

IT outsourcing – threats and benefits

Case: Central and Eastern Europe

Alex Kelley
MBA/MS-MIS candidate
Joseph M. Katz Graduate School of Business
University of Pittsburgh

Summary

This paper is trying to establish a reference on security issues concerning outsourcing, also addressing the special case of the Central and Eastern European region.

With an overview on common outsourcing advantages and problems and with suggestions towards some ways of overcoming the risks and enjoying the benefits, this paper is meant to provide a starting point for a more in depth research on outsourcing in Central and Eastern Europe.

Above all the theoretic and exemplified information, the most important factor in outsourcing refers to knowing the existing legislation of the country the company is interested in outsourcing IT services, and understanding the differences in cultural attitudes. These can go a long way towards ensuring a secure outsourcing relation.

About the author

Born and raised in Romania, Alex Kelley is currently a MBA/MS-MIS candidate at Joseph M. Katz Graduate School of Business of the University of Pittsburgh. Her interests are oriented towards the general issue of information security, with applications in the countries of Central and Eastern Europe.

Please write to Alex Kelley at aokelley@katz.pitt.edu with questions or suggestions.

Overview

A large number of private and public corporations, governmental agencies and other institutions deal with personal information, like social security number, bank accounts, and so on. An even larger number deals with corporate-specific information, from employee files to new project development plans, new product budgets, research results, merger and acquisition information for future events, and other documents that would hurt the corporation if destroyed or made public. There's also the military-tactical sector to be considered (usually top secret data). Except for this last category, all other information is usually either processed at the company level or outsourced to another country in order to save costs.

Logically, there's an increasing trend of protecting this sensitive information against various events, like data destruction or information theft just to mention a couple of the existing threats¹. For the first one, different storage media have been developed over time. For the last one, the debate over what should be done to better protect personal data is far from being over. It addresses the network security, the protection of data transfers, the software vulnerabilities on any given network, as well as the human factor.

Outsourcing

IT outsourcing is the process of contracting a third party for managing an IT process or system outside the institution that uses it (*Outsourcing definitions*). There are two main ways of outsourcing: **offshoring** (outsourcing to another country, usually in order to take advantage of lower costs) and **nearshoring** (where the company or institution outsources to a contiguous or same continent country, typically to make use of cultural similarities and time zones).

There are a variety of IT services that can be outsourced (*Outsourcing definitions*):

- mainframe management
- database and/or remote systems administration
- security management (*Cisco Systems whitepaper*)
 - access control services

¹ See *Computer Security Threats*.

- intrusion detection systems
- firewalls and antivirus protection
- encryption
- content filtering
- website design and hosting
- application hosting
- software development and maintenance.

When deciding towards outsourcing, a company usually does so because IT management (or any of the above mentioned services) is not a core competency – which in turn means that by outsourcing it the company can obtain a competitive advantage by using the vendor’s competencies (possibly enhanced by complementarities that are offered)² and save on overall cost. There is, however, the always present issue of security. If the vendor (the company that provides IT services for the outsourcing entity) doesn’t protect the outsourcer’s interests and information, the latter has most to suffer than the former – above all, there is a reputational (*D. Daniel*) risk.

Outsourcing market key numbers

By the end of 2009, the global market for shared services and outsourcing is expected grow to \$1.43 billion, compared to \$930 billion in 2006 (*R. King*). As for IT outsourcing alone, in 2006 companies spent about \$233 billion, which is more than a quarter of the total amount spent on outsourcing in general. The “Eastern Europe ICT and Outsourcing Market (2007-2011)” study by the research company RNCOS in October 2007 (cited in *Sims, D.*) presents the development of the Eastern European outsourcing market in numbers. Thus, the information and communication technology sector in this area is one of the largest growing segments in the world, with \$61 billion in 2006 and expected to reach over \$70 billion in 2008. Within the segment, the software grew to \$3.6 billion in 2006 and is expected to register a growth of 11.6% by the end of 2007. According to the study, the EU accession of the countries in this area is the important factor drawing more IT players to invest in the information technology industry in Eastern Europe. The main customers looking for service providers in the area are telecommunications, banking and financial services, manufacturing companies, as well as government administrations (with larger scale projects).

² For a case study on how vendors as service providers in outsourcing relations accomplish their core competencies and are able to provide complementarities in order to become more attractive refer to (*N. Levina – Cost advantages in IT outsourcing*)

Advantages of outsourcing IT

A company's management would typically consider outsourcing all or part of the IT department in order to put the company in a more advantageous position.

- One of the advantages of outsourcing is the **reduction in cost**. These are an outcome of establishing economies of scale on the vendor side that could not be matched by small and medium-sized institutions. In addition, the result of the salaries paid to vendors' work force being typically lower than the ones in the country of origin of the outsourcer typically lowers total costs.

- A side effect of the efficiency obtained is the **improved time** from the beginning of a project until it is launched in the market. This can easily be exemplified in the case of introducing new services and products, where it would take a relatively longer time for building the infrastructure needed for supporting the new product lines, for instance, and where the experience and speed of a specialized vendor would enhance the outsourcer's ability to innovate.

