

2015 State of IT Changes Survey

Regardless the size **70%** of IT teams make undocumented changes and put their systems at risk of security breaches

Contents

Introduction.....	3	Security vs. System Uptime	
Survey Highlights.....	5	Overall Overview.....	25
Survey Responses.....	7	Organization Overview.....	28
Change Management and Documentation		IT Team Overview.....	31
Overall Overview.....	7	Conclusions and Recommendations.....	33
Organization Overview.....	9	Respondent Demographics	
IT Team Overview.....	11	Organization size.....	35
Change Auditing		Industry Vertical.....	36
Overall Overview.....	13	IT Team Size.....	37
Organization Overview.....	16		
IT Team Overview.....	17		
Hidden Threats			
Overall Overview.....	19		
Organization Overview.....	21		
IT Team Overview.....	23		

Introduction

700+

IT professionals surveyed

40+

industries covered

69%

of companies are SMB

One of the growing challenges in IT infrastructure management is the need to strengthen security, protect against data breaches and ensure business continuity. In the world where IT infrastructures are constantly changing to meet the growing needs of organizations, IT teams often find it hard to succeed in keeping track of every user's activity. Many changes to data and system configurations are made every day, and every change may result in violation of internal security policies, cause system downtime or take the organization out of compliance.

Last year, we initiated a survey to find out how companies deal with change management; this resulted

in the [2014 State of IT Changes Survey](#), which revealed that organizations are not as good at managing changes across their IT infrastructures as they believed they were. The results showed that companies are constantly making changes that impact service performance and even result in security breaches. One of the main reasons for this was lack of visibility into what is going on in IT systems and low ability to conduct further root cause analysis. However, companies were the only ones to blame for these issues as more than half of them made undocumented changes and 62% had little or no real ability to audit what modifications they had made.

The survey showed that organizations turned out to be absolutely unprepared for the avalanche of security breaches that hit all industries in 2014. Throughout the year we have been reading about new companies being breached and have been terrified by the amount of sensitive data stolen and the amount of loss to be compensated. These disappointing results made us continue to research this problem and initiate a second survey to find out how massive security breaches and violations of compliance standards have changed the organizations' attitudes toward change management. We were

curious as to whether organizations have decided to implement change management controls and try to document every change made.

Or, maybe they prefer to either rely more on the responsibility of their employees to document everything they do or hope for the best, assuming that all changes are adequate and made only by authorized users.

This year we have surveyed more than 700 IT professionals to find out whether they have made any upgrades to their frameworks throughout the year. In order to

make the results as representative as possible, we have covered small, medium and large businesses that are involved in more than 40 industries. IT professionals answered questions about change management controls in their organizations and shared some insights about how these policies worked in the real world. The main question that intrigued us was whether companies became more proactive in achieving visibility into their IT infrastructures, and therefore became more successful in strengthening security and ensuring system uptime.

Survey Highlights

1. Change Management and Documentation

- The same number, 60% of organizations, continue to claim they have established change management controls, and 80% try to document changes they make. However, the number of those who still make some effort in documentation despite the lack of any change management controls in place has increased by 19% throughout the year and reached 59%.
- The number of small companies that have started to track changes despite the lack of change management controls has doubled throughout the year (30% in 2014 against 58% in 2015).

- Smaller IT teams with up to 5 employees also became more responsible for documentation of changes. The number of IT departments that started to document changes has increased: for IT teams consisting of 1 employee from 37% to 68% and for IT teams of 2 to 5 employees from 45% to 77% throughout the year.
- However, organizations with large IT departments and no change management controls in place proved to be more lax about documentation. The number of IT teams that still document changes has decreased by 11% for teams of 6 to 10 and by 15% for teams with more than 10 IT pros on the staff, providing us with more proof that too many cooks can spoil the broth.

2. Change Auditing

- Companies started to take change auditing more seriously than they used to only a year ago. The number of organizations that have established change auditing controls has increased from 38% to 52% throughout the year.
- This technology continues to capture the market. Both small and midsize companies showed quite noticeable interest in establishing change auditing processes. The demand from large enterprises has increased even more and reached 75%, compared to 52% the previous year.

- Organizations tend to opt for several methods of auditing changes at the same time. Manual monitoring of native (system) logs is more common for SMBs, whereas enterprises choose automated auditing and even develop homegrown scripted solutions, although 35% of them still continue to look through native logs.
- Change auditing mechanisms gradually spread over IT teams of various sizes with the largest demand among smaller IT departments that have just started to be drawn to this technology.

3. Hidden Threats

- The number of IT pros who do not always document changes has reached 70%, compared to 57% in the previous year. The frequency of those changes has also increased.
- The number of large enterprises that forget to document changes has

increased by more than 20% and reached 66% throughout the year.

- Continuing the trend, enterprises make undocumented changes more often than SMBs: weekly against monthly.
- Organizations fail to document changes no matter the size of their IT departments. All IT teams from time to time forget to document changes they made.

4. Security vs. System Uptime

- 67% of organizations, no matter their size or the size of their IT teams, still suffer from system downtimes caused by incorrect or unauthorized changes, continuing the trend of 2014. Large enterprises are the worst offenders as 73% of them regularly make changes that interrupt sustainability of business processes. SMBs keep up with this deplorable

trend as more than half of them from time to time cause services to stop.

- The overwhelming majority, 83% of organizations, claim they never made a change that was a root cause of a security breach. However, given that only half of them have auditing processes in place, we assume that companies remain in the dark about what is going on across their IT infrastructures and are not able to detect a security violation or find the root cause of incidents.
- Due to established change management controls, more thorough documentation and automated auditing processes, enterprises are far more successful in security breach discovery than their SMB counterparts. The number of large companies that managed to find the changes that were a root cause of security incidents has doubled since 2014.

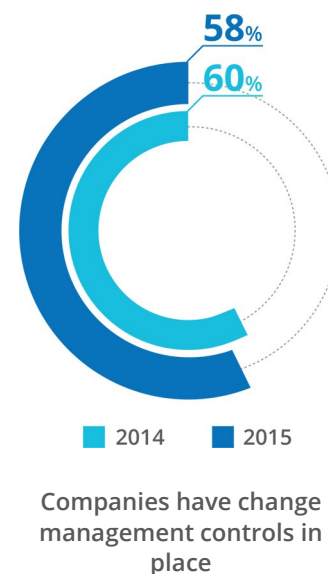
Survey Responses

Change Management and Documentation

Overall Overview

We have decided to find out how organizations in the whole deal with changes across their IT infrastructures. Having surveyed over 700 organizations, we found that on average 58% of them claimed to have some kind of change management controls in place, which is almost the same result as in 2014.

Still, 58% is a narrow majority compared to the relatively large 42% of organizations that haven't established any effective workflow or implemented any system to control changes made across their IT infrastructures.



However, establishing controls that help manage changes is only half of the job. The other half is to ensure the possibility to trace those changes for future reference, e.g., root cause analysis or internal audit procedures.

Being able to prove that no activity goes unnoticed across the infrastructure is a key element when meeting compliance standards or satisfying internal security policies. So it's not surprising that the overwhelming majority of organizations aim to achieve visibility across their IT infrastructures and make some effort to document

The survey results showed that the need to have all changes documented remains unchanged throughout the year, and has even increased in 2015

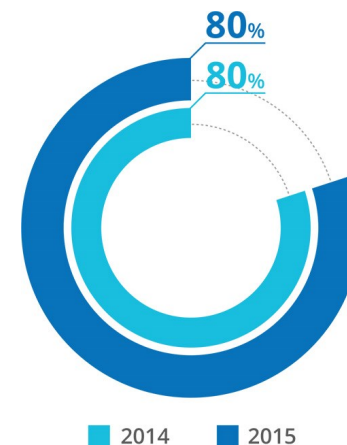
changes they make, with an average of 80% of organizations, which is the exact same ratio as in 2014, meaning that the need to have all changes documented remains unchanged throughout the year.

We also have decided to dig more deeply into the data and find out how many organizations try to document changes despite having no change-management controls in place.

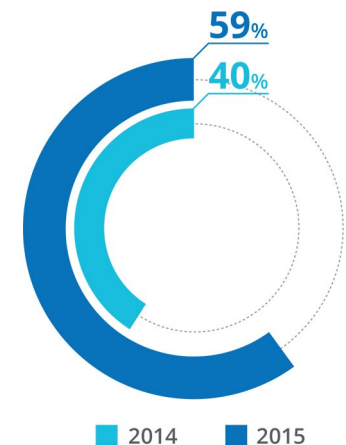
We found out that their number has increased by half throughout the year. Compared with the previous results, it's obvious that the question of visibility into IT changes is still relevant. Organizations, even if they don't have instruments to manage changes, still try to keep records and make some efforts to

document all changes they make. However, on average, 40% of organizations, no matter their size, are out of control and lack visibility into their IT infrastructures. They neither establish change management controls nor

document changes made. The majority of them expose themselves to danger of going through a hard time when they need to find a root cause of a security violation or system downtime.



