ANALYSIS OF INTERNAL SECURITY

Anonymous Company

This document presents outcomes of internal security audit performed in an anonymous company by means of Safetica. The analysis was carried out on 46 working stations in time period of May 1, 2016 - May 31, 2016. The data refer to the company's working hours (9:00 a.m. to 5:00 p.m.). A XLS document with complete set of monitored data is avalailable too and can be used for further processing.

safetica®

CONTENT

DATA HANDLING

E-mails

L. Baker sent file *project.dwg* to e-mail address of competition *m.wilburn@competitivefirm.com*.

In this part we analysed files being sent via e-mail clients. Following the customer's demand, we focused on protection of company's know-how, which is mainly comprised of CAD software files.

In total 31 e-mails containing CAD files were sent out of the domain *anonymouscompany.com* in the analysed period. We examined the e-mails and found out that in most cases they were addressed to company's clients. However, on May 18, 2016 we observed **one case in which a file was sent to competition. The file's name is project.dwg and it was addressed to m.wilburn@competitivefirm.com** by employee L. Baker.

Sender	E-mail subject	Recipient	Date and time
T. Mclain	Model CX290 – Details	s.merritt@clientfirmA.com	May 3, 2016 11:14 a.m.
R. Bragg	Category C separately	ian.hopper@clientfirmB.com	May 5, 2016 3:35 p.m.
V. Hanley	BS1200	purchasing@clientfirmC.com	May 6, 2016 10:07 a.m.

CAD files sent via e-mail – selection

Among recipients there appeared addresses of public e-mail services, e.g. *yahoo.com*, *gmail.com* and *outlook.com*. We recommend a proper consideration of whether sending files to this type of domains is allowable. These e-mail boxes might represent anonymous channel for data leaks to competition. Safetica allows you to limit domains where e-mails can be sent to, also with possibility to specify allowed attachment types for various domains.

It is worth mentioning that **all the e-mails contained the information unencrypted, which presents a security risk to the confidential data**.

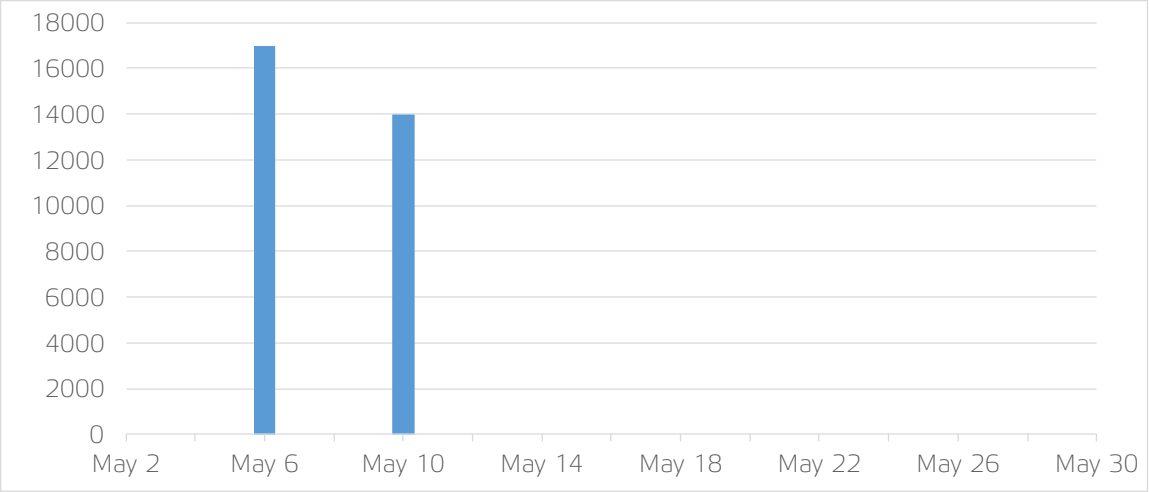
Recommended settings in Safetica:

- forbid CAD files to be sent to e-mail addresses of competition
- monitor CAD files sent to public e-mail domains
- encrypt CAD attachments so that they can not be opened by unauthorized recipients

Recording files to USB and other external devices

Employees T. Mclain and A. Hatcher recorded **32 588 sensitive documents** (total size of 19,12 GB) to USB drives in a single action.

