How much can the wrong IT management cost?

The optimization of IT infrastructure management process brings about a number of business benefits. One of the most prominent of these is reducing both the ongoing and potential operating costs. How much can you benefit by implementing the right tools and policies in this area? How much can you lose through wrong IT management?

Network failure worth millions

An IDC survey[1] showed the average downtime resulting from failures in computer networks, systems and applications in mid-size companies and organizations was 11 hours per year. The costs of stoppage in the entities which were surveyed amounted to USD 10,000 per hour. Gartner analysts suggest[2] larger companies can lose even up to USD 300,000 per hour during IT infrastructure failures. The long unavailability of IT systems can result in multi-million losses, which was the case of Delta Airlines and Southwest Airlines[3] Co, for example. For many smaller companies, not backed up with robust budget provisions, such downtime may even lead to bankruptcy. British Chambers of Commerce reports that 93% of companies, which lost their data for more than 10 days as an effect of IT failure, disappeared from the market within a year after the incident.

How to minimize the risk?

Even the largest and best protected organizations must face the fact that there is no one-hundred percent protection against potential failures, as these may also be an effect of vis major, e.g. earthquake or hurricane. However, foreseeable threats, such as faulty equipment breaking down or even server room fires can, to a certain extent, be eliminated. The previously mentioned IDC survey states the consequent use of IT management software minimizes costly computer network and system failures by 65%. With tools to monitor the condition of the infrastructure, the network administrator can has access to knowledge about e.g. service statuses, the condition of hard disks, and – with additional sensors – also the temperature and humidity in the server room.

The weakest link in the security system

The proverbial natural perversity of inanimate objects is one of the sources of IT infrastructure failures and, therefore, an avoidable potential cost. Another one is the unauthorized actions of the employees. One of Gartner reports[4] reads that 80% of critical service stoppages is a result of unauthorized user activities. Employees are often responsible for strategic data leaks or the inadvertent introduction of viruses or spyware to the network. Sometimes education falls short, so the corporate security policy should provide for the preventive monitoring of the potentially harmful actions of the staff. The IT department should be also equipped with the right tools.

---

[1] https://www.mercurymagazines.com/pdf/IDC_RiskAssessment_WP_Final.pdf

[2] http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

[3] http://www.businessinsider.com/r-delta-says-flights-grounded-nationwide-after-system-outage-2016-8?IR=T

[4] https://img2.insight.com/graphics/no/info2/insight_art6.pdf

Software which reports suspicious user activities to the administrator perfectly complements security systems and antiviral programs. At the same time you need to remember that the purpose of the software is not invigilation, but to increase corporate protection against data leaks and external attacks. The software solution for IT management, supported by the user activity monitoring module, is the right choice when you want to protect your business against high financial losses resulting from the unauthorized actions of the employees

–emphasizes Marcin Matuszewski,
Senior Technical Support Engineer at Axence.

The implementation of employee activity monitoring tools does not only strengthen the network protection chain, but also increases the employees' productivity, which means a potentially higher profit can be generated within a specific timespan. For instance, an IT company employing 5,000 persons increased its yearly profit by USD 2 million[5] after the deployment of employee monitoring. Furthermore, since the staff was informed about the applied software, they spent, on average, 90 minutes more on their professional tasks. The very awareness of being monitored has the effect that they resign from spending time on private affairs whilst at work – regardless of the fact that the administrator is not following their every step, but is only informed about suspicious activities.

Costly licenses

Hardware and application failures or the risky behavior of the users are not the only incidents which can be potentially damaging for a company's finances or image. The improper management of licenses for utilized software also poses a high risk. Mass media often relate the cases of companies which have had to pay millions in penalties. An administrator equipped with the right software can quickly audit the used applications and can see which ones do not have a valid license. The collected knowledge will enable you to decide what licenses should be purchased and what software should be uninstalled.

An equally valuable element is the insight into the usage of specific licenses, which can be obtained with IT asset inventory software. It forms the basis for the administrator to decide which licenses are redundant, i.e. are paid for by the company, while the software remains unused. For instance, the US Government Accountability Office has identified, after an audit, that the proper management of software licenses may produce huge savings in the public sector. One of the prominent US federal agencies (its name was not disclosed) reported that only in 2012 it had saved USD 181 million[6] in that regard.

[5] http://www.bostonglobe.com/business/2016/02/18/firms-step-monitoring-employee-activities-work/2l5hoCjsEZWA0bp10BzPrN/story.html

[6] http://www.gao.gov/products/D07403

Smart management

Comprehensive network management allows the risk of costly stoppages and data leaks to be significantly reduced and penalties for the possession of illegal software to be avoided. This, in turn, means shorter downtimes and the increased productivity of expert employees which reduces the fixed costs. Data collected by survey institutes and the cases of companies and organizations from all over the world show that in order to improve profits on the balance sheet, it is worth considering the deployment of suitable tools for monitoring the network and its users, as well as for hardware and software inventory management. There are several all-in-one solutions in the market, which allow all of these issues to be addressed from the level of one console. What is more, they include mechanisms which automate some of the processes, enabling the person responsible for IT management to focus solely on the important alerts.

Wrong IT management **costs**

Every company loses **11 hours** on average each year due to downtime caused by IT system failures.

Source: IDC

One hour of downtime due to an IT system failure can cost as much as **USD 300K**.

Source: Gartner

93% of companies that lost their data due to an IT system failure went into liquidation within a year from the incident.

Source: The British Chambers of Commerce

80% of critical service outages are caused by unauthorized user activities.

Source: Gartner

Benefits yielded by IT management software implementation

The implementation of IT management software can minimize infrastructure failures by **65%**.

Source: IDC

By installing employee activity monitoring software, an IT company employing 5,000 people increased its annual profits by **USD 2 million**.

Source: Boston Globe

Following the deployment of staff activity monitoring software, the time employees spend performing job-related tasks has increased by **90 minutes a day** on average.

Source: Boston Globe

One of the major US federal agencies reported that in 2012 only made **USD181million** of savings by establishing a software licence inventory.

Source: Government Accountability Office

In our conversations, the administrators often emphasize that, for them, managing the infrastructure with one comprehensive tool is much easier and faster, as they do not need to become accustomed to different systems and then to keep switching between them. This is especially significant in the case of large networks consisting of a few hundred workstations. It is another argument for the deployment of an all-in-one tool, which will enable the administrator to save time and focus on other, more important aspects of the job

– adds Marcin Matuszewski from Axence.