Companies try to document changes



Companies that don't have change management controls still document changes

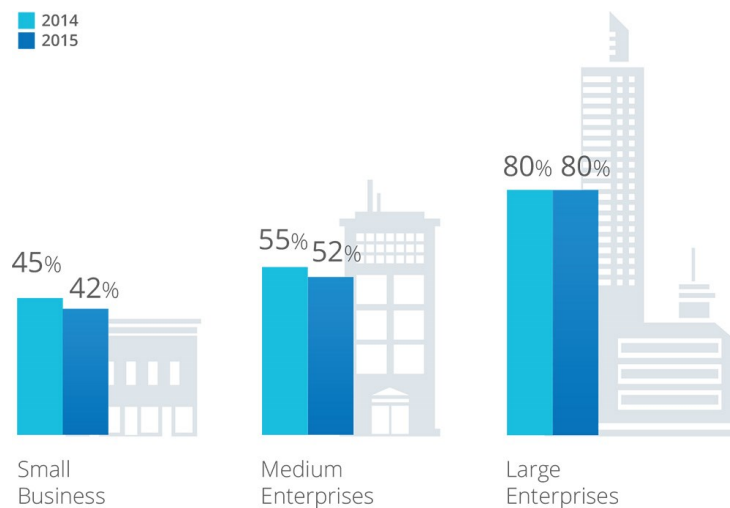
Organization Overview

If we divide organizations based on their size and compare with the previous year, the situation will be rather predictable. Small businesses remain the least concerned about changes made across their IT infrastructures, which means that the majority of small companies still refrain from

investing in change management controls. Large enterprises, on the contrary, are more likely to establish change management mechanisms for better visibility and more advanced control over changes made to business critical systems. Since security violation, internal or external audit failure or

interrupted business continuity might cost enterprises a fortune, they tend to monitor changes across their IT infrastructures more thoroughly than their SMB counterparts.

When it comes to documenting changes, we won't see any huge shifts in establishing this as a regular process for organizations of various sizes in 2015 compared to the previous year. Small companies still leave the changes undocumented more often than the others, but not as much as it might have seemed at first sight.

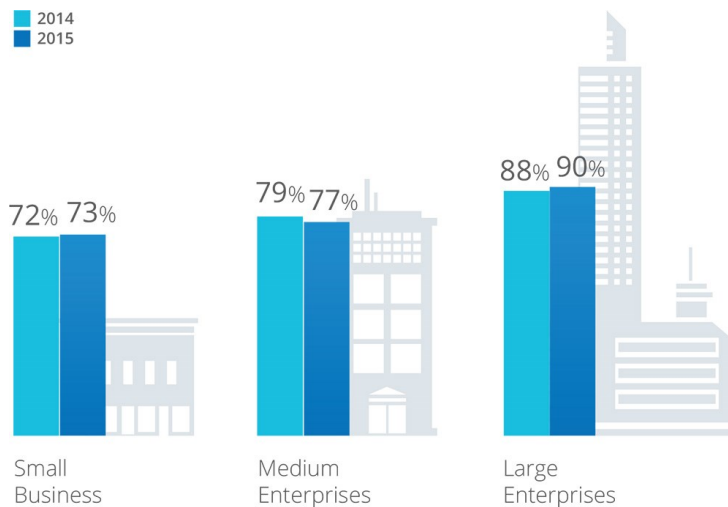


Companies have change management controls in place

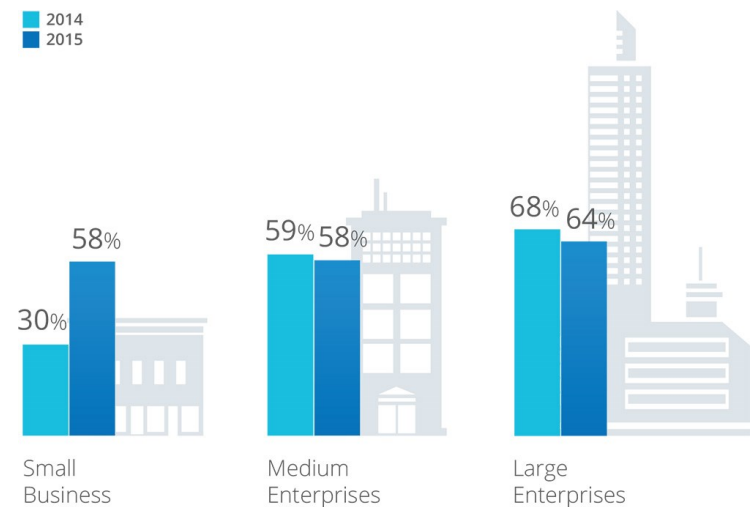
Given that not many small businesses have implemented change management controls, the majority of them tend to document changes by and large, while large enterprises, as expected, occupy the leading position. Having deployed change management controls in 80% of cases, enterprises also demonstrate the nearly widespread use of change

documentation processes for better visibility across their IT systems to help them in their efforts to cope with rapid workflow, an excessive number of personnel and the need to ensure business continuity. This year small companies have demonstrated a bold interest in tracking down changes and became more responsible and attentive to tracing

users' activity. Compared to the previous year, the number of small businesses that have started to document changes, despite the lack of change management controls in place, has doubled throughout the year and reached 58%, which is the exact same ratio as midsize enterprises and pretty close to the results of the enterprises.



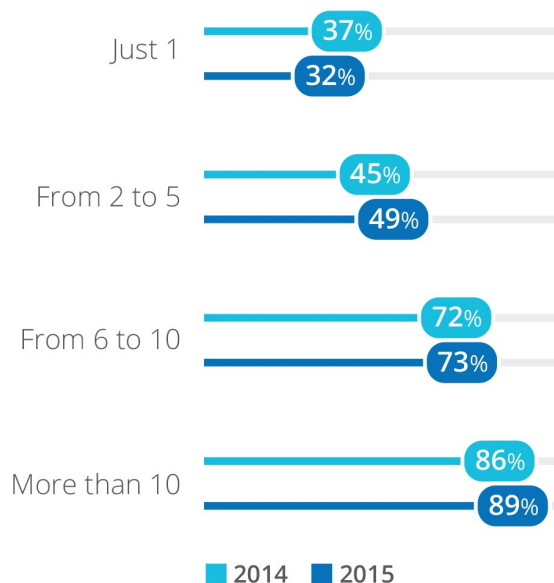
Companies document changes when they are made



Companies don't have change management controls in place but still document changes

IT Team Overview

Digging even more deeply into the data and comparing companies by the size of their IT departments rather than organization size, we have discovered that companies with more than 10 employees in the



IT teams have change management controls in place

IT department tend to have change management controls in place in the overwhelming majority of cases. On the contrary, only a third of tiny IT departments consisting of just one employee have established change management mechanisms in place. If we compare the results of 2014 and 2015, we see that the interest in such processes hasn't dramatically changed throughout the year for IT departments of various sizes. While tiny IT departments show a slight decrease in adopting change management controls in comparison to the previous year, this result is within the statistical error, and we suggest that it should not be considered a significant finding.

Further surveying the IT professionals, we have asked them whether they document changes. The diagram shows that the more co-workers IT pros have in the IT department, the more likely they are to document changes they have made. Large IT departments with more than 10 employees tend to document changes in the overwhelming majority of cases in order to keep IT staff informed about what is going on. Smaller IT organizations of up to 5 IT pros in 2015 became more careful when implementing any changes across IT infrastructure without documentation, demonstrating the need to achieve visibility.

IT Team Overview

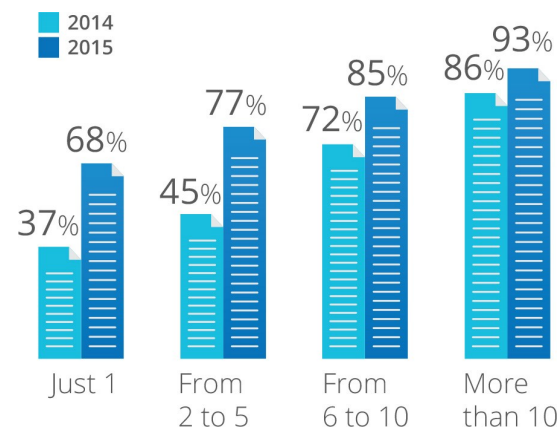
The trend for 2015 for IT pros is to document a change made, no matter how many IT pros work with you

The number of IT organizations consisting of one person that have started to document changes since 2014 has increased by almost a third of the total. The same increase of 32% is demonstrated by IT departments with up to 5 employees. The total overview shows that in comparison to the previous year, IT organizations of all sizes became very careful when implementing any changes across

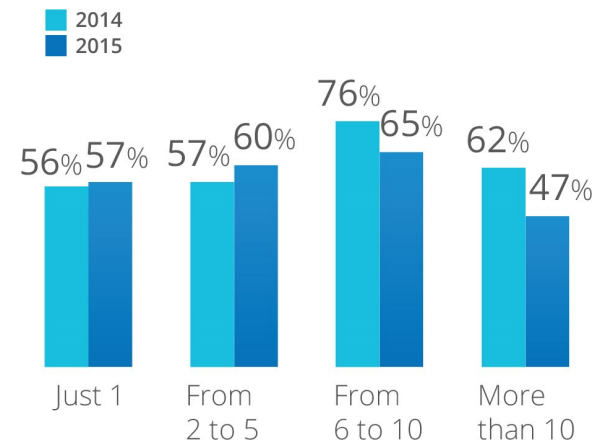
their IT infrastructures without documentation. The trend for 2015 is to document a change you made, no matter how many IT pros work with you.