Another potential channel for data leaks are USB drives and external devices in general. In the analysis we concentrated on CAD files being recored to this type of media. We discovered two significant deviations.



Timeline of recording files to external media

To blame for this deviations are employees T. Mclain and A. Hatcher who in a single time action recorded files to external media. In total there were **32 588 documents recorded, with the aggregate size of 19,12 GB. The files were of various types, including CAD files.** T. Mclain copied 70 DWG files, while A. Hatcher copied 23 DWG files. We recommend to examine this event and then set up a security policy - for example forbidding confidential company files from being recorded to external media.

Recommended settings in Safetica:

- forbid CAD files to be recorded to external media that are not in the company's ownership
- set up immediate notifications for the cases when a significant size/amount of files is copied

Utilization of web file storages

As for the set security rules, all activities on web storages and file hosting servers were OK.

Cloud storages and file hosting servers in general stand among potential channels for data leaks too. The only visited web in this category was www.dropbox.com.

File name	Date and time	Cloud
Graphics.zip	May 20, 2016 3:38 p.m.	Dropbox
13_0425_AnonymousCompany_aggregates_catalog_french.PDF	May 22, 2016 3:22 p.m.	Dropbox
Panel.PDF	May 22, 2016 3:48 p.m.	Dropbox
1-4(950x2340).PDF	May 22, 2016 3:57 p.m.	Dropbox
13_0425_AnonymousCompany_aggregates_catalog_RU_data(EU).PDF	May 26, 2016 9:27 a.m.	Dropbox
13_0425_AnonymousCompany_aggregates_catalog_(EU).PDF	May 26, 2016 9:27 a.m.	Dropbox
13_0425_AnonymousCompany_products_catalog_french_data.PDF	May 26, 2016 12:31 p.m.	Dropbox
13_0425_AnonymousCompany_agreggates_catalog_(EU).PDF	May 26, 2016 12:31 p.m.	Dropbox
1-9(950x2340).PDF	May 26, 2016 9:29 a.m.	Dropbox

We examined the individual records and found that the web storage was only used by employee A. Parker for recording work related content.

Recommended settings in Safetica:

- forbid sensitive files to be recorded outside of (allowed) cloud storages

PRODUCTIVITY

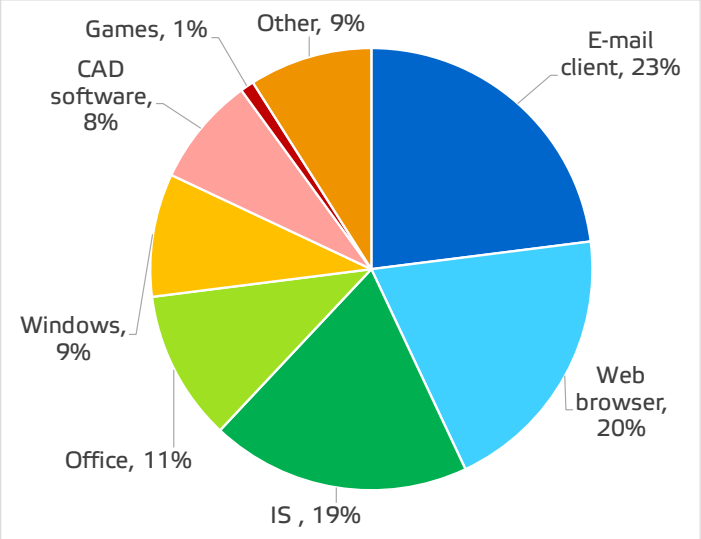
Utilization of applications

Employees played games in their work time, the most active in playing were V. Hanley (23 hours) and T. Howes (12 hours).

