

**Faculty Name**

**Name of the cathedral**

Specialization name

**First name Surname**

Album number xxxx

**Thesis title**

Type of work (e.g. bachelor's,

engineer's, master's, design)

Name of the promoter

Place, month, year of defense

**Preface**

I must confess, I have a certain fondness for the versatility of Microsoft Word. It's a powerful tool that allows for a wide range of tasks, from simple note-taking to the creation of complex documents. Its user-friendly interface and extensive features make it a valuable asset in both professional and personal settings.

**Table of Contents**

[1. Introduction 3](#_Toc187676410)

[2. Colocation, server room or cloud? 4](#_Toc187676411)

[2.1. Colocation — what is worth pushing out of... 4](#_Toc187676412)

[2.2. Own server room — with which you can not part ... 5](#_Toc187676413)

[2.3. Cloud Computing — a departure to the cloud... 6](#_Toc187676414)

[3. Network security - predictions 9](#_Toc187676415)

[4. Conclusion 11](#_Toc187676416)

# **1. Introduction**

This paper presents the challenges, threats and safeguards associated with new information technologies developing at a dizzying pace today. The development of mobile and cloud technologies has blurred the boundaries of the functioning of enterprises, and makes the traditional approach to information protection - based on securing borders - completely inadequate to the current situation. Failure to take appropriate action is a simple path to an incident that can cause a serious threat to the security and development of the organization. "Unauthorized disclosure of sensitive information may expose the company to legal liability or financial loss.

To minimize such risks, a good protection plan, the right tools and employee engagement are essential."

# **2. Colocation, server room or cloud?**

****What services should we keep in our corporate stronghold, defended from the outside world by the high walls of our data centers? What should we lead to distant collocations and allow independent living?

Figure 1, server room

Administrators must also be ready for a bitter separation from services that will fly away to the cloud.

From the purely economic side, the profitability of maintaining your own server room is questionable. However, it is still being done.

The main reasons for maintaining your own data center are:

* security and innate distrust of companies,
* complicated financial/investment issues,
* law — sometimes sluggish reacting to changes in reality,
* the desire to keep your belongings with you.

However, change is inevitable and necessary. You have to abandon the old, sentimental scheme (even though it gives the impression of security) – your own data center with rack cabinets stuffed to the "roof", servers and arrays – and choose a different path. Less romantic and uncompromising, but perspective.

## **2.1. Colocation — what is worth pushing out of...**

Services that we can definitely colocate in a remote location are:

* web server,
* DNS,
* mail (in some cases).

We may wonder why? First, the most security-sensitive systems are moved outside of the company's locations and address pools. Secondly, it will not be obvious, that right behind the corporate web or MX servers are our data.

Figure 2, web server

Thanks to the fact that colocation centers have a much more advanced infrastructure than a standard server room of a small company, we can forget about dilapidated UPSs, leaking air conditioning, continuous ISP transmission failures, or the fight against SLA.

It is necessary, and even required, to see the location to which we migrate. The list of customers of a given colocation center can also tell a lot about the quality of services offered by them. Let's remember that the Internet is like paper - it will endure everything, and then we will not get to the "colocation center" in the "dugout".

The level of business continuity of our services can increase significantly if the company we choose provides standards that meet our expectations. For example, it will be a great achievement for us to have two truly independent Internet providers. On the other hand, a circle center usually has several.

The same with the power supply – we have Mr. Gucia for a quarter of the time and with the problem of "Filipino" disease, and they have Tier 3 – filled with aggregates, UPSs and what else we dream of.

Figure 3, server

To sum up, thanks to colocation, our servers will be in a server room monitored 24 hours a day, equipped with cooling and air filtration systems and emergency power supply. In addition, most data centers are located in locations least exposed to natural disasters (floods, earthquakes, fires, etc.).

Backup issues with this availability can be solved in a simple way by creating it to yourself - to the company. Colocation support can also ensure that you perform regular full backups of your data and enable continuous monitoring of backup status. You can also be more systemic - with the Disaster Re-covers plan, based on a separately operating environment in an autonomous colocation, several hundred kilometers away.

We now come to the economic issues. When we calculate very carefully, with all the details, creating our own data center and its maintenance (generating very high fixed costs including expenses for infrastructure, energy, staff, etc.) and compare it with remote colocation, it may turn out that our own server rooms do not make any sense, and "throwing out" our servers, along with the services running on them, will turn out to be very profitable.

## **2.2. Own server room — with which you can not part ...**

We must not touch devices that store sensitive information:

* personal data
* laboratory and design data,
* mainframe systems.