When we asked IT pros who stated they don't have any change management controls in place whether they try to document changes anyway, interesting numbers were revealed. In most

cases IT departments of 6 to 10 people make some effort to document changes they make, but when the number of employees exceeds 10, IT professionals forget about documentation immediately. In both cases, the results of 2014 are much worse compared both to the results of 2015 and the results of smaller IT teams, providing us with more proof that too many cooks spoil the broth.



IT teams of various sizes document changes



IT teams that don't have change management controls still document changes

Change Auditing

Adopting change management controls as well as documenting the changes is only a first step toward achieving complete visibility across the entire IT infrastructure. If it is done thoroughly, it provides a unique source of data not only for root cause analysis, but also for

proving that internal security policies in place are actually working. However, without established audit processes, these data remain an excessive and uninformative list of events that is hardly helpful when investigating a security violation or system downtime, or providing a rigorous

auditor with a detailed report. We wanted to find out whether companies are able to benefit from documenting changes by using IT auditing and what methods they use to understand who does what, when and where across all IT systems.

Overall Overview

Back in 2014, the gap between those who used some kind of change auditing process and those who didn't was huge. More than 60% of respondents claimed that they had little or no real ability to audit changes they

made. However, in 2015 the situation changed dramatically, as 48% stated they don't have any mechanisms to monitor changes across their IT infrastructures. Comparing the survey results with the previous year, it is obvious

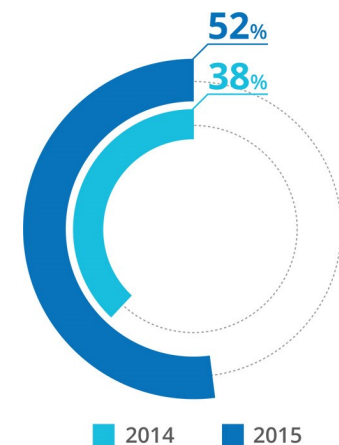
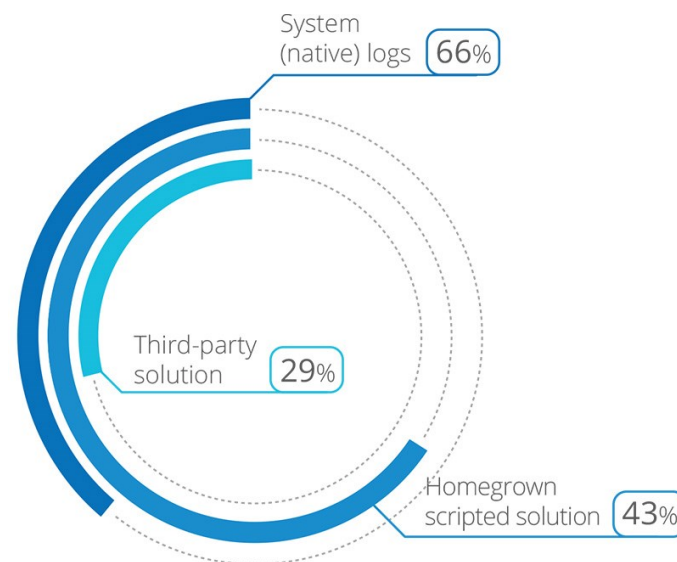
that organizations started to take IT auditing more seriously and made more efforts to establish change auditing controls to monitor IT infrastructures than they did only a year ago.

Organizations started to take IT auditing more seriously and made more efforts to establish change auditing controls to monitor IT infrastructures than they did only a year ago

Delivering visibility into who changed what, when and where across all IT systems with the help of auditing is a versatile task that can be performed in different ways. We have decided to investigate which methods are the most popular among organizations and IT teams.

Native system logs remain the most common source of information for tracking changes made across the IT infrastructure. System log monitoring doesn't require huge investments in software or hardware, but it is very labor-intensive and time-consuming engagement, while remaining the

least efficient of all. Because changes are tracked manually audited data can easily become a victim of human error or even malicious intent. This makes automated auditing solutions a better option as a reliable and impartial source of information.



Companies have established change auditing processes

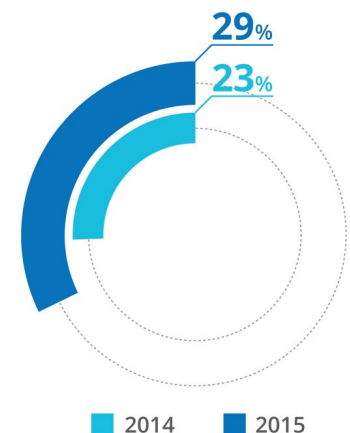
Among them, homegrown scripted solutions are favored the most, leaving third-party auditing solutions behind. Organizations prefer to invest in developing their own scripted software to do the job to achieve optimum system performance by better integrating with business critical systems and existing business processes. However, this option will require large financial investments in both software and hardware, as well as specially trained staff who will be able to support the solution.

Third-party solutions that audit all IT changes automatically are deployed by a 29% of the companies, whereas in 2014 only 23% of surveyed organizations stated they had either an audit process or a specialized auditing solution in place to validate that all changes are authorized. Third-party solutions provide organizations with a turnkey product that on the one hand has all the benefits of

automated auditing and on the other hand removes the burden of having to invest in software development, technical support and staff training. The main benefit for third-party solution is a possibility to deploy it right out of the box and its ease of use. However, the number of those who have decided to purchase automated IT auditing from a third-party vendor hasn't drastically increased throughout the year.

Having asked respondents to choose one or several options of the preferable methods of IT auditing, we see that the overall sum of the percentage exceeds 100. This allows us to say that despite the fact that all three methods are very different, the need for better visibility forces organizations to choose more than one option when establishing control over changes across the network.

The demand to implement change auditing mechanisms varies depending both on the size of organizations and the size of their IT teams. We decided to compare how enterprises and IT departments of various sizes attribute to IT auditing.



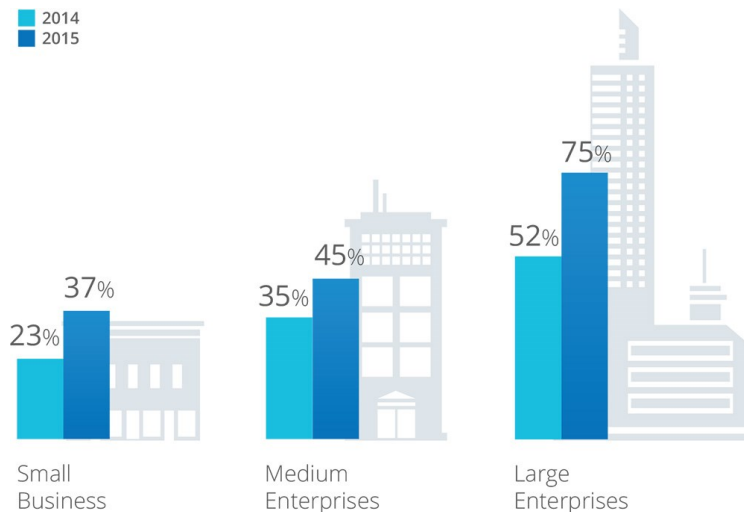
Companies have third-party auditing solution in place

Organization Overview

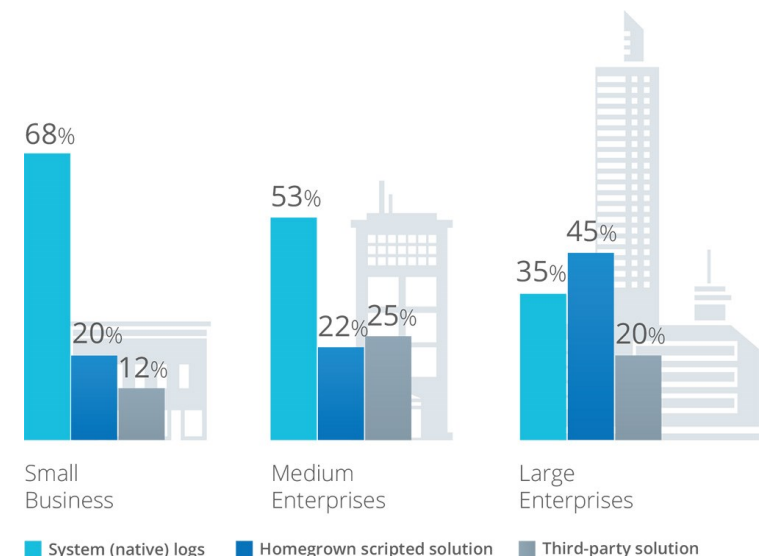
Quite expectedly, due to larger IT infrastructures, enterprises demonstrate much more interest in auditing than SMBs. According to the results of the survey, small and midsize companies still struggle to implement IT auditing across-the-board, as less than half of them have implemented change auditing controls. However, this technology continues to capture the SMB

market with quite a noticeable increase in demand for this solution in 2015. Large enterprises started to invest more in IT auditing processes than a year ago, demonstrating a significant 75% of those who already have implemented some sort of change auditing mechanisms in place, compared to a little bit more than half of the enterprises in 2014.