- Outsourcing offers a **focus on core competencies** and thus **competitive advantage** for the client, by taking advantage of the experience of the vendor instead of training an in-house IT department and increasing the operational burden for companies that do not have information technology as their main focus (*S. Ortiz jr.*). Companies that operate with strong IT departments can use their resources on developing and improving processes to support their corporate strategy, while outsourcing the strictly operational applications.

SLAs

Service level agreements are determined at the beginning of any outsourcing relationship and are used to measure and monitor a supplier's performance.

Often, a customer can charge an outsourcer vendor a penalty fee if certain SLAs are not met. Used judiciously, that's an effective way to keep a vendor on the straight and narrow. But no CIO wants to be in the business of penalty charging and collecting. Bad service from an outsourcing vendor, even at a deep discount, is still bad service, and can lead to greater problems. It's best to expend that energy on finding out why the SLAs are being missed in the first place and working to remedy the situation.

- Another advantage consists of a ***better security coverage and service***. Through an SLA³, for instance, the parts involved can agree on a 24 hour extended coverage, when the outsourcer itself would not have been able to provide that without increasing the costs to an unwanted level (this is also referred to as *cost avoidance* – *NaviSite whitepaper*). Also, since the vendors are highly specialized, compared to the outsourcer's own IT employees that are limiting their experience to a narrow spectrum of security incidents, they may be able to notice new threats faster.

Security issues and other threats concerning IT outsourcing

- Through outsourcing in general, a company ***transfers and/or shares part of the risk*** with the third parties. This argument makes the transition between opportunities and threats, since the transfer of risk widely depends on legislation in the countries involved. This is the point where an SLA proves its force or the lack of it: under different judicial systems, the conditions on the contract may not be enough to make the service provider liable for any damage or loss of information that may have occurred⁴. In other words, if the service provider fails to fulfill the contractual duties, the outsourcing company may be able to get something from a law suit in the vendor's country, but is still held accountable (*J. Leigh*) in its own country for breaches that took place, if they break the law in the respective country (the outsourcer's).

- One of the main threats is the ***loss of control*** over the outsourced operations. This brings with it the necessity of allocating managers to the outsourced relationship. One step further⁵ would be to set a rather rigid frame for the outsourcing agreement, with clear-cut checks and balances, and also organize training sessions for the employees of the service provider. Indeed, this practice would help towards establishing a higher security level, but on the other hand it would significantly contribute to the overall costs.

- In some cases, the vendor is either not willing to or can not change and easily adapt processes to better fit the company that is outsourcing. This ***lack of flexibility*** is a notable disadvantage of the outsourcing process, and can be partially addressed through the initial SLA, or even before that: when making the decision as to where to outsource, by eliminating from the beginning the destination where the information available points toward inflexibility in the work practices.

³ A service level agreement (SLA) is a contract between an IT services provider and a customer that specifies – at the beginning of the outsourcing relationship and in measurable terms – what services the vendor will furnish (*CIO's ABC*).

⁴ The *Information Security Survey 2007* (Informationweek Research & Accenture, July 2007) finds that almost half of the US companies believe that security vendors should be held legally and financially liable for security vulnerabilities in the products and services they offer (*Outsourcing definitions*), indifferent of the country of practice.

⁵ As recommended in *S. Ortiz, jr.*

- There is also an **impact on human resources** and **assessment of security issues** given the status of the vendor's employees, as the outsourcer experiences a loss of direct control over who is hired to work on its IT functions. Depending to the vendor's cultural context, this may lead to differences in categorizing information into private and public and thus creating a real threshold over what needs to be protected from breaches.

- IT outsourcing can determine a **relocation of IT equipment** from a safe and known environment to an unknown one (*D. Twing*), thus further creating risks for the company.

- In addition, possible security risks come with the opening of the company towards a third party providing services that often involve **sensitive information** (exposure of critical data, intellectual property such as patented processes or source codes).

- The complexity of the security process determines an **increased vulnerability** to data breaches, especially under outsourcing agreements (*A. Coro*). The reason is that most outsourcers do not take the time to understand all the details involved and thus are more likely to make mistakes in either choosing the vendor or in determining the SLA.

- From the same reasons mentioned above, the **compliance with internal regulations** may be harder to meet through outsourcing, especially if the service provider is not sufficiently aware of the legislation regarding IT in the country of origin of the outsourcer. As far as liability goes, even if the service takes place in the vendor's country, the outsourcer is still the one that has to comply with the law (*J. Leigh*).

- More of a general threat, not IT outsourcing specific but nevertheless important in the decision process for outsourcing is represented by the **currency risk**. Financially, the changing exchange rates can make an initial cheap contract become quite expensive – especially, in the case of the United States for instance, in the light of the diminishing purchasing power of the dollar during 2007.

