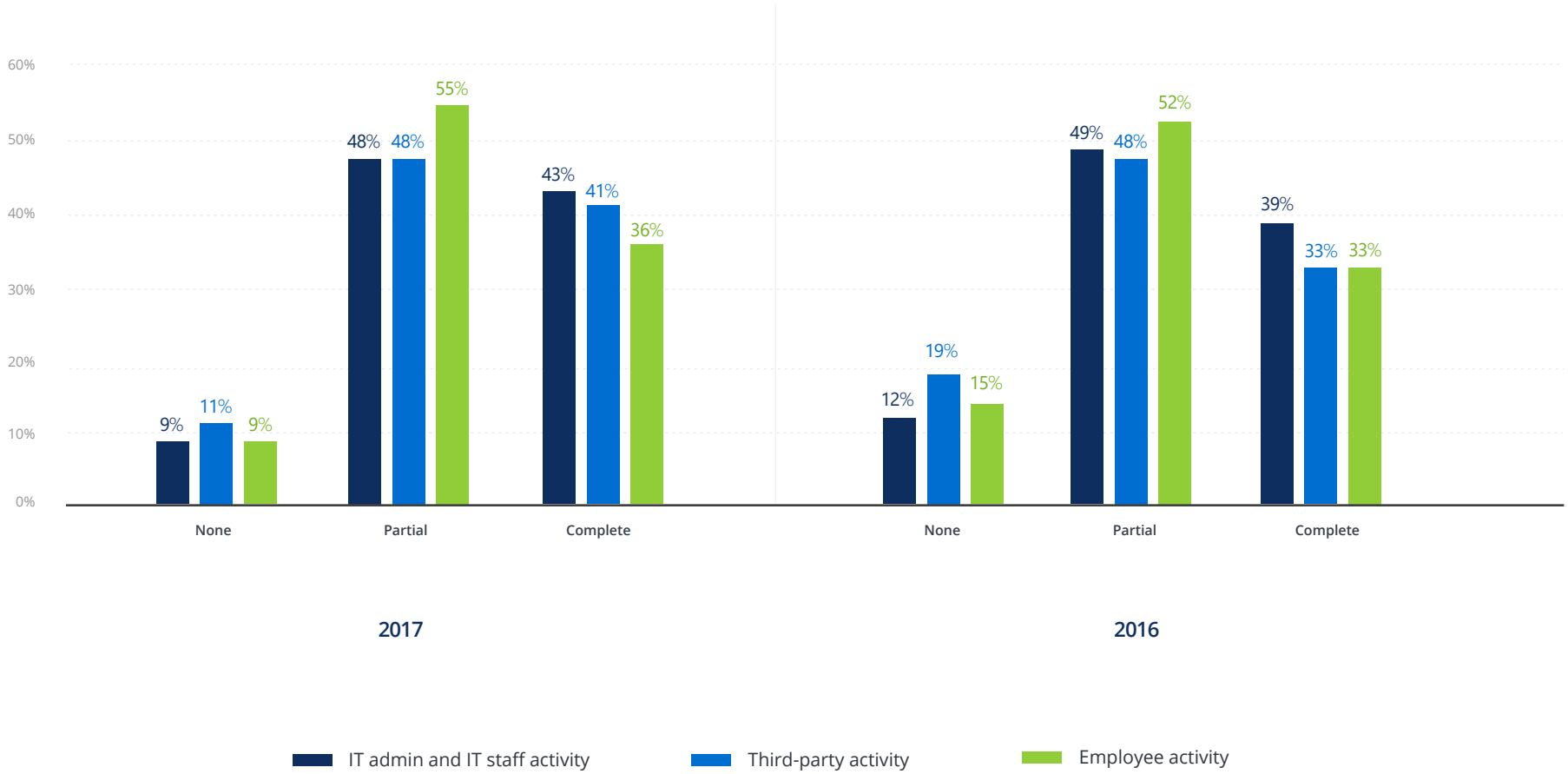
As we see, still less than a half of respondents have a deep understanding of what people who are given access to the internal IT systems are doing across the network. However, we cannot ignore that the number of organizations that do not have any visibility slowly decreased compared to the data we received last year. Another piece of good news is that the average number of organizations that have complete visibility has slightly grown.

Visibility organizations have into user activity and IT changes in their IT networks: weighted average[2] (1 – none, 2 – partial, 3 – complete)



[2]Here and after, we are using an average value to show the importance of each factor. In this case, we asked respondents to evaluate which level of visibility they have for each of the proposed variants in order to calculate a weighted average across all replies.

Visibility organizations have into user activity and IT changes in their IT networks



2.3 Visibility into User Activity in Various Systems

> *A third of organizations find it difficult to gain visibility to control shadow IT and BYOD.*

Traditionally, organizations claim to have maximum visibility into endpoint protection (61%), virtual infrastructure (59%), on-prem systems and databases (both – 52%). These results correspond to the ones we received last year (see the 2016 Netwrix Visibility Report), though the number of organizations that have complete visibility for these systems has slightly increased.

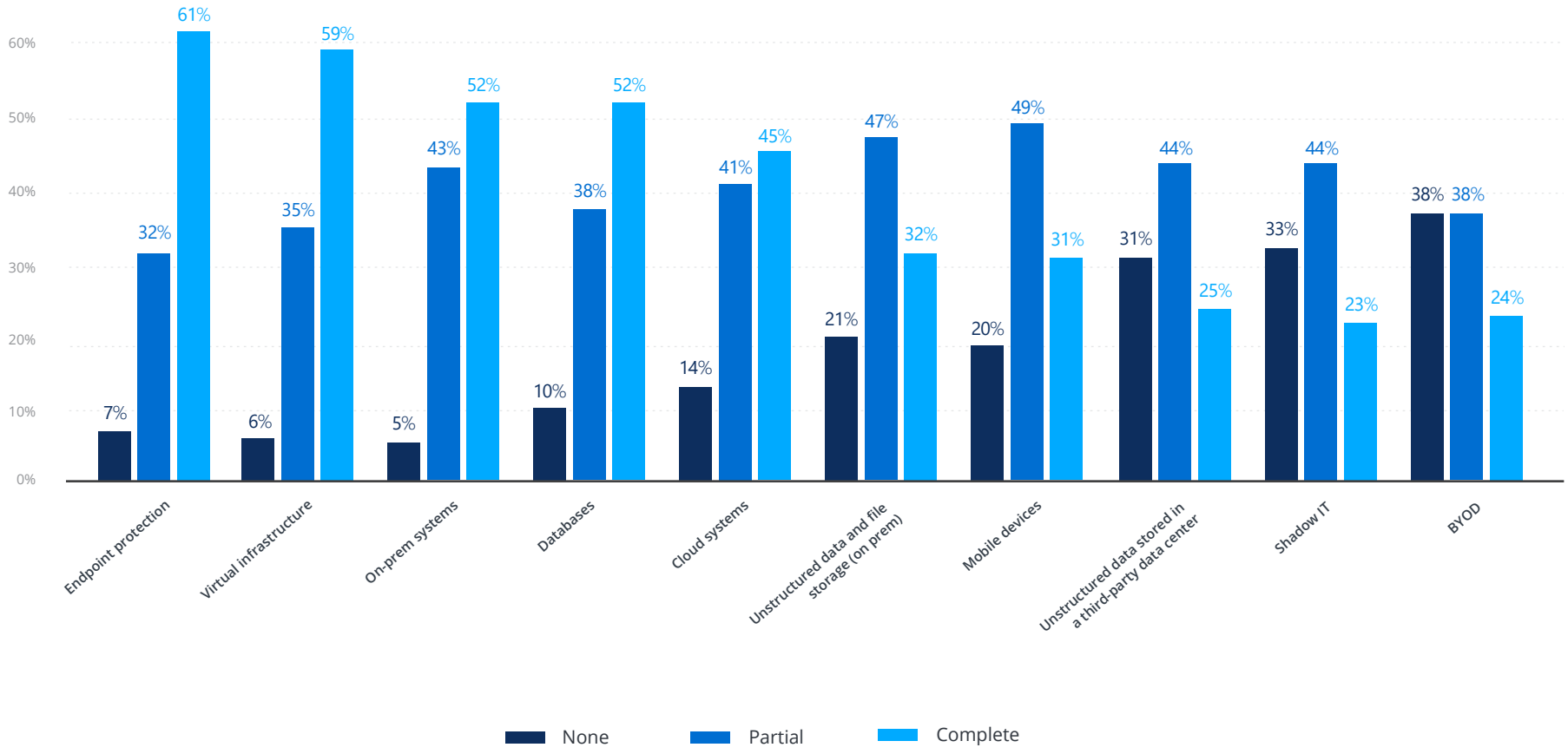
Organizations still struggle to gain visibility into cloud systems (45% - complete / 14% - none). However, compared to the data obtained last year, we observe a significant improvement, which is quite expected considering the effort cloud providers make to enhance security[3] and provide proof of security to customers.