When it comes to choosing methods of IT auditing, quite naturally searching through event logs, permissions and system settings can be named the most common for small and medium-sized companies due to limited financial resources, or perhaps the secondary role of IT security among their business goals.



Companies audit changes



Companies prefer various methods to audit changes

However, since they have only a limited number of employees in their IT departments, time spent in digging through countless native logs influences the workload and adds additional responsibilities to IT professionals, still putting companies' security at risk.

Large enterprises, on the contrary, tend to opt for homegrown scripted solutions, which is also quite understandable. The need to increase visibility and optimize staff and system performance forces enterprises to develop customized solutions that are fully integrated

into their IT infrastructures. However, more than a third of them are still busy analyzing system logs, leaving IT pros flooded with numerous changes and the risk of overlooking malicious activity that may compromise overall cyber security.

IT Team Overview

Quite expectedly, IT auditing is a more common activity for larger IT departments with more than 10 people on staff who need to be aware of all the changes their co-workers make. About 80% of large IT teams make some effort to audit changes, whereas only a third of the smallest IT departments consisting of one employee do the

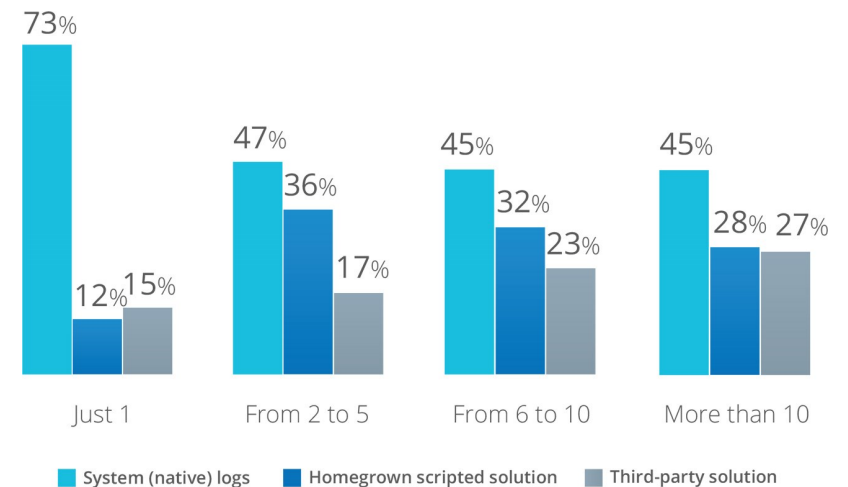
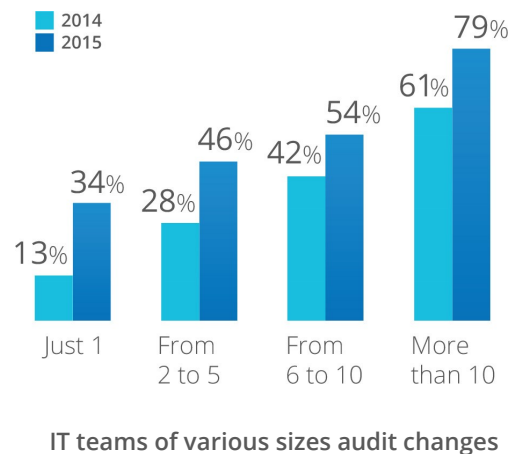
same. However, if we compare the results with 2014, we will notice that even small IT departments nowadays try to use change auditing processes to understand what's going on in their IT infrastructures. The number of IT pros using change auditing and being responsible for the entire IT infrastructure on their own has

almost tripled over the year. The trend for 2015 is a gradual spread of change auditing mechanisms across IT teams of various sizes; however, the biggest increase is spotted among small and mid-sized departments that have just started to be drawn to this technology.

If we look closer and compare the choice of IT auditing methods depending on the size of the IT organization, we will notice that in the overwhelming majority of cases organizations with only one IT pro on board tend to use system log monitoring as it is the cheapest way

to complete this task. However, IT teams with more personnel in the majority of cases choose native log monitoring as well. While they can afford to allocate staff for this job without any harm to established workflow (even with a risk of missing malicious activity),

organizations with only one IT professional can find serious gaps in cyber security and the IT pro buried under vast amounts of data trying to tie everything up together.



Hidden Threats

The survey has showed that organizations regardless of size try to get visibility into what is going on across their networks. But why do they need that? Is IT

auditing implemented just out of curiosity, or to establish strict control over the employees' actions, or only as a part of compliance checklist? We have

decided to find out what risks arise when changes are not documented and what impact it has on the business processes on the whole.

Overall Overview

The notion that every single change made is thoroughly documented by every employee is utopic. We are all human beings who can become overwhelmed by duties and simply forget to make an appropriate note. Despite

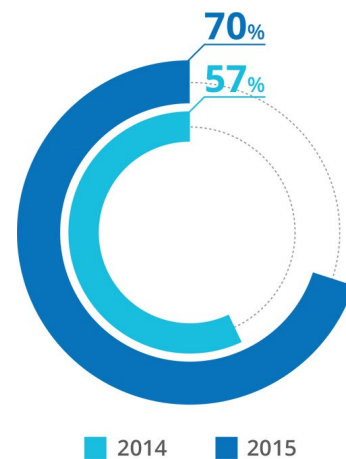
claiming they document changes, the majority of organizations from time to time still forgets about it. If in the previous year 57% of organizations stated that they from time to time don't document changes made, 2015 showed

quite a significant increase of forgetful staff and demonstrated 70% of those who occasionally skip documenting changes they made.

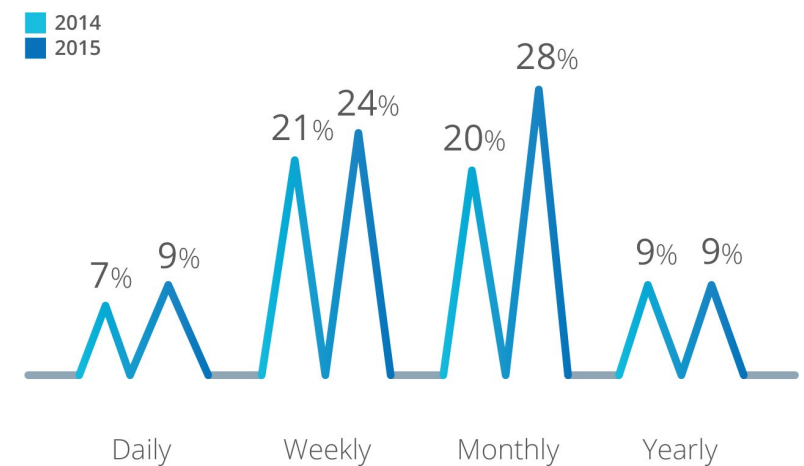
We went further and decided to find out how frequently organizations make changes without letting anyone know. The results showed that almost a third of undocumented changes are made every month and a quarter of

them every week, meaning that organizations lose visibility across their IT infrastructures quite often. This may result not only in failure to successfully pass compliance validation and receive a list of recommendations to fix the

problems, but also in more serious consequences such as insider misuse or an external hacking attack followed by sensitive data loss.



Employees make changes without documenting



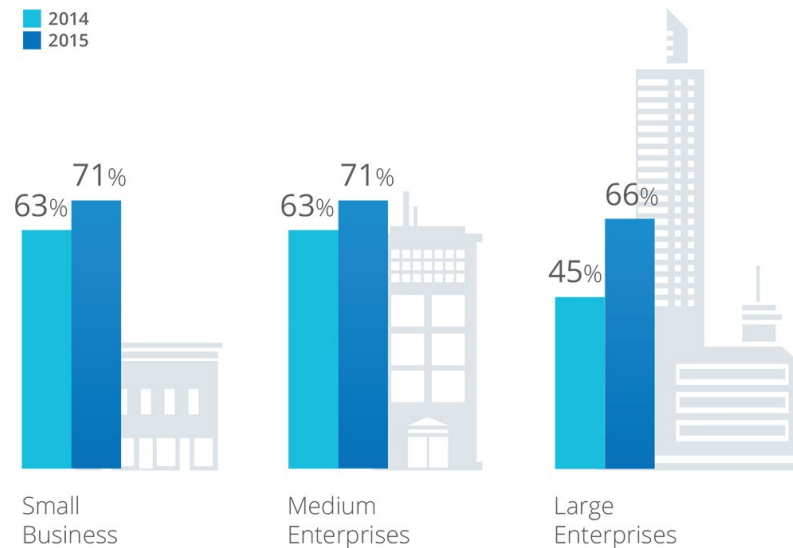
Frequency of making changes without letting anyone know

Organization Overview

Small and medium-sized businesses make undocumented changes more often than large enterprises, which can be explained by stronger security controls and established workflows in the large

companies. However, the results for enterprises are disappointing. If compared with the results of the previous year, the number of large businesses that forget to document changes has increased by more

than 20%. Of course SMBs also became more lax toward documenting for the year, but their results are not even nearly as bad as those of enterprises.