Personal data is a matter of course. The influence of GIODO (Inspector General for Personal Data Protection) on the activities of IT specialists resembles the experiments of Ivan Pavlov. If during any discussion about server infrastructure, its security, architecture, etc., the magic word "personal data" is mentioned, everyone participating in this conversation freezes for fear of the consequences that these words imply. Disputes about whether "unfortunate" personal information can and should move beyond one's location are fierce and endless.

Of course, you can direct your questions to GIODO and receive a comprehensive answer. For example, GIODO may request access to the server room from us during the inspection. And what if the server room is in Germany or the Netherlands? The answer is simple - in every Member State of the European Union there is an equivalent of GIODO and our institution may ask the local services to carry out an inspection or issue an opinion.

But what if such a server room is outside the EU? Here you have to consider whether it will be in accordance with the Act and the EU Directorate when we have an appropriate written agreement on entrusting the processing of personal data with a company from outside the EU. In the EU, this is simple, as Directive 95/46 EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data should be invoked, Article 17(3) to (4).

Finally, it should be remembered that the answer from GIODO does not have the force of a formal position:

* "... The Inspector General for Personal Data Protection may make a binding assessment of the circumstances of processing personal data only in an administrative decision, after conducting an appropriate procedure and examining all the facts of the case, as well as after analyzing the relevant legal provisions. This means that this letter cannot be invoked as a legal case. However, on the basis of the content of the letter, it is possible to presume the position of the inspector in assessing the situation during the ongoing proceedings, which would end with the issuance of an administrative decision."
* "So it seems that it is best to do 'nothing'. It is true that this "nothing" can be very expensive and problematic, but definitely much less risky than playing with the "Big Brother" GIODO."

Design and laboratory data should be kept in your own server room because of its great value. They are assets of our company and are much more valuable than information about how much the CEO earns, etc. A very important factor in the case of this type of data is the provision of extremely fast access times. In addition, they occupy terabytes on our arrays. The above elements mean that maintaining these services in a remote location could cost us many unnecessary problems – economic, technical, legal.

Let's now move on to the big black boxes that hold databases, i.e. the systems found in our server rooms mainframe. They are large, very fast and terribly hungry for electricity. In addition, they require a crystal clear room and properly cooled air. Any dust contamination or too large temperature fluctuations in the server room causes the possibility of shutting down and damaging the machines. Transferring something like this to a collocation is equal to a "death" sentence in the company. Nobody knows where it turns off, people from the service want cosmic sums for service, and the president of the company gets a heart attack seeing the valuation of the whole enterprise. In addition, the colocation centers will properly charge for special rooms for these big black boxes (cleanliness and proper cooling system) and for the consumed energy. Migration plus maintenance costs will in most cases turn out to be a spectacular financial failure.

## **2.3. Cloud Computing — a departure to the cloud...**

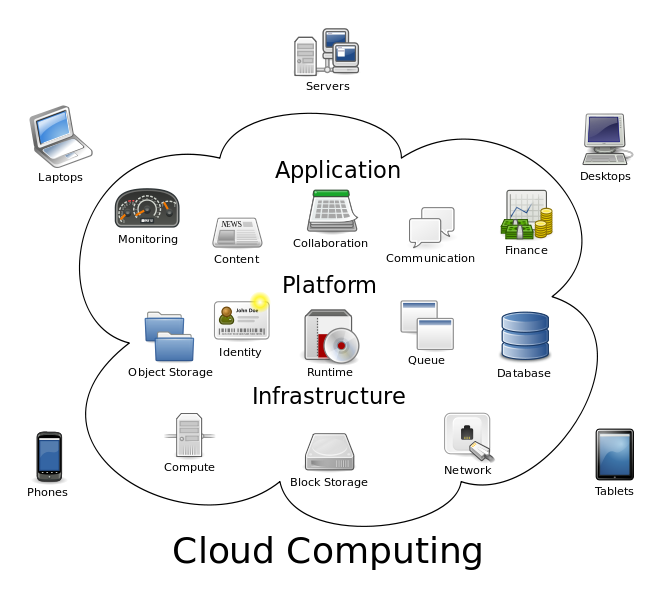
An intermediate solution to the cloud is colocation. Organizational and mental problems solved during the move to colocation will no longer be taken into account for the subsequent migration to the cloud, which will make it extremely easier for us to convince our management. Of course, it will not be without new challenges, but at least we will have a lot behind us.

Figure 4, cloud computing

Cloud Computing already has a certain level of service maturity. The software in the colocation center presents us with resources in a business way. We are no longer dealing (as in the colocation model) with inserting servers and counting their power consumption, etc. Here we pay only for the real use of computing power by our applications. The important thing is that the public cloud deprives us of rigid costs – such as, m.in hardware. It is irrelevant to us because we rely entirely on the supplier's resources. Therefore, the way costs are presented and their structure are changing.