Manipulations with unstructured data, regardless of the storage location, are still hard to control and are not fully tracked by the majority of organizations. The visibility for unstructured data stored on the premises is not much better (32% - complete / 21% - none) than for data kept in a third-party data center (25% - complete / 31% - none).

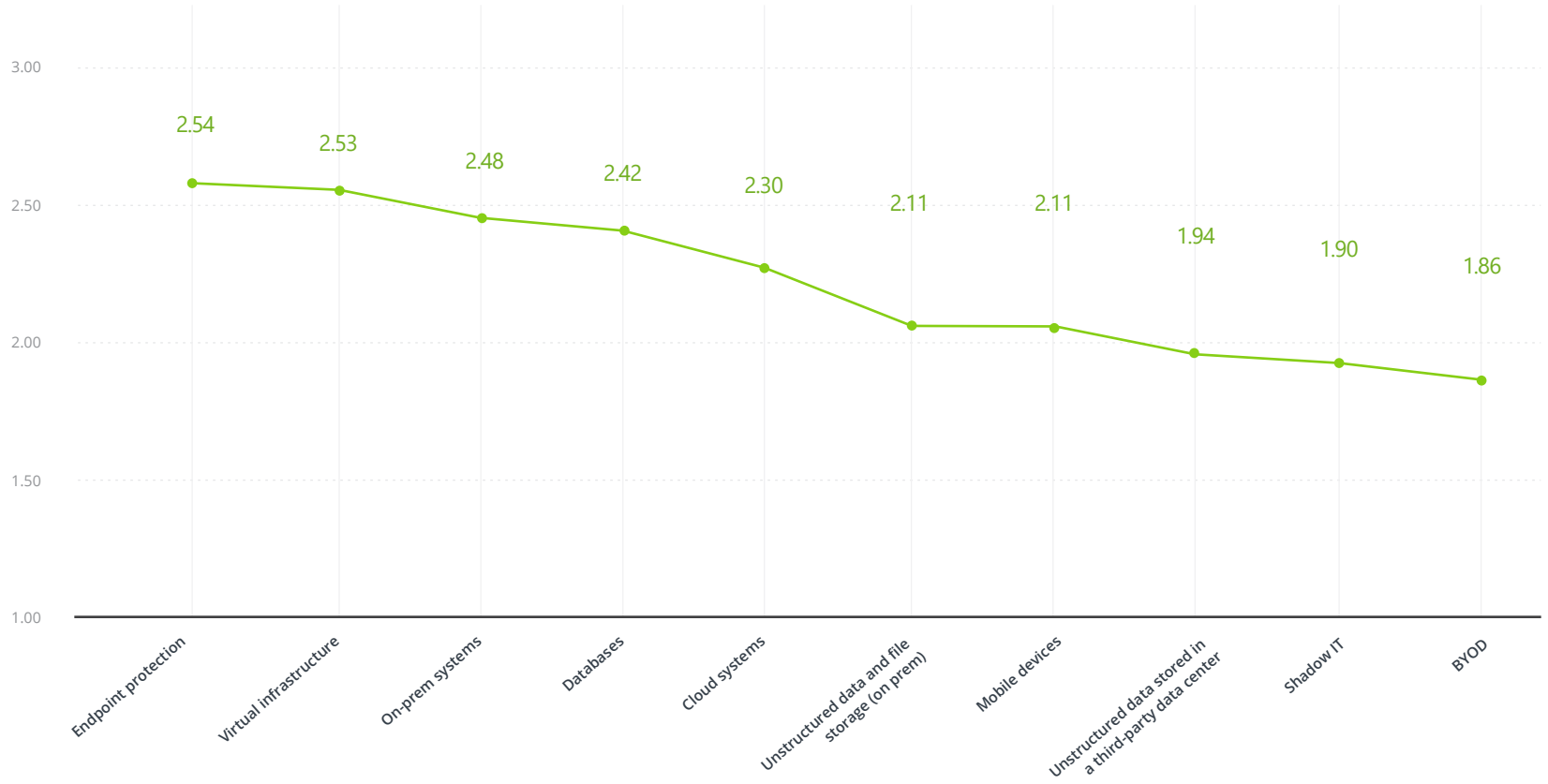
Only 23% of respondents claim to have full control over user installations, and another 33% of them do not have any visibility into it. Organizations continue to have little control over mobile devices, both corporate (31% - complete / 20% - none) and personal (24% - complete, 38% - none). These findings further confirm respondents' perceptions of having low visibility into employees' activity.

[3]To learn more about cloud security, please read our 2016 Netwrix Cloud Security Report.

The level of visibility organizations have into user activity and IT changes



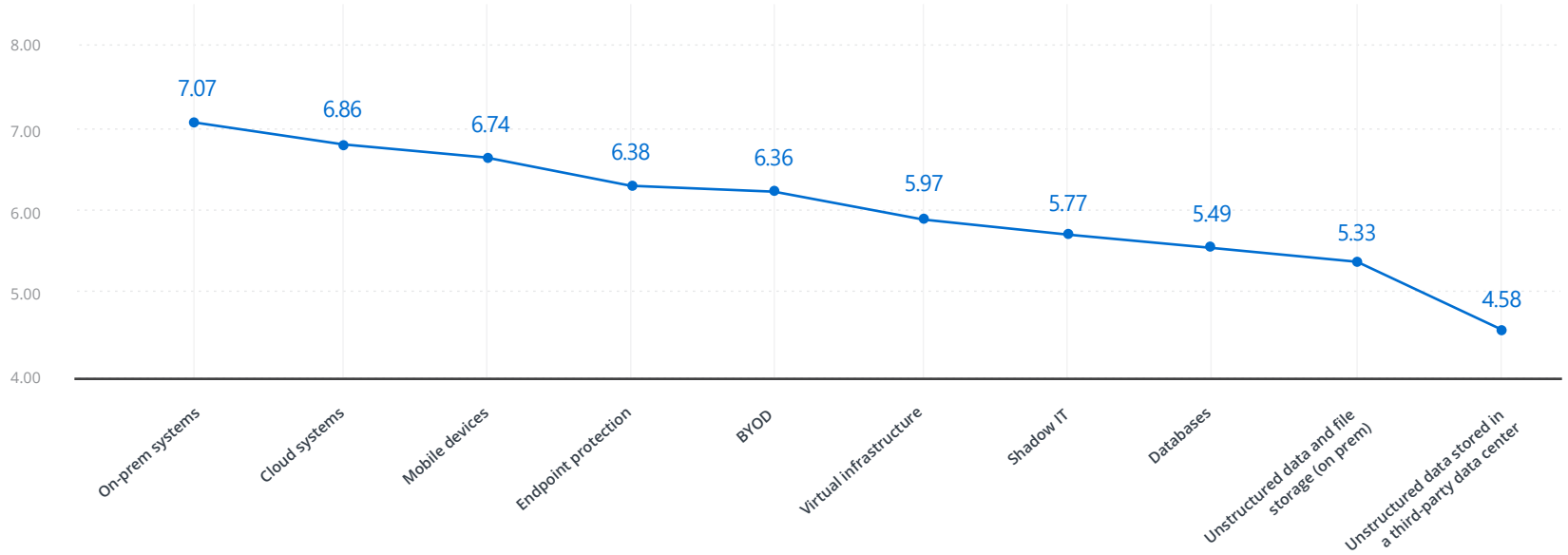
The level of visibility organizations have into user activity and IT changes: weighted average (1 – none, 2 – partial, 3 – complete)



Despite the generally poor understanding of the activity in various IT systems, it is hard to make any conclusions about organizations' ability to deal with cyber risks as we don't know what is critical and what is not.