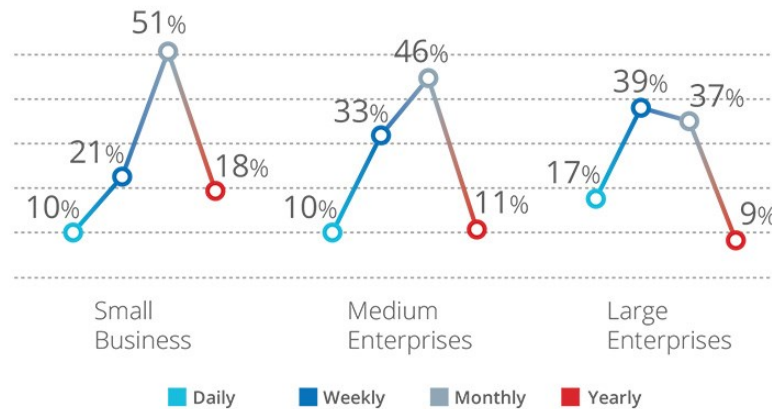
Companies of various sizes make undocumented changes

Continuing the trend, enterprises turned out to be the worst offenders when it comes to frequency of making undocumented changes. Almost

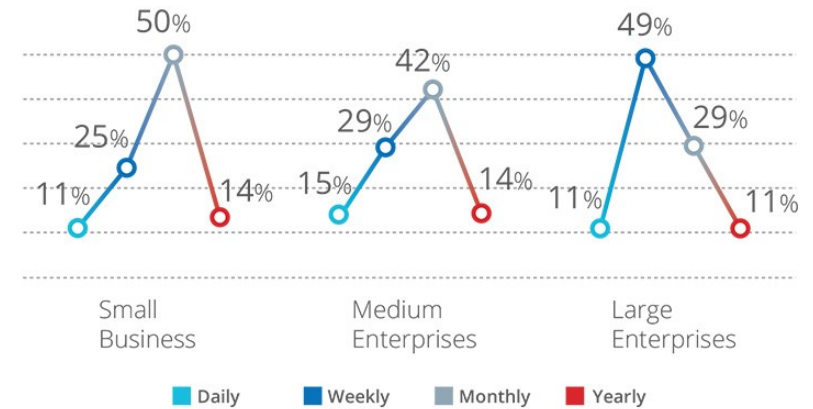
half of changes made by enterprises without letting anyone know is made every week, whereas SMBs in most cases break the rules every month. Compared to the

results of the previous year, enterprises became more irresponsible and failed to document weekly changes more often.

2014



2015



Frequency with which companies are making changes without documentation

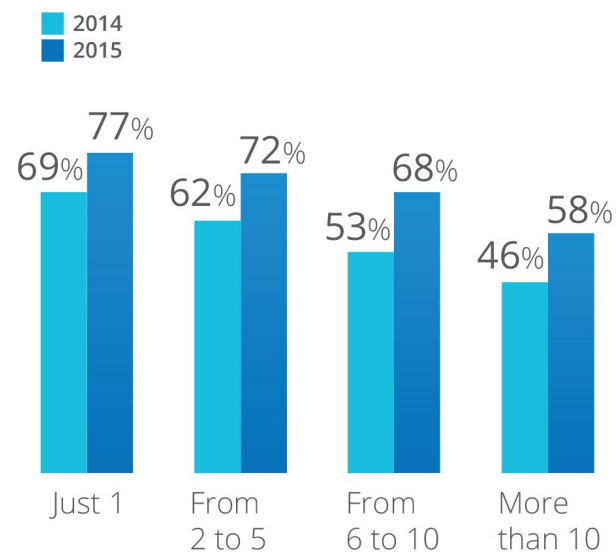
IT Team Overview

Having compared organizations by the size of their IT teams, we found that the fewer the number of employees, the more often they make changes without letting anyone know. IT teams with only

one professional on board in 77% of cases skip this step and assumes to remember everything done, whereas IT teams with more than 10 professionals employed do the same 20% less often. However, it

turned out that all IT teams no matter their size proved to be more irresponsible and failed to document more changes than a year ago.

The larger the department, the more likely it will put cyber security at risk

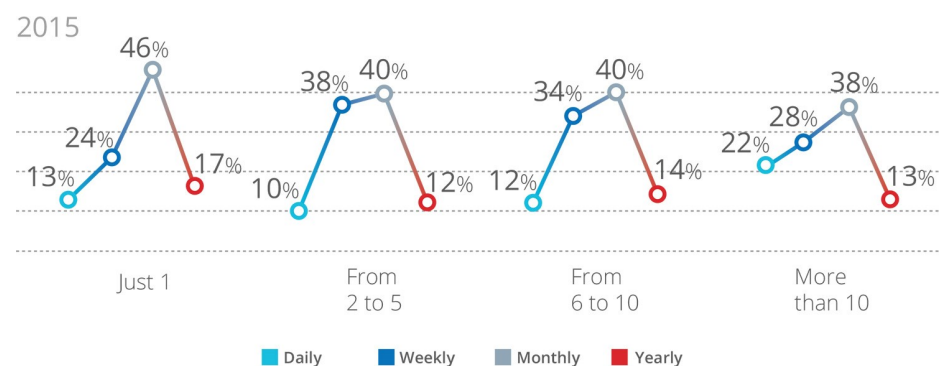
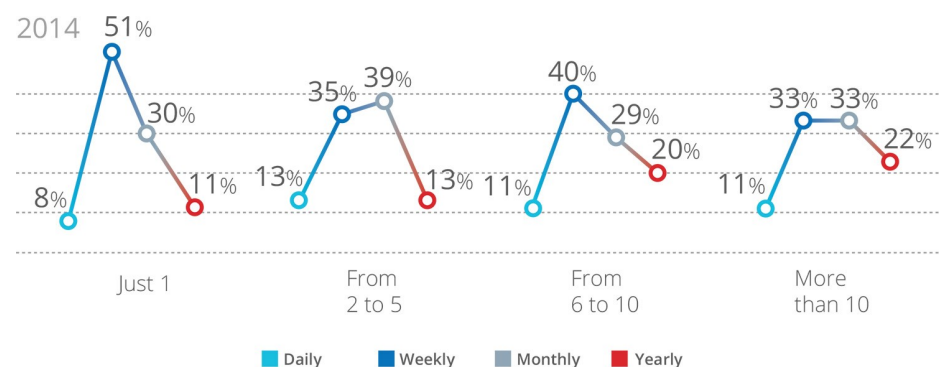


IT teams of various sizes make undocumented changes

IT Team Overview

When it comes to the frequency of undocumented changes, half of small IT teams of only one employee claimed to make undocumented changes every month.

However, the survey revealed that the larger the department, the more likely it will put cyber security at risk. If we look at the results, it becomes obvious that 22% of IT teams consisting of more than 10 IT pros forgot to document changes that are made every day, which is almost twice as much compared to the average results of smaller IT departments as well as to the results of the previous year.



Frequency with which IT teams make undocumented changes

Security vs. System Uptime

We have already found that establishing change management processes along with regular documentation of the changes aren't able to eliminate serious gaps in security. Since not every change is documented, organizations put themselves at

risk of overlooking abnormal activity of user accounts or unauthorized changes to system configurations. The loss of visibility into what is going on across the entire IT infrastructure may cost companies a fortune, especially if it results in serious data breach or

long-period system downtime. We have decided to ask IT pros whether they have ever made changes that could potentially compromise security or interrupt business continuity, and if so, how often it usually happens.