As for active time spent in applications, work in productive apps prevailed in the analysed period. The most used application belongs to the category E-mail client, other frequently utilized productive apps fall into categories IS and Office. Second most used app category was Web browser - it accounted for **20 % of total working time of employees.** (Read more about activity in web browsers in the chapter Visited webs.)

Application name	Running time
Microsoft Office Outlook (outlook.exe)	1127:22:12
Queris MES (queris.exe)	931:04:13
Chrome (chrome.exe)	531:13:59
Firefox (firefox.exe)	449:10:44
Explorer Windows (explorer.exe)	440:34:12
Microsoft Word (word.exe)	300:04:20
SolidWorks 2014 (sldworks.exe)	287:41:54
Microsoft Excel (excel.exe)	239:21:07
AutoCAD LT Application (acadlt.exe)	107:07:45
Solitaire (solitaire.exe)	24:02:44
Heroes of M. and M. III (heroes3.exe)	11:56:43
Minesweeper (Minesweeper.exe)	09:52:57
Adobe InDesign CS3 (indesign.exe)	02:01:36

Time spent in selected applications



Time spent in application categories

Category Games is completely unproductive. Employee V. Hanley spent about **23 hours playing games** Solitaire, Pinball and Minesweeper. T. Howes spent **12 hours playing** Heroes of Might and Magic III. Employee J. Nelson spent 6 hours playing Solitaire, employees R. Bragg and L. Brooks spent 3 hours each with the same game.

Recommended settings in Safetica and further actions:

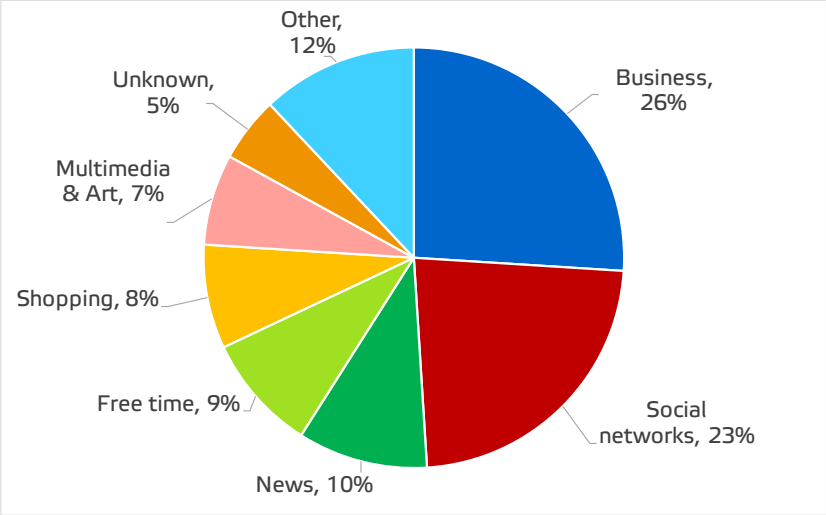
- block games in working hours, beyond the scope of e.g. 30 minutes
- use information from monthly summaries of utilized applications to save money on unnecessary expensive licences

Webs visited

74 % of the time online was spent unproductively. The most active visitors of unproductive webs were J. Myers and J. Nelson.

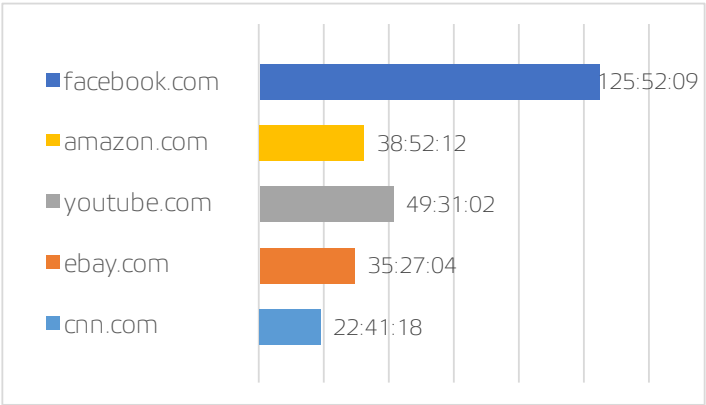
Employees spent almost 1/4 of the time on servers that fall into web categories Social networks, News and Free time. Other frequently visited webs belong to unproductive categories Shopping and Multimedia & Art.