Therefore, next, we asked our respondents to estimate the importance of visibility into various aspects of the IT infrastructure. What is also interesting is that organizations that in most cases dread a data breach don't consider file storage to be critical for security. The majority of them think that visibility into systems and devices is more important for organizations' well-being than visibility into unstructured or structured data.

Systems and data that pose the biggest risk to organizations when visibility is low (on the scale from 1 – "lowest risk" to 10 – "greatest risk")



2.4 Value of Visibility

> *Visibility primarily benefits security initiatives, helping organizations to detect, investigate and mitigate risks, and to prevent damage.*

When it comes to the benefits visibility into user activity and IT changes brings to organizations, respondents almost unanimously distinguish its value for security of the IT infrastructure. About 79% of all respondents consider it to be crucial for detecting and mitigating the human factor, regardless of whether it is a malicious misuse or accidental error. It is also important for quick and efficient investigation of security incidents (73%), security of the network and data in general (55%) and mitigation of security risks (53%). Even though visibility is important for a great number of organizations to increase the efficiency of internal operations and system uptime, as well as to pass compliance audits, there is no doubt that primarily, it has become crucial to build a security strategy that is able to deal with threats at all stages of attack.

Value of visibility. Choose all that apply

79%	Detecting and mitigating human factors (errors, misuse, etc.)
73%	Investigating security incidents
55%	Ensuring the security of network and information assets
53%	Proactively preventing threats and mitigating risks
44%	Optimizing IT processes and operations
44%	Gaining a deeper understanding of processes and risks
42%	Maximizing system uptime
41%	Ensuring proper internal control processes
40%	Making better decisions about IT processes and controls
36%	Optimizing IT infrastructure and storage management
31%	Delivering audit and/or compliance reports quickly
29%	Facilitating compliance (reducing time, budget, stress level)
21%	Facilitating IT infrastructure transformation

Part 2. **Summary**

The results clearly demonstrate that IT pros prefer to concentrate their efforts on perimeter and cloud systems rather than get a deeper understanding of what is happening inside of their IT networks. Despite the slightly positive shifts in this year's data, the majority of organizations continue to stay in the dark about user activity in the network. This is true especially when it comes to employee and third-party activity, as well as any manipulations with data.

Such focus comes as no surprise since all IT tasks mostly fall on the shoulders of IT operations, and even basic processes and mechanisms have some major flaws. Being responsible for everything leads to prioritizing the challenges and increases efforts to succeed in the short term. For IT pros, this means that maintaining daily operations and ensuring systems availability come to the fore. In this context, more high-level tasks, such as ensuring data security and understanding manipulations with sensitive assets, may recede into the background until organizations gain visibility around the perimeter.

Taking into account that IT pros are more often unaware of the activity and changes in their IT infrastructures, it seems fair to assume that for the most part, organizations are not ready to manage even well-known IT risks.

Low visibility into data and their own employee activities makes organizations easy targets for fast-paced attacks, such as ransomware. The saddest part is that early detection of a data compromise or data tampering is almost impossible for organizations with low visibility into business-critical assets.

It is interesting to note that the top benefits organizations gain thanks to visibility are directly related to security. However, most of organizations consider low visibility into structured and unstructured data, stored on the premises or in the cloud, an acceptable situation.

PART 3

IT Risks: Operations, Security, Compliance

Roughly speaking, all IT risks can be divided into three categories: operations, security and compliance. Failure to deal with any one of them can have serious consequences for organizations – from financial losses and reputational damage to inability to do business.

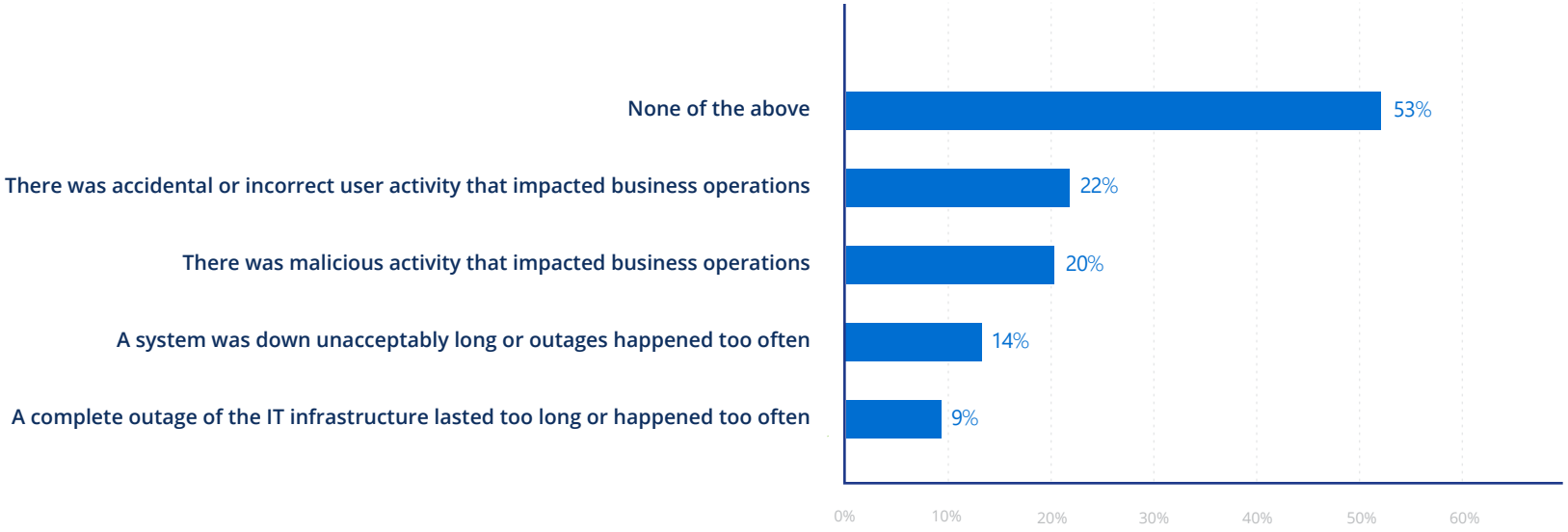
Further, we are going to examine the organizations' exposure to risks by analyzing various incidents they experienced in 2016. While there is no way to completely prevent all incidents, we are mostly interested to see whether the companies can efficiently deal with the threats they face.

3.1 Operational Risks

> *81% of organizations have taken the risk of operational failures seriously, which made them take actions to speed up incident investigation.*

About half of surveyed organizations (47%) continued to experience various operational issues during the last year. The most popular reason for that was incorrect user activity (22%) and malicious activity (20%), which resulted in disruption of business operations.