Overall Overview

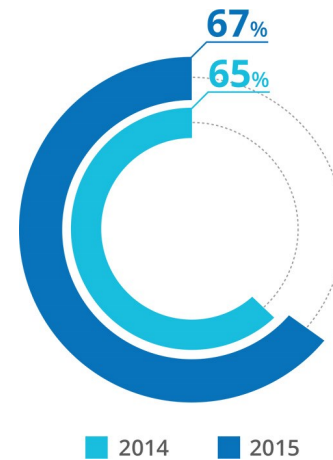
Incorrect or unauthorized changes to system configurations can impact sustainability of business processes and cause IT services to stop. The majority of IT

pros admit that they still are not able to control sustainable performance of their IT systems and continue to make changes that were a root cause of system

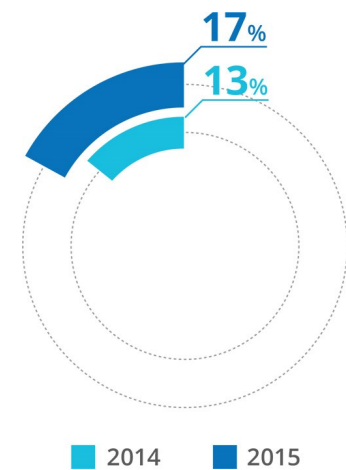
downtime; the share has even increased throughout the year.

However, when it comes to cyber security, organizations tend to be either much more conscious and try not to make changes that can cause a security breach or experience difficulties in discovering violations. In 2015, the overwhelming majority of IT pros continue to claim that they have never made a change that compromised security.

This is an interesting finding that demonstrates that organizations have more visibility into operations rather than security issues. Although they both affect the effectiveness of the enterprise performance, and ultimately the amount of profit, IT pros are more likely to notice failure of system performance rather than spot data leak.



Companies make changes that caused services to stop



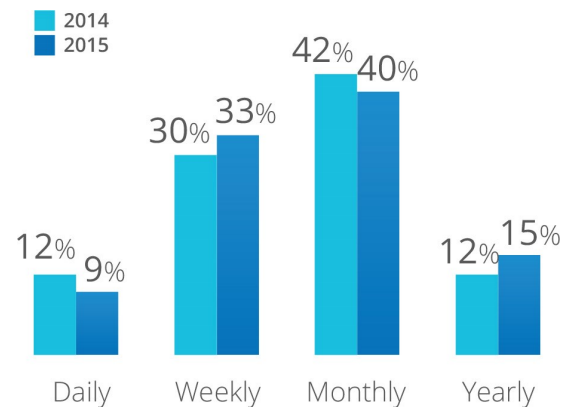
Companies make changes that caused security breach

However, when it comes to the frequency of such changes, organizations demonstrate the same ratio. 40% of organizations

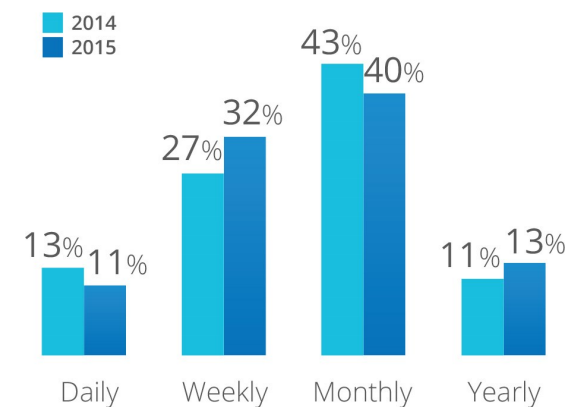
make changes that both degrade service performance and security every month, and a third of organizations are at risk every

week. In comparison to the previous year, weekly changes started to impact organizations more often.

40% of organizations make changes that both degrade service performance and security every month, and a third of organizations are at risk every week



Frequency with which organizations made changes that caused services to stop



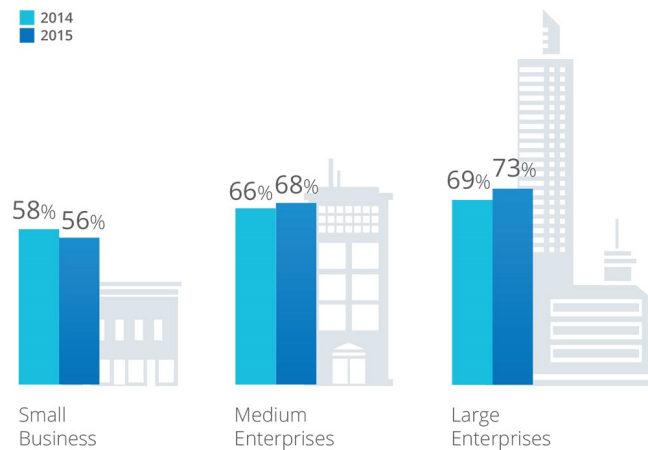
Frequency with which organizations made changes that caused security breach

Organization Overview

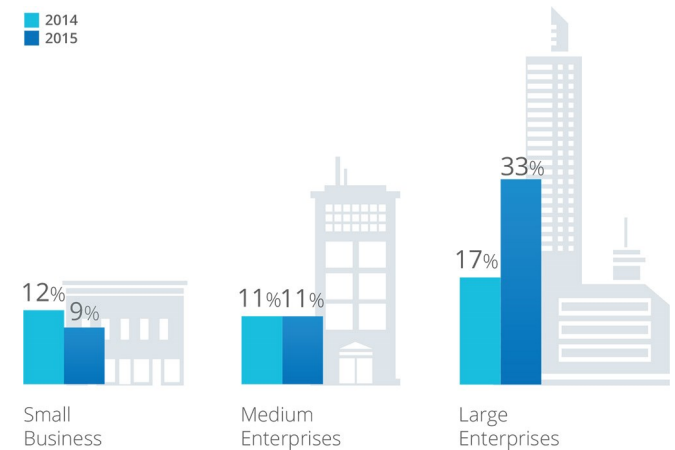
Despite the increased focus on internal management controls among organizations, they continue to fail the mission of ensuring business continuity, and the larger the enterprise, the more likely it will be exposed to system downtimes. 73% of large companies encounter

service downtime, which can result in costly production downtime and interruption of established business processes. Given the fact that more than half of enterprises from time to time fail to document changes, IT organizations are likely to have a hard time wading through

calls of furious users trying to find out what was a root cause of this incident. SMBs continue to keep up with their larger peers as the performance of the majority of them is affected by accidental or unauthorized changes.



Companies of various sizes made changes that caused system downtime

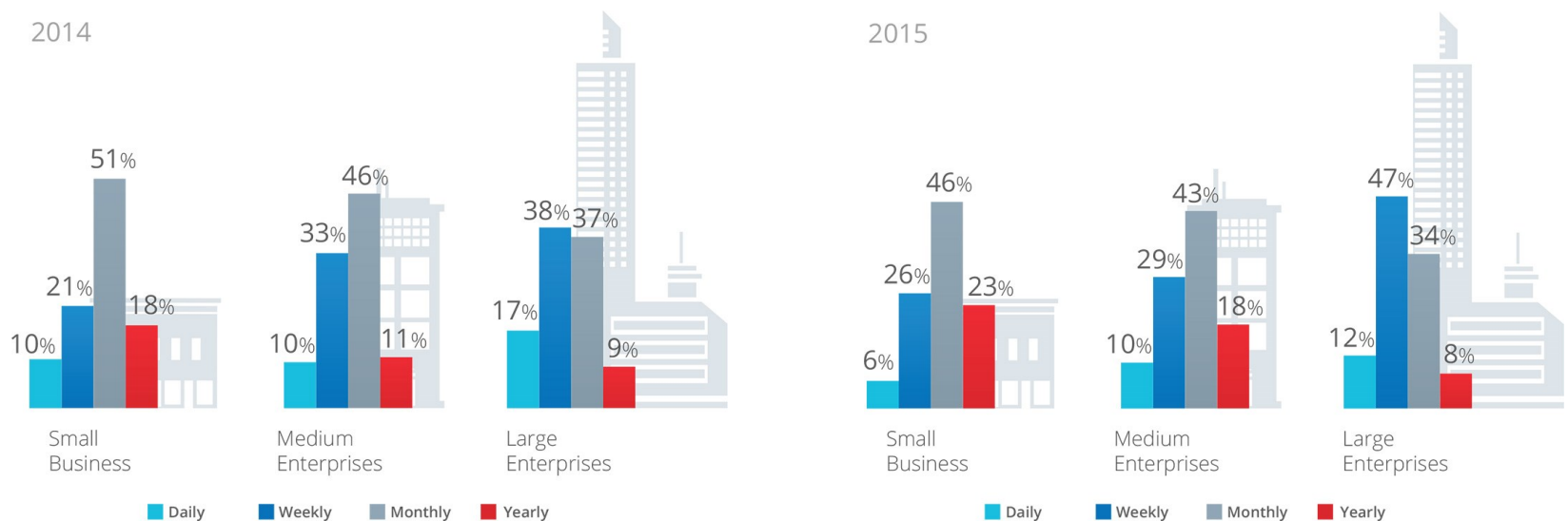


Companies of various sizes made changes that caused security breach

Looking at the chart, we could conclude that small and medium-sized companies have fewer security issues than enterprises. But this is only at first glance. Given that here we speak only about revealed security incidents, we can assume that SMBs may not even

know that they have been compromised. Enterprises, on the contrary, more often discover security incidents. The number of large organizations that managed to find a change that was a root cause of a security incident doubled since 2014. This is

absolutely logical given that more enterprises audit changes than their SMB counterparts, and if they do, SMBs still don't have automated auditing solutions in place and are satisfied only by the results of manual native log overview.