We want to bring into focus visits of servers with **pornography and games**, both comprised in category Other. Besides the fact that these account for unproductive time and are in contradiction to internal guidelines, for computers they represent a high risk of getting infected by harmful software. The most active in this category were employees J. Myers and P. Thomas.

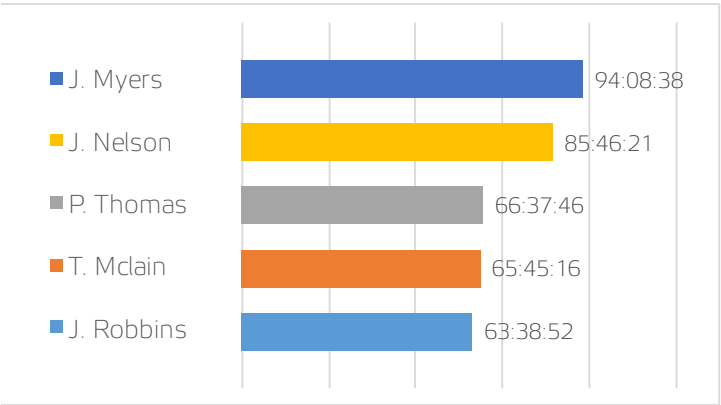


Time spent in web categories

All in all, as much as 74 % in web browsers was unproductively spent. The website that consumed the biggest portion of time is www.facebook.com.



Most visited unproductive webs [hours]



Employees most actively visiting unproductive webs [hours]

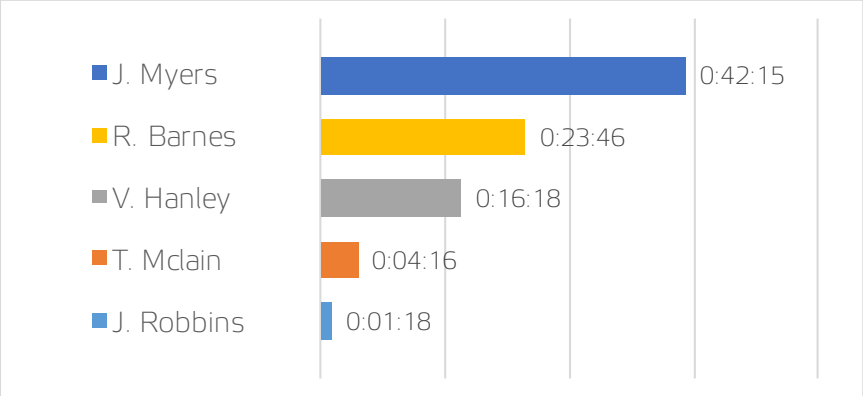
Recommended setting in Safetica:

- block selected servers that are not related to business activities (in working hours)

Job search

J. Myers searched for resignation letter template.

Employees who actively spend time on webs falling to Job search category are, from our experience, usually not performing sufficiently and leave their workplace within couple months. They present an increased risk of data leak.



Employees most active in Job search category

Our analysis indicated that employee J. Myers searched for resignation letter template. Employees R. Bragg, V. Hanley and T. Mclain actively searched out job offers. J. Robbins got to a web which belongs to Job search category by clicking on a link sent to her. It was a short, one time access, which might be considered unsignificant.

We recommend not to underestimate this situation. What belongs to good practise in such situations is a discussion about satisfaction with workload and team, as well as change of working conditions or contents.