The main advantages of the cloud are the ease of scaling resources, high performance and no problems related to hardware maintenance. We can create "servers" ourselves and configure them freely. Full control, the ability to change settings and hourly billing make it the most flexible solution. We determine the way of managing the available resources, while we have the opportunity to increase the amount of available operating memory or increase the performance of the processor practically on demand. There is no need to complete any additional formalities in the form of contracts or annexes and it works both ways, i.e. we can easily increase and decrease the available resources. Another advantage of this solution is that servers in the cloud can be put to sleep for night hours, and the next morning they can be started with one click or a pre-planned task. The cloud server is a toddler who moves slowly and burns very little, but in a second he can become a Ferrari speeding at unoffensive speed and devouring hectoliters of fuel. This is not possible in the case of buying/renting dedicated servers, which must be "calculated" to cope with the "performance peak" - which usually occurs infrequently, so most of the time the computing power of these machines is "wasted".

The cloud gives us the opportunity to run different types of services. It is necessary to take into account the nature of our company, its resources and requirements – just like in the case of co-location. The main systems to be moved are web, DNS and mail servers. Other candidates for migration to the cloud are project management systems or group work. Also, a file repository, accessible from any location in the world and on any device, is a great solution. Design services that require a very detailed cost accounting are by far the best candidates for moving to the cloud. The ease of calculating the resources used, and thus the financial outlays, is a very important element that allows for huge simplifications in interdepartmental settlements.

Other systems to consider migrating are dev and test systems. This gives you access to a very clear system of information about the project's operation, its financial balance and profitability, and – what is the most important from our point of view – the opportunity to show the project team that every move in IT costs money.

Finally, an example will be presented showing the advantages of the cloud when setting up a start-up:

* you do not have to spend money on the purchase of servers, infrastructure and support for them,
* you can increase or decrease your resources in the cloud at any time – easy cost adjustment and the ability to increase and decrease computing power in times of business growth or market stagnation,
* no surprises like: hardware damage, maintenance

And we deal "only" with our business...

Regardless of whether we choose colocation or cloud computing, we must be aware of what we are doing, aware of our requirements, our reputation and the quality of the company that provides us with the above-mentioned services. We must also not forget about our weaknesses and shortcomings of the supplier. The choice between your own server room and a remote physical data center or a virtual one in the cloud seems to be – looking at the other challenges – the final, most pleasant step.

# **3. Network security - predictions**

The chapter refers to an article from the industry portal [www.computerworld.pl](https://www.computerworld.pl/), which perfectly presents network threats for 2013. An additional value of this report is the inclusion of our national specificity, which speaks in favor of including this publication in this work.

"In 2013, we should be most afraid of attacks on mobile devices, phishing of confidential information by cyber-criminals and leaks of entire databases," predict Polish network security specialists.

The list of the most serious threats in 2013 was created on the basis of a survey prepared and prepared by the Safe Cyberspace Foundation. The survey was addressed to national network security experts, seventeen of whom provided comprehensive answers.

The survey included a summary of potential threats in 2013.

Their list was created on the basis of international reports and ideas of the authors. In addition, the list was supplemented by experts when a significant threat did not appear in the list. Survey participants were asked to give their opinion on the likelihood of a widespread hazard occurring and the level of danger if it occurs.

The strength of the report is its anchoring in Polish realities. The national specificity in some cases is clearly visible, for example in the assessment of legal and regulatory activities or the occurrence of some specific technical threats that have already occurred in Polish cyberspace."

Likely most common hazards (scale from 0 min. to 5 max.):

* threats to the Android platform - 4.35;
* phishing – via e-mail and websites – 4.24;
* information leaks from databases containing sensitive data - 4.12.

The most serious consequences in the event of an attack (0-5):

* cyber conflicts between states - 4.18;
* information leaks from databases containing sensitive data - 4.00;
* attacks on Cloud Computing - 3.65.

As you can see, our specialists highly appreciate the possibility and consequences of potential leaks of sensitive data. They also point to the disturbing regularity of using the same logins and passwords for all services. Which, in the case of data leakage from a social networking site, can result in serious problems - e.g. access to bank accounts by unauthorized persons.

The report also indicates the types of threats not provided by the provided list.

Financial:

* attacks on stock exchange systems,
* attacks related to electronic payments (m.in. theft of credit card data using Malwa-Re),
* attacks on paypass debit cards and NFC payments.