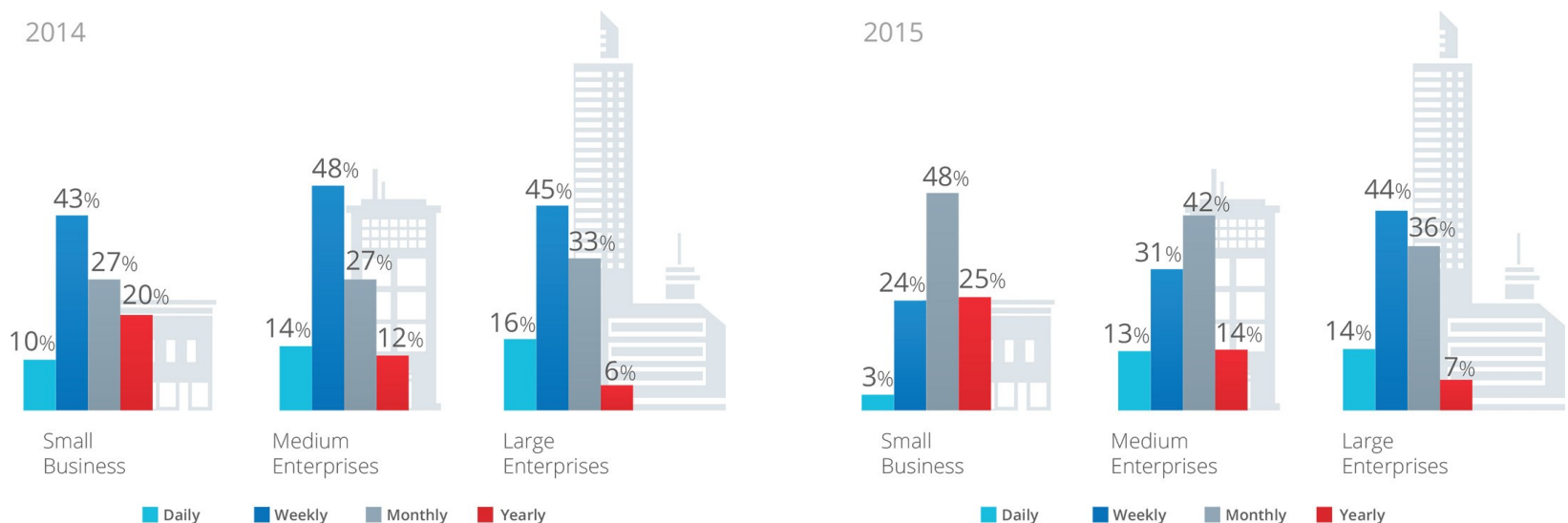


Frequency with which companies of various sizes made changes that impact performance or service uptime

When it comes to the frequency of changes impacting system uptime, small and medium-sized companies tend to affect the organizations' business continuity every month with an average of 45% with more than a quarter of changes that are made every week. However, if we compare this data with that of the enterprises, we will see that large companies due to the superior number of users put their business

continuity at risk more often. 45% of changes that caused services to stop are made every week, and the rest, one third, are made every month. Moreover, 56% of changes made by IT pros in enterprises daily or weekly impact enterprise operations' stability, resulting in system downtime and interruption of business continuity. From time to time, organizations still have to make critical changes that if done

incorrectly may result in security violations and sensitive data leaks. SMBs are mostly affected by changes that may impact security every month, whereas 44% of large enterprises due to their more intensive workload are in danger of compromising their internal security policies every week, with more than a third of them jeopardizing security every month.



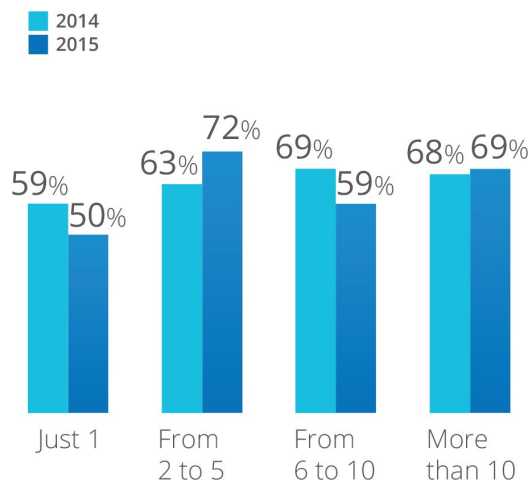
Frequency with which companies of various sizes made changes that impact security

IT Team Overview

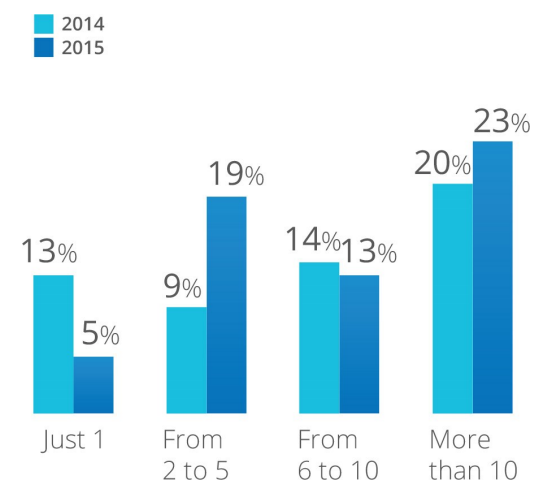
Taking a closer look at the IT teams, we can conclude that despite the size, all IT departments can be influenced by incorrect or unauthorized changes made to sensitive data and system configurations. The number of IT pros that claimed they have made changes causing services to stop exceeds the number of those whose changes caused security

incidents. However, while in the case of system downtime you can easily spot the problem, when it comes to security breaches, you may not even notice malicious activity that resulted in sensitive data theft. Of course, big IT teams (that are more common for large enterprises) have instruments to track the misbehavior as they have resources to invest more in security

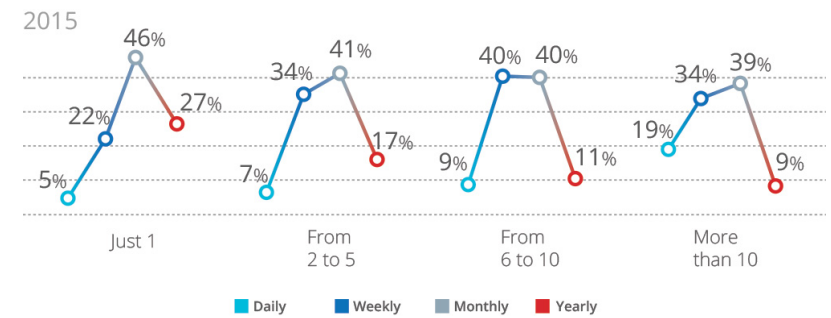
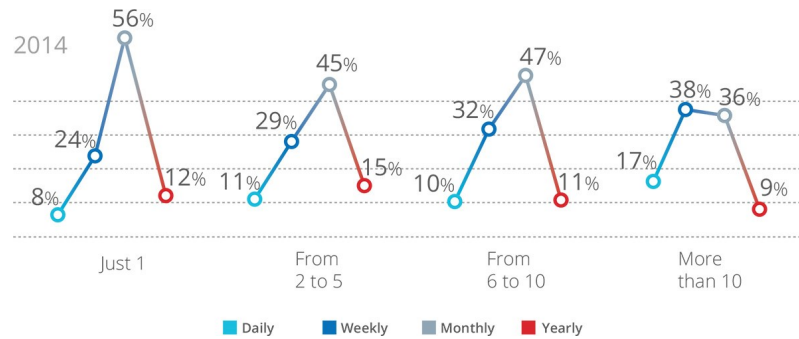
mechanisms, change management systems and IT auditing. On the other hand, small IT departments in most cases have tight budgets and, despite showing the best results security-wise, remain in the dark, automatically assuming that if they don't know about the misuse, there is no misuse.