Recommended settings in Safetica:

- set up warnings to get notified when employees visit web dedicated to job search
- it is possible to completely forbid accessing this kind of servers, but this does not diminish the problem

Total unproductive time and its costs

In Utilized applications we found out that 20 % of the employees' working time was spent in web browsers. Out of all this time, 74 % was then spent in an unproductive way. Applications were used unproductively in 1 % of cases. When added up, the numbers show that about 15 % of all activities was unproductive. On average, this comes up to **45 minutes of unproductively spent time per employee per working day.** By a quick look into Safetica you can easily identify the least productive employees. Our recommendation is to limit allowable unproductive time by means of internal guideline and then enforce its adherence with Safetica.

We can easily calculate how much Anonymous Company is spending for unproductive time on salaries. When taking into consideration $28,851 as median yearly income of individual American, then Anonymous Company with 100 employees pays $2,885,121/year on salaries.15 % share of unproductive time then means **$432,768/year spent on activities not related to work performance**.

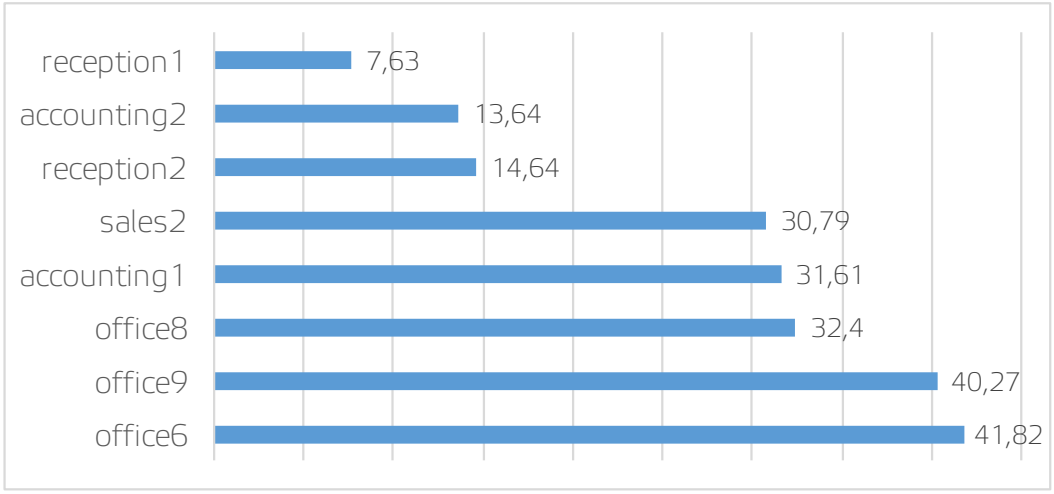
It is imperative to say that 55 % of the total unproductive time comes from the above mentioned employees: J. Myers, J. Nelson, P. Thomas, V. Hanley and T. Howes. These 5 employees, out of the whole monitored group counting 46 people, constitute the most significant area for optimization.

UTILIZATION OF IT RECOURCES

Utilization of work stations

⚠ Computer *Reception1* was utilized in only 7,63 % of its total running time.

This part presents case of Anonymous Company as far as IT recources are utilized. As an example we feature a comprehensive table of the least used computers:



Utilization of work stations [%] – stations with lowest activity

Worth mentioning is computer *reception1* on which the total activity was only 7,63 %. This station was on, but not used for almost 226 hours. A couple of other computers were underutilized too. On average, the stations were used to 56,14 %. Area for improvement is obvious: implement a policy commanding employees to power off computers after working hours, in order to save costs. Active usage rate should be at least 75 %.

ⓘ **Recommended measurment:**

- implement a policy commanding employees to turn off their computers after working hours

Print

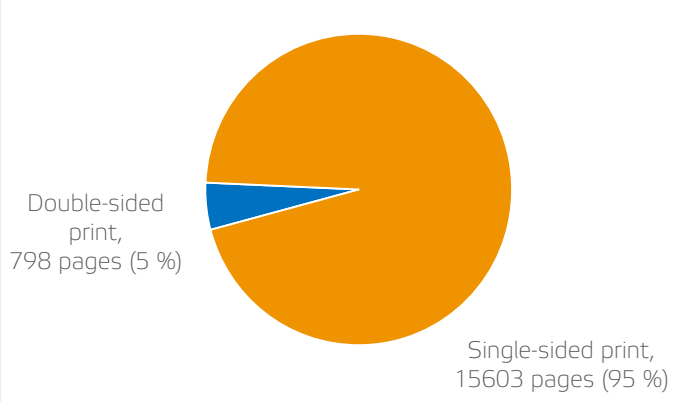
Print not related to work counted tens of pages. The black & white to colour print ratio was appropriate.