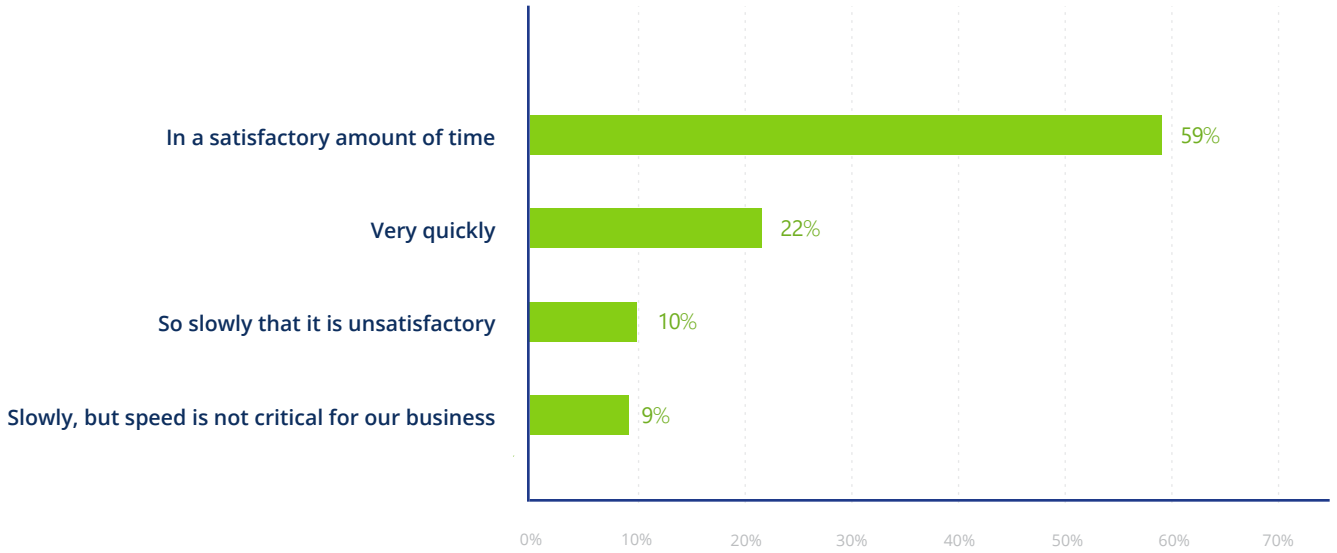
IT incidents in 2016, experienced by organizations due to insufficient visibility into user activity across infrastructure. Choose all that apply



Meanwhile, the majority of respondents estimated time needed to find the root cause of the incident as “very quickly” or “satisfactorily quickly” (81% overall), which is a huge success compared to the results of 2016, when only 49% were able to investigate the incident fast enough.

The initiative to keep systems up and running and find the root cause within the minimum period of time greatly helps to mitigate risks of system downtime and allows businesses to ensure stable operations.

Time needed to identify the root cause of system downtime



3.2 Security Risks

> *Malware and human errors lead the list of the root causes for security incidents in 2016.*

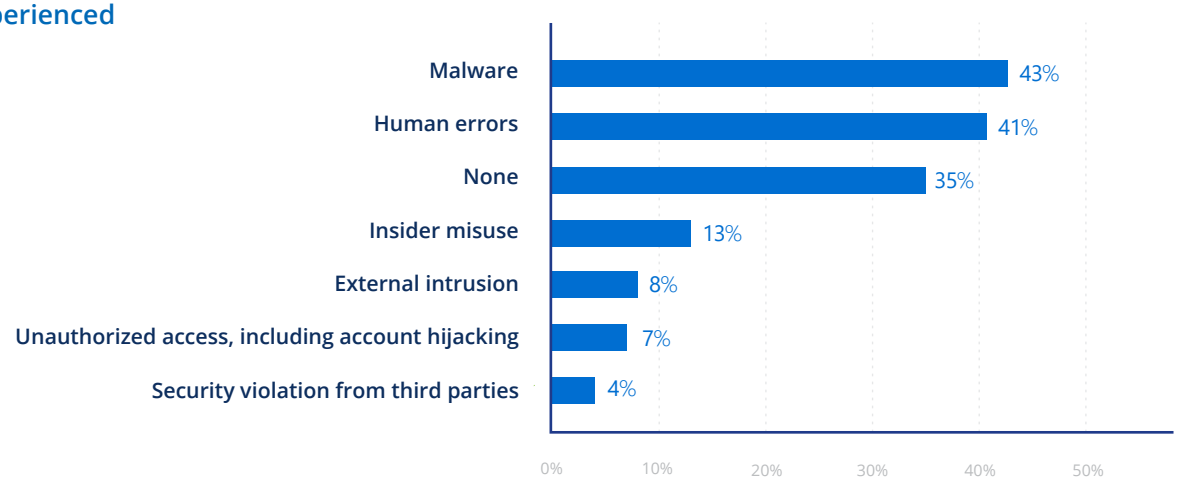
Overall, 65% of organizations experienced one or more security incidents in 2016.

Just as last year, malware (43%) and human errors (41%) again lead the list of security incidents. Now, they changed places (in 2015, human errors attributed to 47% of security incidents and malware to 39%), which comes as no surprise, as last year was marked by the rise of ransomware.

Insider misuse remains an issue for 13% of surveyed businesses. It is interesting to note that 4% of organizations also experienced security violations from third parties (partners, contractors, vendors, etc.) with legitimate access to the corporate IT network.

External intrusion (8%) and unauthorized access (7%) complete the list of the most popular reasons for security incidents this year.

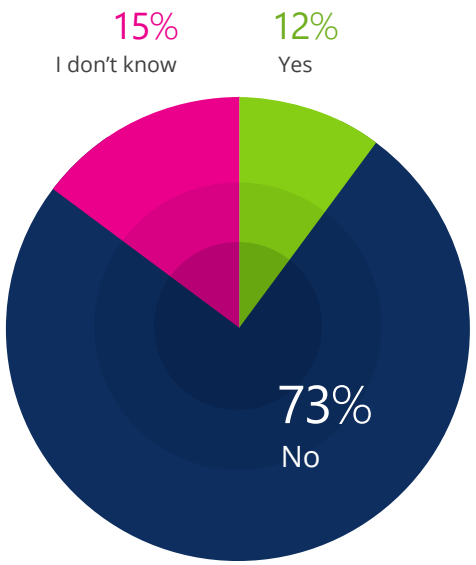
Security incidents that organizations experienced in 2016. Choose all that apply



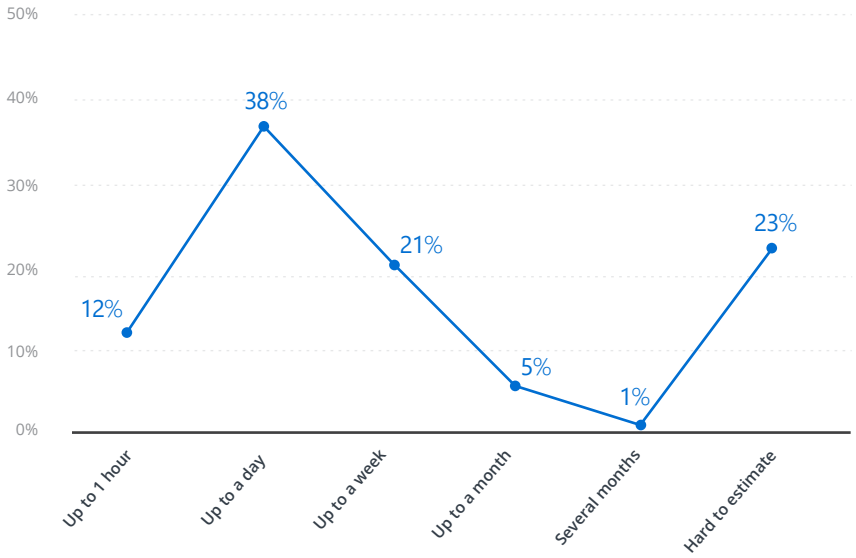
Among those companies that experienced any of the incidents listed above, 12% of respondents admitted that the incident (or occurrence of incidents) resulted in a data breach. What is more disturbing is that 15% of organizations have no ability and/or desire to check if the incident led to data exposure.

When it comes to time spent on incident investigation, only 12% of organizations claimed that it takes them about an hour after incident discovery to learn a root cause, while almost 40% can do it in one day, and 21% require about a week of time to identify what has happened.

Did any of those incidents result in a data breach?