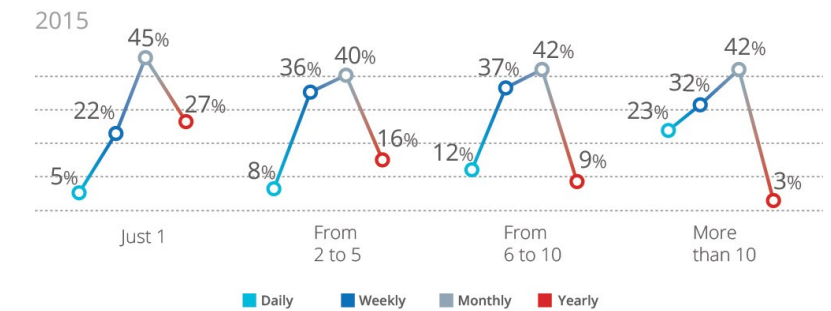
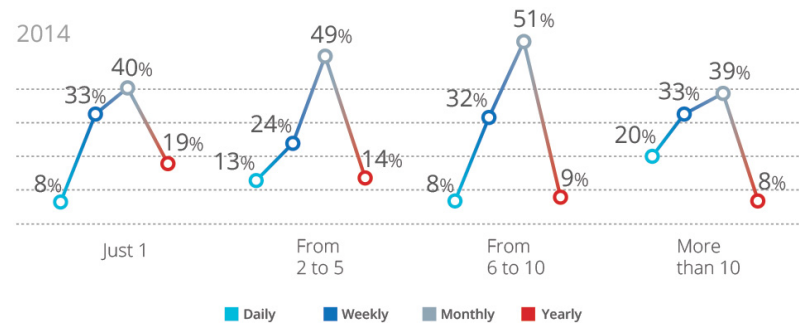
IT teams of various sizes made changes that caused system downtime



IT teams of various sizes made changes that caused security breach



Frequency with which IT teams of various sizes made changes that impacted service uptime



Frequency with which IT teams of various sizes made changes that impacted security

Conclusions and Recommendations

1. Control and document changes into IT systems

Organizations should be aware of what is going on in their IT infrastructures, as a minor change may result in system downtime or violation of security policies. Establishing effective change management controls helps organizations to be proactively prepared to determine the cause of the problem and fix it as fast as possible, eliminating risks of interrupting business continuity. However, just tracking changes is not enough for establishing complete visibility over IT infrastructure. Another significant step is upgrading manual

processes of change documentation to automated ones. Security, as well as continuous performance of all IT systems, is always about the people, and since the share of IT pros that forget to document what modifications they made is growing, solutions that track down changes automatically can provide a reliable data source to facilitate further root cause analysis.

2. Enable auditing

When it comes to auditing changes, the key factor is thoroughness and sustainability of the process. Organizations should control and audit changes on a

regular basis in order to achieve a visibility of what is going on and, as a result, long-term peace of mind that established security policies are working. Although constant verification for errors and malicious changes helps to strengthen security of critical IT systems, it might become a time-consuming and costly practice if it is done manually. Therefore, it is highly recommended for companies of all sizes, especially SMBs, to replace manual auditing processes with faster and more cost-effective automated methods. This will help to minimize risks of missed malicious activity and therefore ensure data security, streamline compliance and optimize operations.

3. SMBs should learn from Enterprises

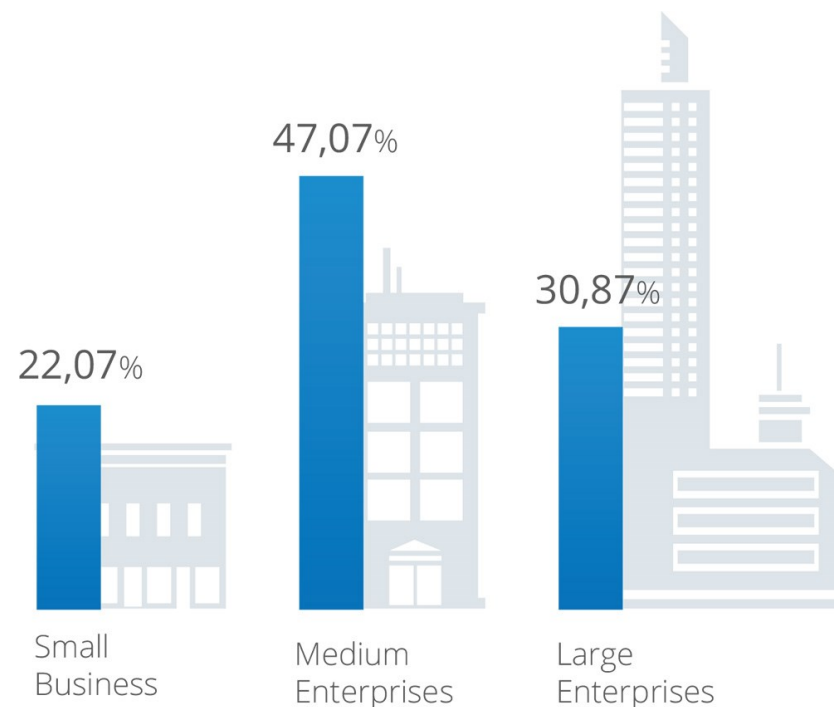
As the survey revealed, enterprises showed that they are more protected against malicious activities due to established automated change management

and IT auditing controls. Regular auditing procedures integrated into the framework help companies to identify threats addressed to the network and reduce security risks for sensitive data. Regular monitoring of business critical IT systems is the most simple and

effective way to protect internal assets by reporting on malicious activity. After all, in an age of hacks and insider jobs, it is much better to prevent a data breach at an early stage than fight the devastating consequences of a full-force cyberattack.

Respondent Demographics

Organization size



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

The majority of IT pros who took part in the survey work for midsize companies, about a third of respondents work for large enterprises, and less than a quarter represent small business.

*Based on [Gartner's definition of small and midsize business \(SMBs\)](#) by the number of employees.

Industry Vertical

This year we managed to include more than 40 different industries in the survey, which is almost two times more than last year.

The majority of IT pros represent IT and Technology, Manufacturing, Education, Construction and Engineering, Health Care, Banking

and Finance, Government and Non-Profit Organizations.

Top 8 industries represented in the survey



18%
Technology



9%
Manufacturing



9%
Education



9%
Construction



8%
Health Care



7%
Banking



7%
Government



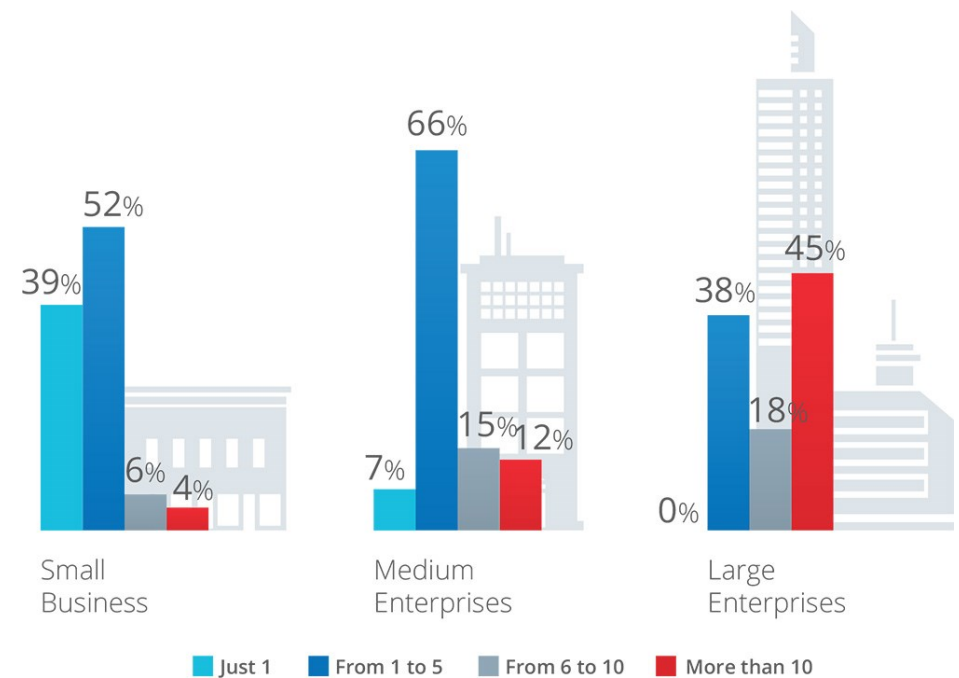
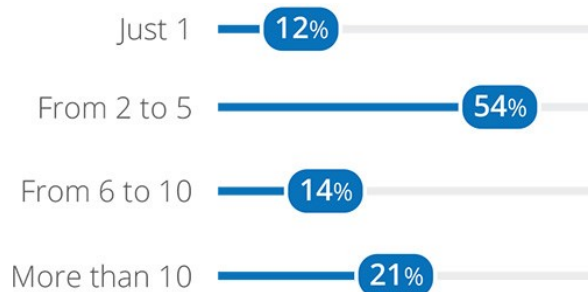
4%
Non-Profit
Organizations

IT Team Size

The number of IT staff varies depending on the organization size. In most cases, large enterprises hire more than 10 IT pros to support their IT infrastructure.

Midsize and small companies don't go beyond 5 employees in their IT departments to fulfil everyday duties in supporting the entire IT ecosystem. Interestingly enough,

the number of IT personnel varying between 2 and 5 people is recognized as the most common for all companies, regardless of size.



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



Corporate Headquarters:

300 Spectrum Center Drive, Suite 820, Irvine, CA 92618

Phone: 1-949-407-5125

Toll-free: 888-638-9749

Int'l: 1-949-407-5125

EMEA: 44 (0) 203-318-0261



netwrix.com/social