Detailed reports acquired in the analysis do not suggest that the printers would have been misused for private intents. At the most, employees printed tens of pages not related to work:

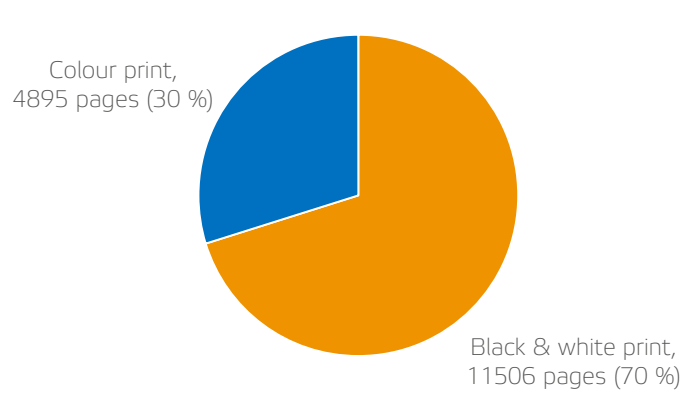
- P. Thomas – files from web mail (49 b&w pages)
- R. Barnes – panasonic-manual.pdf (34 b&w pages)
- L. Brooks – Microbiology1a.pdf (20 b&w pages)

t's up to the company's management whether they allow employees to print private documents or rather implement a policy. With Safetica you can either block print of selected files only, or globally. It is also possible to set printing quotas for employees.

The highest amount of pages printed in a working day was 1090, the lowest was 510. In following graphs it can be seen that there exists area for optimization of the single-sided vs. double-sided print ratio, as well as the colour vs. b&w print ratio.



Single-sided vs. double-sided print ratio



Colour vs. black & white print ratio

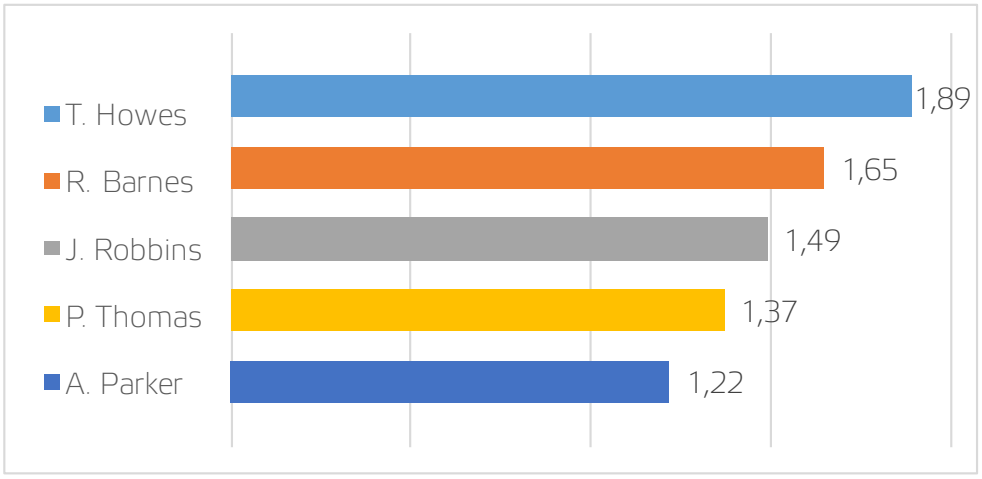
Eventual settings in Safetica:

- block print of selected files, set printing quotas, block print globally, or let your employees print freely, as a form of employee benefit