Average time spent on investigating a security incident



3.3 Compliance Risks

> *Almost half of organizations still struggle to ensure continuous compliance, provide complete evidence to auditors and pass IT audits.*

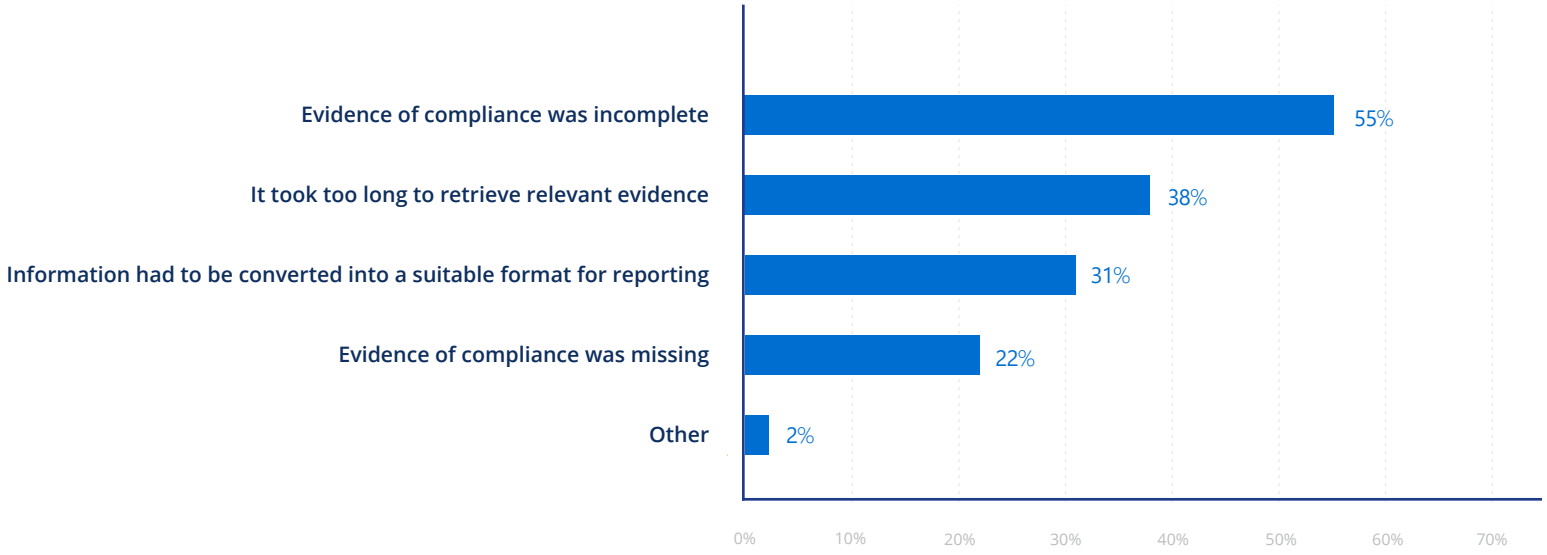
Further, we are going to examine the practices of companies that comply with any internal or external requirements.Despite the fact that the majority of compliant organizations do not have a separate person or team responsible for compliance, about half of respondents (52%) claimed they didn't have any compliance or audit-related issues in 2016. Every fifth organization was found to have unsatisfactory IT auditing processes, even though they did not experience any difficulties with passing regular IT audits. Every sixth organization didn't pass internal (14%) or external (16%) audits at least once. On average, one in ten organizations was not able to quickly provide specific information to meet auditors' requests.

Issues experienced during internal or external IT audits in 2016. Choose all that apply

Among the organizations that had at least one incident during an internal or external IT audit, 55% were not able to provide complete evidence of compliance, 38% had to spend a long time finding the required information and 31% couldn't share information in a readable format that was suitable for reports.

This means that the major problem organizations encounter is inability to gather all compliance-critical data and work with it to normalize it, clear out the mess and present it in an easy-to-read format.

Causes of issues during IT compliance audits. Choose all that apply

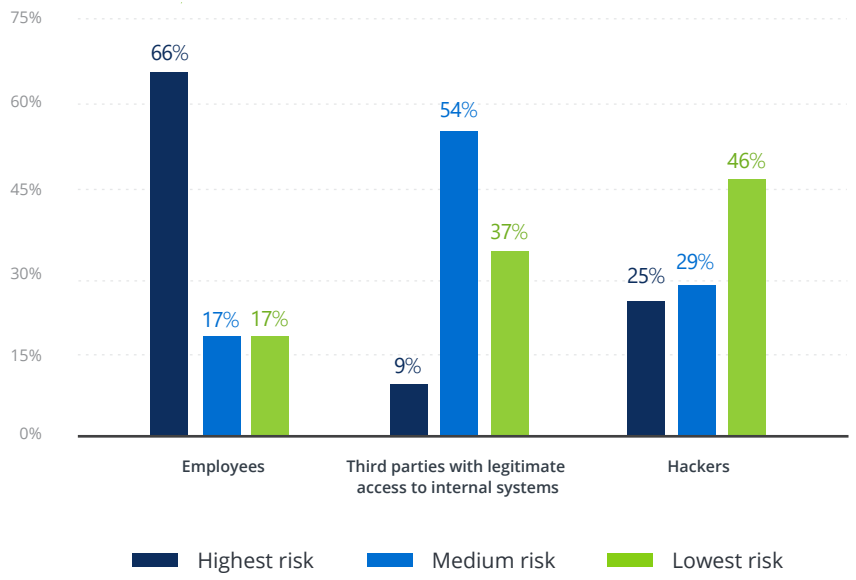


3.4 Human Factor as a Threat

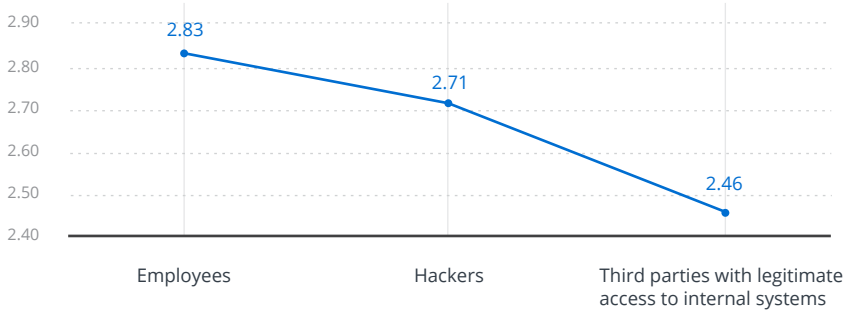
> *66% of organizations perceive employees as the biggest threat to system availability and security.*

Respondents were asked to estimate, based on their experiences, who poses the biggest risk, both from security and system availability points of view. The absolute majority (66%) see the greatest threat coming from employees. This doesn't fit with the fact revealed earlier that only 36% of companies have visibility into the activity of their regular users. Hackers are perceived as even less dangerous. What is more confusing is that only 9% of respondents considered third parties, such as vendors, contractors, partners and so on, to be the primary risk. Even though third parties have legitimate access rights to internal systems and may operate with sensitive data, their risk level is considered medium or low.

Biggest threat to security and system availability



Biggest threat to security and system availability: weighted average (1 – lowest risk, 2 – medium, 3 – highest)



Part 3. **Summary**

In the previous part of the report, we learned that the majority of IT pros estimate their visibility into systems and data to be incomplete or close to zero.

Visibility itself would not decrease the number of incidents, but it translates into better awareness about vulnerabilities, lack of certain policies or failure to follow them, and missing controls. This, in turn, should result in higher accountability of all users, improved processes and policies, and better controls should the follow-up measures be taken to eliminate drawbacks.

All of these positive dynamics naturally lead to fewer operational issues, less employee negligence, increased security and decreased efforts for compliance, according to 78% of the respondents who already have visibility[4].

Thus, the perceptions discussed in the previous part correspond to the results demonstrated in this part: More than half of organizations experienced operational, security and compliance issues in 2016.

While some of these issues are inevitable, no matter what you have in place, others can be significantly reduced or eliminated more quickly when organizations gain better visibility.

An even more interesting finding is that organizations continue to see their own employees as the biggest threat to security and business continuity. However, as we previously saw, the visibility organizations have into employee activity and even into that of IT staff has not improved much since our last survey, and for many organizations, it is far from being complete.

[4] 2016 Netwrix IT Risks Report

PART 4

Threat Resistance and Next Steps

In previous parts, we learned what controls organizations have in place, how IT pros perceive them and what risks they faced over the last year. Now, we are going to find out whether organizations are well prepared to beat future IT risks and, if they are not, what stands in their way.