Law, regulations and good practices:

* increasing control over the Internet by international and governmental institutions,
* lack of effective methods of cooperation between the public sector (especially the government) and the private sector in the field of broadly understood IT security,
* lack of clear criteria for assessing and comparing the effectiveness of protection measures against network attacks,
* confusion in the regulations resulting in the closure of websites.

Another important information is that "in the prestigious ranking published by the American security team TeamCymru, Poland has been taking the infamous first place in the ranking of the largest botnet activity for many weeks and practically does not fall out of the TOP 10 list, the countries from which harmful ICT activity originates."

Another problem pointed out is "that the level of security on the Internet is very important for the correct approach to matters of legislation, regulation and dissemination of good practices. This is a signal that should encourage action on both sides of the dialogue. Our experience in this matter is not the best and it is worth taking this voice as a fear that the effects of similar negligence may be dangerous. The opinions should be dedicated to the Ministry of Administration and Digitization, which during the preparation of the document >Cyberspace Protection Policy of the Republic of Poland< completely omitted the comments that appeared during public consultations."

However, from a global perspective, it is necessary to look at such threats in particular:

* attacks on Cloud Computing - more and more corporations keep data there, so insufficiently protected cloud computing services can be a weak point in the company's security,
* Advanced Persistent Threat attacks targeting specific public figures (CEOs of the largest companies, politicians) via mobile devices,
* attacks exploiting vulnerabilities in M2M (Machine-to-Machine) communication - usually targeting platforms related to national security - facilities specializing in the development of weapons and production of military technologies,
* botnets will attack mobile and stationary devices simultaneously - new forms of DDoS attacks that will hit both types of devices at the same time,
* The increase in malicious programs targeting mobile devices – users are moving away from traditional platforms in favour of newer, smaller mobile devices – securing these devices is now more difficult than ordinary computers.

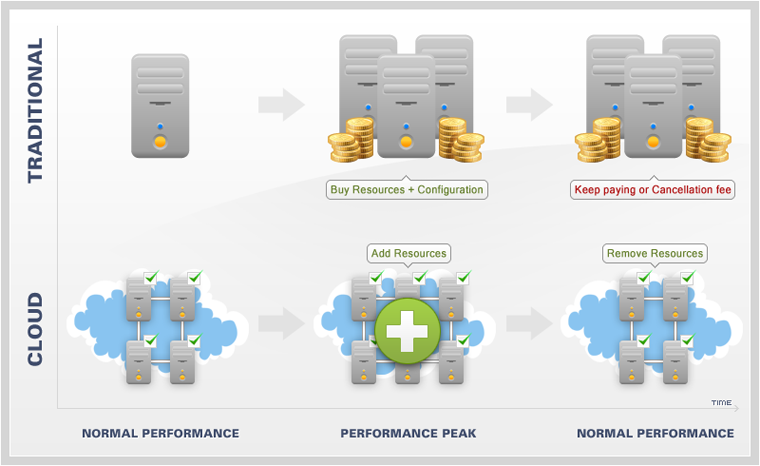


Figure 5, traditional/cloud platforms

It can be seen that threats related to mobile platforms and data leaks are mainly increasing. Hard days are also coming for Cloud Computing, which is developing more and more and thus appears more and more often in the crosshairs. This paper presents ways to mitigate the risks associated with these hazards. But you have to be vigilant all the time and use common sense - even the best security will not help if the attack is directed at a person. And it is known that it is the weakest link and most of us will find a way.

# **4. Conclusion**

To sum up, the field of Information Security in general will continue to develop dynamically and new threats will appear in this area - some already exist, but we are not aware of them. The constant race between new security methods and innovative attack methods will drive the development of pioneering solutions in the so-called Information Security in order to try to keep up with the so-called Progress. Because it is very fast, especially in terms of hacker mechanisms and their detection, the material contained in this work will quickly lose its relevance.

# **Bibliography**

1. Cade, M. (1999). Servers. W M. Cade, *"Data Center Migration: A Guide to Planning and Execution"* (strony 99-200). San Fransisco: Works Press.
2. Packard, C. (2022). *"Information Security for Dummies".* LA: Works Press.
3. Vel̲authap̲pan, K. (2009). *"Cloud Computing: Theory and Practice".* Kyiv: Works Press.

**Table of figures**

[Figure 1, server room 5](file:///Z:\wsi\Diploma.docx#_Toc187679955)

[Figure 2, web server 6](file:///Z:\wsi\Diploma.docx#_Toc187679961)

[Figure 3, server 6](file:///Z:\wsi\Diploma.docx#_Toc187679966)

[Figure 4, cloud computing 8](file:///Z:\wsi\Diploma.docx#_Toc187679967)

[Figure 5, traditional/cloud platforms 13](file:///Z:\wsi\Diploma.docx#_Toc187679971)