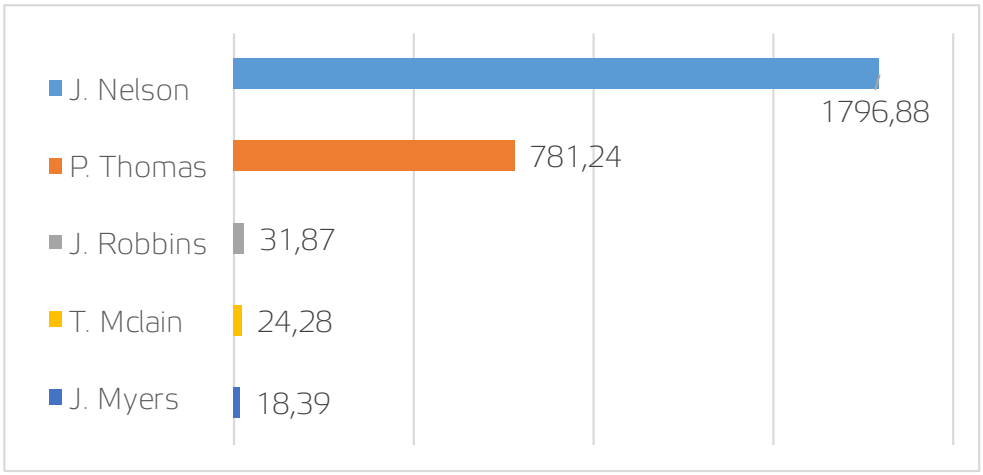
Downloads and uploads of files

J. Nelson used bittorrent client to download illegal material with total size of the 1,8 TB.

Network usage plays an important role as far as IT resources optimization is concerned. We focused on extremes present in this area.



Data uploaded [GB] - most active employees



Data downloaded [GB] - most active employees

Recommended settings in Safetica:

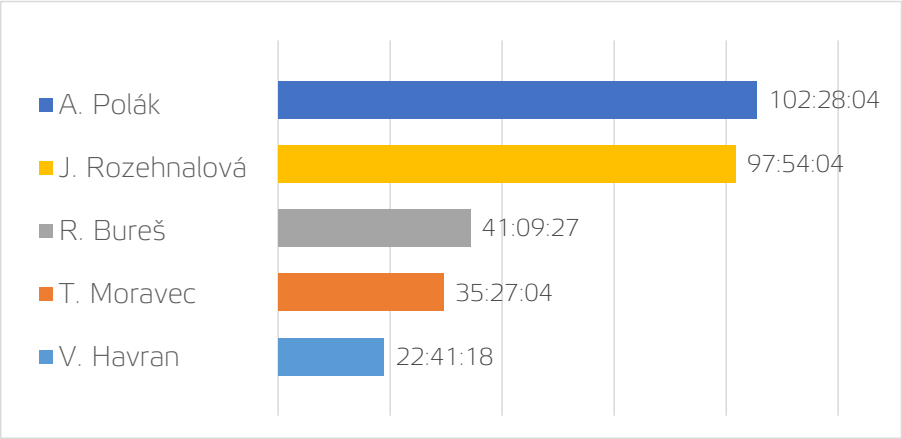
- block torrent aplication used for downloads
- set up immediate notifications for cases when significant volume of data is downloaded

Expensive licences

Application SolidWorks 2014 was actively used for almost 288 hours.

AutoCAD programmes are actively utilized. On the other hand **programme Adobe InDesign CS6 was used only for 2 hours.**

In this section we concentrated on utilization of the applications on which Anonymous Company spends significant sums of money, as it is the interest of the company to use it as effectively as possible. Our focus was especially on utilization of the high-priced application Solid Works 2014. We found that during the analysed period 5 people worked with this app, for a total time of 287 h 41 m 54 s.



Utilization of SolidWorks 2014

Recommended settings in Safetica:

- use information from monthly summaries of utilized applications to save money on unnecessary expensive licences