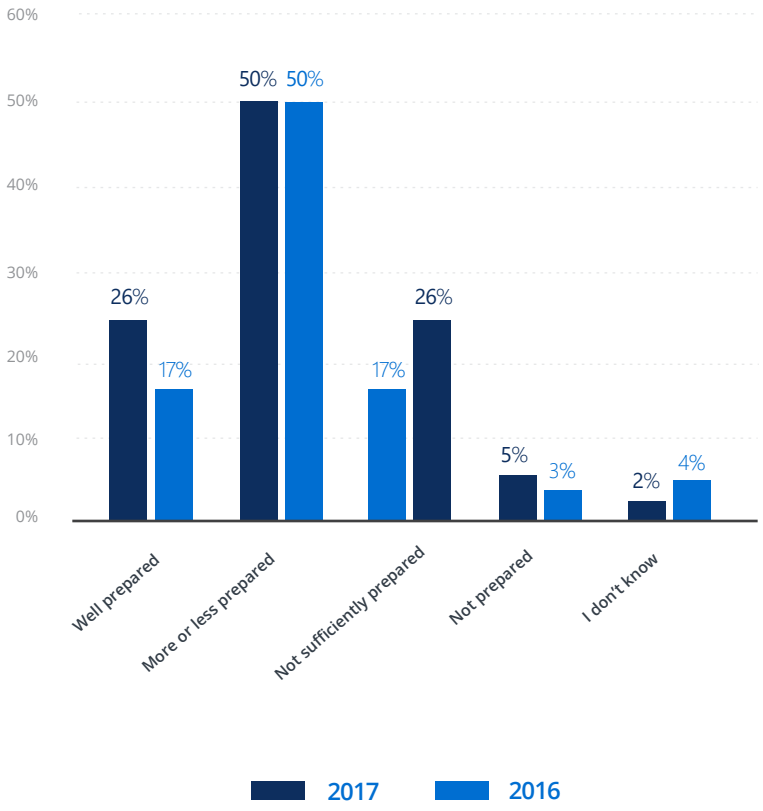
We are also going to find out what steps IT pros are going to take next, what will be the focus of their efforts and what the threats are that need maximum attention.

4.1 Threat Resistance

> *Only 26% of organizations are well prepared to beat IT risks.*

A risk mitigation strategy is not easy to develop, implement and follow. However, organizations tend to care about it more than they did in the past. Companies have started to take a strategic approach to foresee possible threats and take steps to minimize the impact in advance. The number of organizations confident about their IT risk strategy grew from 17% in 2016 to 26% in 2017. Subsequently, the group of respondents who admitted that their organizations are not sufficiently prepared or not ready at all to deal with any kind of IT risks decreased from 29% in 2016 to 22% in 2017. Still, half of the respondents are somewhat prepared, which means that there is room for improvement.

How well organizations are prepared to beat IT risks



4.2 Obstacles

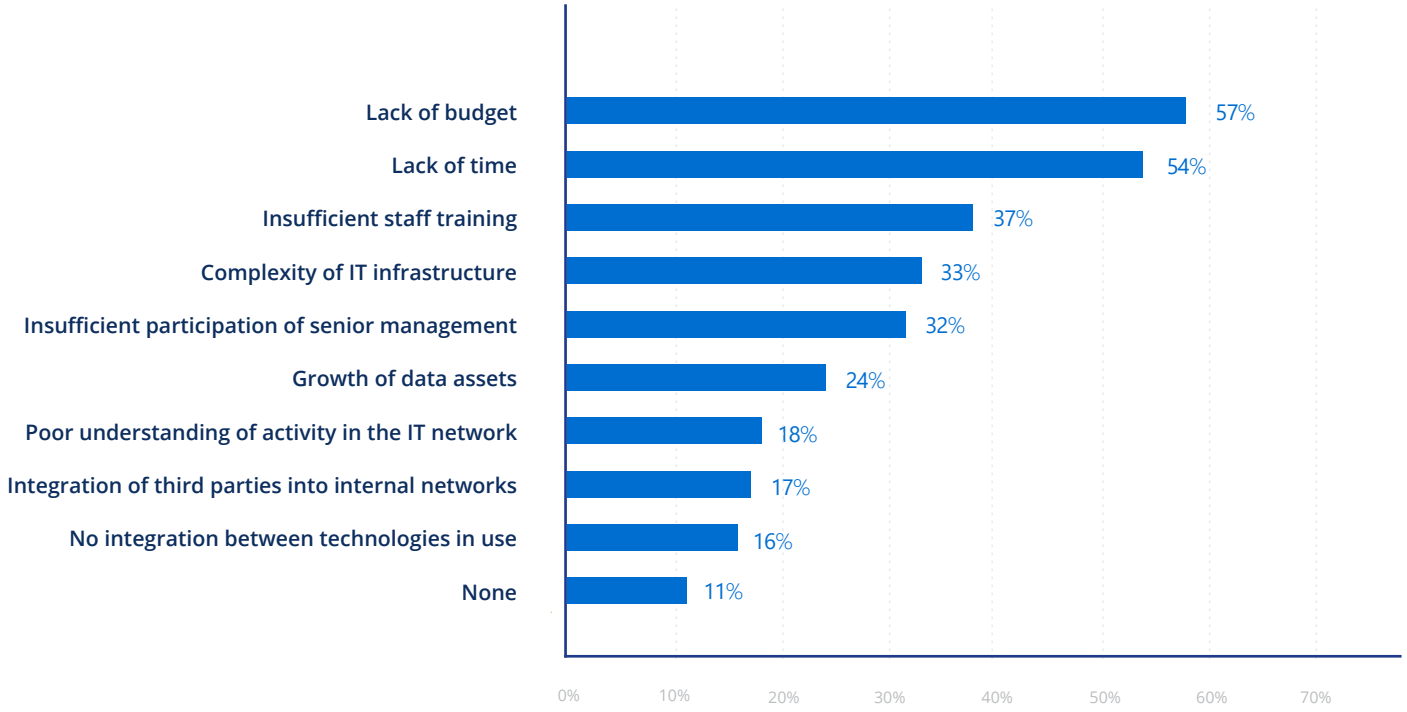
> *Lack of budget and time are the main obstacles to minimizing IT risks.*

The factors that prevent implementation of a more efficient IT risk strategy are the same as last year: lack of budget (57%), lack of time (54%) and insufficient staff training (37%). All three are persistent problems for IT departments worldwide.

Buried under the routine tasks that are not optimized and quite often not automated, having to take various functions and roles, IT teams cannot act proactively, which undoubtedly has a negative impact on organizations' ability to assess and beat IT risks.

Employees' poor knowledge of cyber threats and failure to follow security policies only add to the problem. Already having a lot on their plates, IT departments have to deal with another challenge: lack of involvement of senior management (32%). Although in other circumstances, the management could have offered great help with allocating additional budget and hiring new staff, only a third of respondents indicated poor involvement of the management as one of the major problems.

Obstacles. Choose all that apply



4.3 Next Steps

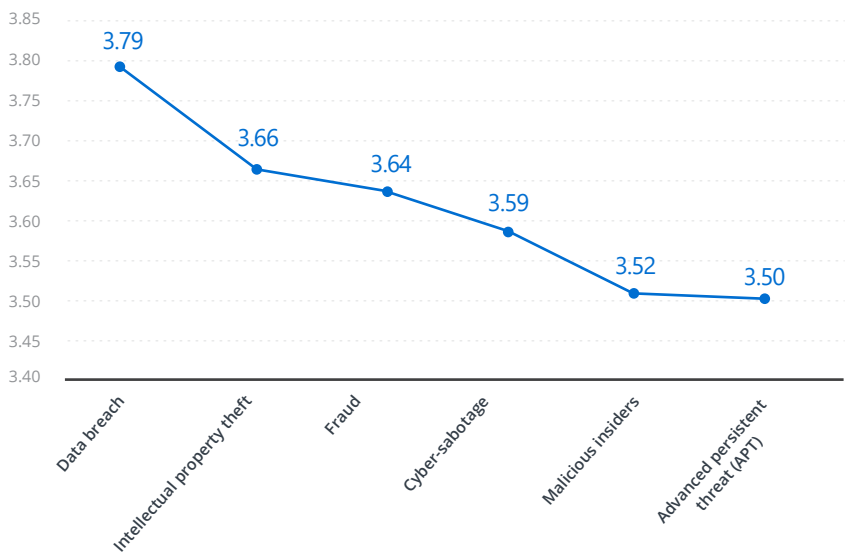
> *Organizations are planning to focus their investments on securing sensitive data, as they cannot foresee every possible threat.*

Organizations have to deal with various threats, but the resources are always limited. Living in the real world, they cannot have everything at once and have to compromise and pick what is more relevant to the situation. Respondents were asked to evaluate their readiness and willingness to invest time and effort into protection from various threats on a scale from 1 (not willing) to 5 (absolutely willing).

The results show that organizations are first and foremost preoccupied with security, integrity and controlled access to sensitive data. Public exposure of data, its leakage to adversaries or intellectual property theft may considerably damage businesses. Cyber-sabotage, malicious insiders and advanced persistent threats, while being concerns as well, are less of a hot topic on the agenda.

Having built a more or less successful perimeter defense, organizations understand that it is only one of many steps they have to take to secure the entire IT environment. And being unable to foresee every possible threat, not having enough resources to deal with the risks, organizations are moving toward a data-centric approach to focus their efforts on business-critical assets.

Readiness to invest time and effort in protection from the security threats (from 1 – not at all ready to 5 – absolutely ready)



Part 4. **Summary**

Few organizations have all the resources available to beat any possible cyber risks. Most of them have to juggle with what they have, often stumbling upon lack of support from senior management. Year after year, IT pros complain that they don't have sufficient budget and time, while complexity of IT infrastructures, dependencies between systems and data volumes continue to grow, worsening their already insufficient visibility.

Having to deal with the great variety of issues, IT departments worldwide manage to take small steps to better support business operations and make their organizations more secure and compliant.

The number of IT pros who are sure about their organizations' readiness to beat cyber risks is still very small, but they are committed to growing further.

As we found out in this part of our survey, IT pros do understand the absolute necessity to protect their data from fraud, theft or breach, and they are willing to invest in data security. However, again, they are at the same time preoccupied with improvement of their system and network security and have many unsolved issues.

It is worth noting that while IT pros face a variety of threats, they are not willing to put all eggs in one basket and invest in protection from just one type of threat. Instead, in the context of a growing variety of threats and lack of resources, they would like to take a more reasonable approach and protect the valuable data from anything that may undermine its integrity and security.

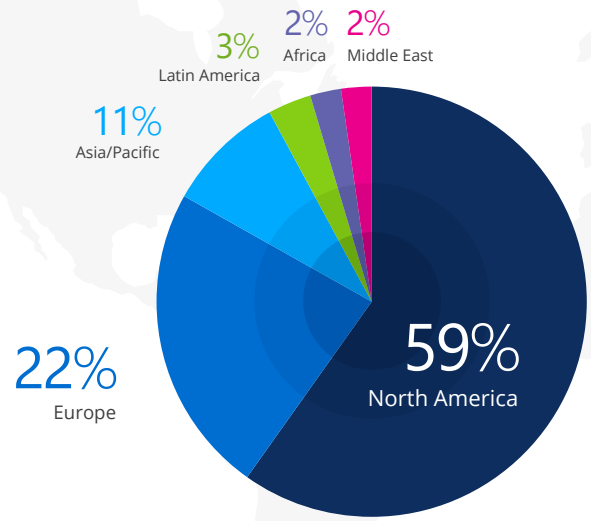
PART 5

Respondent Demographics

Geography

Respondents from **723 organizations** shared their insights, pains and best practices for this report. Traditionally, the majority of them come from North American organizations (59%), followed by European businesses and institutions (22%). About 11% of surveyed organizations are from the Asia/Pacific region. Latin America, Africa and the Middle East are represented by 7% of respondents.

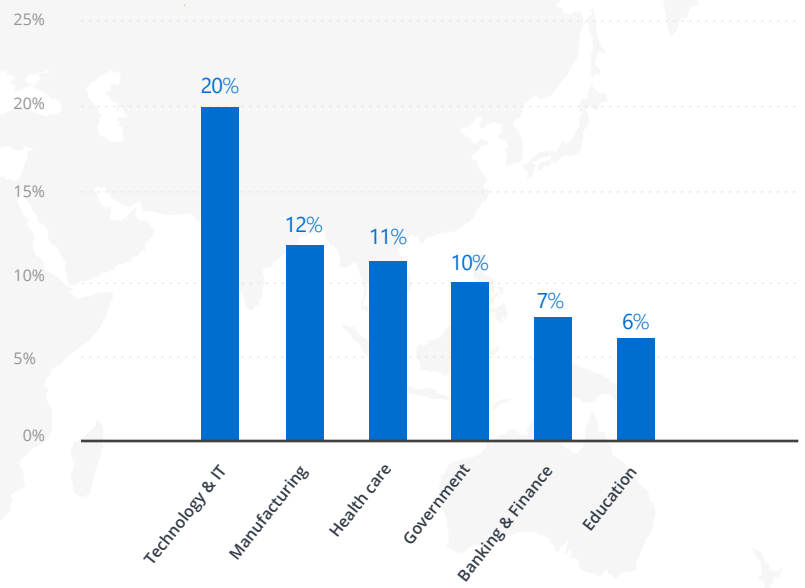
Home region



Industry Vertical Top 6

The respondents of the survey come from more than 30 industries. The majority of them work in technology and IT, manufacturing, health care, government, the financial sector and education.

Industry vertical top 6

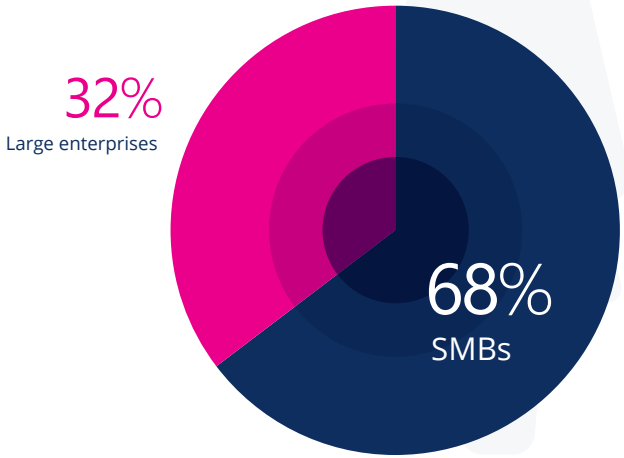


Organizational Size

The surveyed organizations were grouped by size, using Gartner's[5] definition of small businesses (1-99 employees), midsize enterprises (100-999 employees) and large enterprises (more than 1000 employees).

Two thirds of the survey respondents represent small and medium businesses, and about one third represent large organizations.

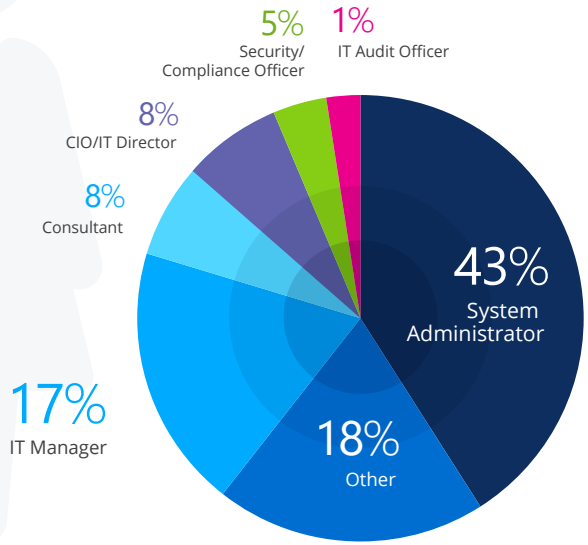
Organizational size



Job Titles

About 43% of our respondents are system administrators, 25% hold management positions and 18% are infrastructure analysts, IT support, IT infrastructure officers, system engineers, network technicians and so on.

Respondents' job titles



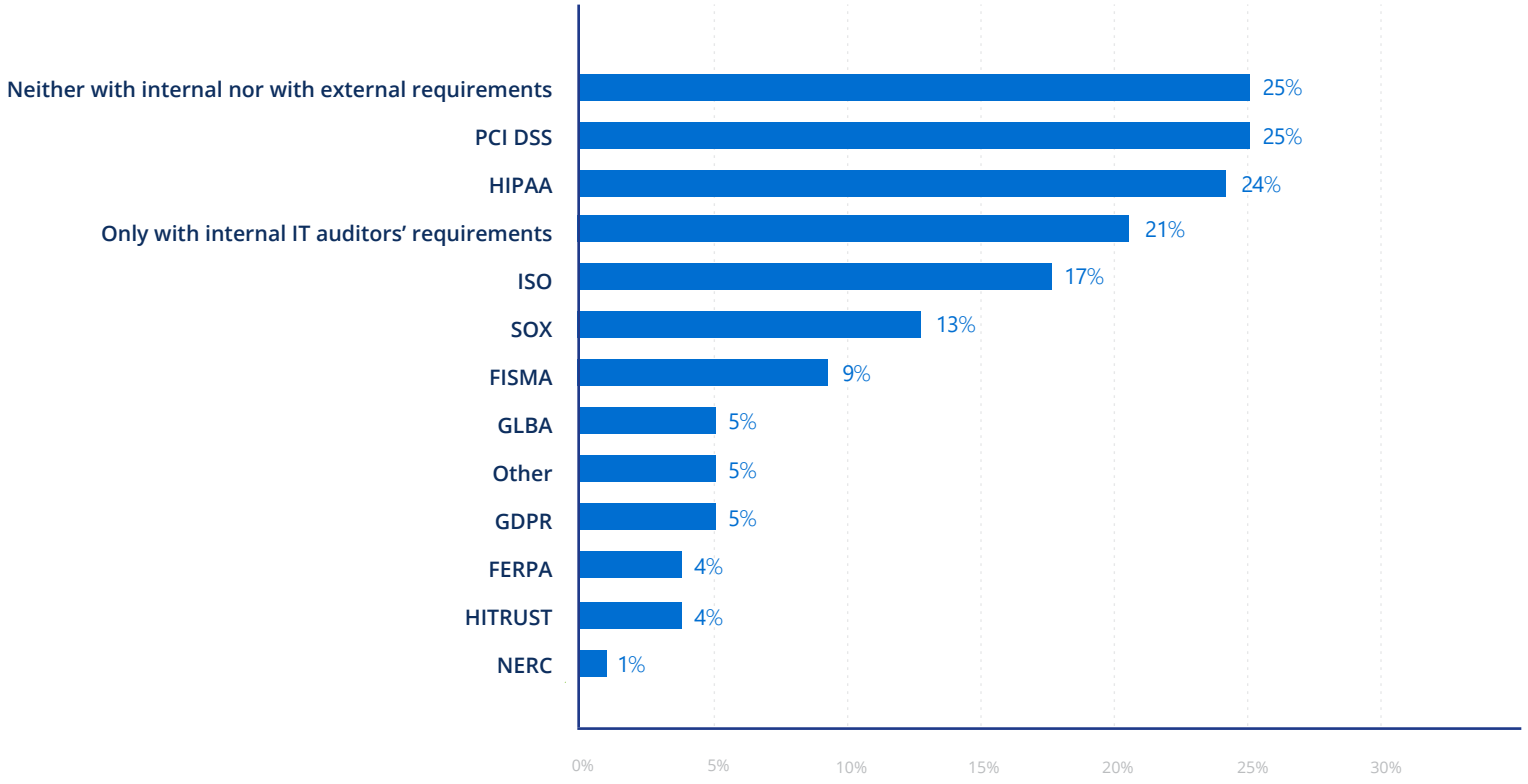
[5] Based on Gartner's definition of small and midsize businesses (SMBs) by the number of employees.

Compliance with Internal and External Standards

The absolute majority of the respondents of this survey (75%) have to comply with various regulations on cyber security.

About a fifth of organizations (21%) deal only with internal requirements, while others have to meet one or more standards.

Compliance with internal and external standards. Choose all that apply



Conclusions and Recommendations

Every year we see more security incidents, even though organizations are working harder than ever to shield their systems and data. Compared to last year, there is a positive dynamic in how organizations protect themselves from various IT risks, handle threats and mitigate potential damage. They have realized that they don't have any other choice but to become more secure, more compliant and more efficient in troubleshooting. A security vulnerability or loophole, employee negligence or malicious intent, or an incident that impacts security or system availability can generally be attributed to lack of visibility and ultimately affect the business as a whole.

There are multiple reasons why organizations aren't keeping up with the speed at which threats are multiplying. First, their IT environments are growing and compliance requirements are getting tighter. In addition, they usually still have legacy challenges they need to work on. And they often face insufficient budgeting, understaffed IT teams, the need to educate and control users, and a lack of support from senior management.

Despite these challenges, organizations generally are gravitating towards a holistic approach to handling IT risks. They understand that perimeter-based defense is not as effective as it used be, and they want to see all the activity inside the perimeter and focus on protecting valuables, rather than everything at once. They also realize that more often than not, incidents are caused by people with legitimate access who either make mistakes, fail to strictly follow established policies, are unaware of today's threats, have an evil plan or whose identity is used by external adversaries to get to the assets.

In this context, IT teams are advised not to rely entirely on the skills, knowledge and good intentions of users who are granted access to internal systems. Instead, they must take a more proactive approach to security, compliance and operations by gaining visibility into what is happening across the entire IT environment. In particular, they must:

- **Know what is happening around sensitive data and business critical systems.**

  System downtime, noncompliance and leakage of sensitive information are serious risks for businesses. IT pros are strongly advised to focus their efforts on incident detection and response. Visibility into user activity in critical systems and manipulations of valuable informational assets help mitigate the IT risks by exposing unwanted activity at early stages. In addition to enabling IT teams to stop incidents from escalating to serious issue, visibility also helps them identify weak spots in their security and compliance processes for proactive improvement. It provides knowledge about real exposure of data and the IT infrastructure to various threats or attacks in progress, even the currently most popular and feared threat, ransomware. This knowledge provides practical guidance for establishing IT controls and practices that are more tailored to the context and business specifics.

- **Analyze all user activity.**

  Organizations should not neglect the activity generated by all users allowed into the corporate IT environment, regardless of whether they are privileged users, regular employees, partners, contractors, vendors and so on.

  Monitoring alone is not enough. Organizations should be notified if there are suspicious activities, such as too many access attempts to data, system logins outside of working hours or any other odd activity for a certain user. IT teams should be able to easily investigate all suspicious events and take appropriate measures to resolve potential or ongoing issues. While external adversaries may attempt to mimic real user activity, identification of normal and odd user behavior patterns is crucial for better protection of the IT environment.

- **Do more with resources you have.**

  It would be unrealistic to hope that anytime soon IT teams will get the management support and budgets they need to unload themselves from the extra security and compliance tasks they perform on top of their normal duties. For this reason, IT pros are advised to identify the most time-consuming processes and see where they can be automated. One of such routine tasks is manual processing of logs when investigating and troubleshooting IT incidents or looking for information required either by auditors or by management. By automating IT auditing, IT teams will be able to improve the efficiency of operations, increase security and compliance, and reclaim the time they need to focus on more high-level tasks.

About the Report

The report is brought to you by Netwrix Research Lab, which conducts industry surveys among IT pros worldwide to discover up-to-date interests and granular trends' analysis of the industry. For more reports, please visit:

www.netwrix.com/go/research

About Netwrix

Netwrix Corporation was the first vendor to introduce a visibility and governance platform for hybrid cloud security. More than 160,000 IT departments worldwide rely on Netwrix to detect insider threats on premises and in the cloud, pass compliance audits with less effort and expense, and increase productivity of IT security and operations teams. Founded in 2006, Netwrix has earned more than 100 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Corporate Headquarters: 300 Spectrum Center Drive, Suite 200, Irvine, CA 92618

netwrix.com/social