Legislation with effects on outsourcing decisions

With the continuing development of online activity and inter-country collaboration on IT issues, different countries adopted a number of regulations that, even if they are not necessarily addressing only security issues, have chapters dedicated mainly to protecting citizens' and corporate privacy and/or determining situations for disclosure.

For instance, in the United States there are HIPAA⁶, SOX⁷, Gramm-Leach-Bliley⁸. SB1386 (which covers a number of privacy disclosure laws) among others. Among regulations that

⁶ A complex reference to HIPAA (the *Health Insurance Portability and Accountability Act*) can be found at <http://www.hipaa.org/>. Its regulatory content falls outside the purpose of this paper.

address privacy issues are California's Database breach notification act⁹ of 2002 and the more disputed Patriot Act¹⁰, which has been critiqued to act against the personal information protection conferred by the legislations mentioned above.

However, even given the various legislative acts, the number of companies that are not in compliance is surprisingly high (only roughly a third of the American companies comply with different regulations, according to *A. Holmes*).

Since 2004, Canada has PIPEDA¹¹, the European Union created the Data Directive¹², and Japan approved a version of the American Sarbanes-Oxley¹³.

The difficulty lies in that, as noted above, different countries have different regulations that affect the information in a different way. Thus, because of different legal jurisdictions and legislation, what is true in the outsourcer's country may or may not stand in the vendor's country, and vice versa. One of the first things to do when deciding the vendor country is to understand (*A. Holmes*) the legislative system.

Factors that influence the outsourcing decision and location

▪ The *linguistic skills and education* of the country towards which a company is outsourcing its IT functions should be a factor to take into account. If the vendor's employees are fluent in the outsourcer's language, then there are fewer problems likely to arise from misunderstandings about what is desired from the service provider. These factors are softened though by the *cultural affinity* between the supplier and the outsourcing customer, which has a less quantifiable effect but still adds to overall productivity¹⁴.

⁷ Introduced in 2002, the *Sarbanes-Oxley* act (also known as the *Public Company Accounting Reform and Investor Protection Act of 2002*) has led many companies to form new departments dedicated solely on ensuring compliance with this regulation; the act is so complex that a great number of companies is still spending resources towards achieving compliance. A summary is available at <http://www.sarbanes-oxley.com/>.

⁸ The bill was adopted in Congress in 1999 and requires financial-services companies to protect the privacy of customer data and prohibits them from sharing it with other entities without permission. The subchapter on disclosure of nonpublic personal information can be consulted on the Federal Trade Commission website (<http://www.ftc.gov/privacy/glbact/glbsub1.htm>)

⁹ It requires companies to notify individuals if any unauthorized person obtained access to private information (http://www.datagovernance.com/adl_data_laws_california_security_breach_notifi.html)

¹⁰ Focusing on expanding surveillance and investigative powers of law enforcement agencies, the *Patriot Act* (<http://www.whitehouse.gov/infocus/patriotact/>) was a legislative reaction at the attacks of 9/11.

¹¹ The *Personal Information Protection and Electronic Documents Act* - http://e-com.ic.gc.ca/epic/site/ceic-ceac.nsf/en/h_gv00045e.html

¹² This directive was adopted in 1995 by the member states of the European Union and contains 34 articles on protection of sensitive information. The unofficial text of the EU *Data Directive* can be found at http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

¹³ So-called JSOX (<http://search.japantimes.co.jp/cgi-bin/nb20061229a1.html>), the legislation will be applied starting the new fiscal year, in April 2008.

¹⁴ A more detailed explanation of the factors, from a nearshoring perspective, can be found in *D. Bradbury*.

- A high **level of skilled work force** (*S. Pruitt*) tends to provide a better performance, since the vendor's employees are more knowledgeable and prepared for addressing possible issues in the outsourced project.

- Differences in **time zones** between the two countries show an influence in the availability of the service provider; in fact, this is one of the arguments towards choosing Central and Eastern European countries instead of the further away Asian service providers and vendors.

- The **economic and politic environment** could strongly influence the stability of the relationship between the two parties involved in the contract. In general, any possible disruptions in the normal work flow (caused by national movements or merely local strikes) increase costs (down time, loss of productivity, even relocation eventually if the situation does not resolve timely).

- Another element to research is the **quality of infrastructure** in the provider country, since frequent power outages, for instance, can lead to data loss to only mention the most obvious effect.

- One of the main elements most companies look for, though, is the **price of labor** in the area where the vendor is situated (*R. King*); the lower this is, the more attractive the respective country is for outsourcing destinations, all else equal.

It is in the balancing of all these factors above that the decision becomes difficult. Related to this conclusion, most companies consider outsourcing part of their IT processes mainly because this would provide a reduction in costs. Experts (*CIO's ABC*) consider though that lower costs constitute only the initial reason for considering outsourcing. After researching offshoring and nearshoring options, companies typically realize the low price sought should be balanced by other considerations, some of them mentioned above – thus, the cost of outsourcing in general and of labor in particular should *not* be, and typically *is* not, the top decision criteria.

What's happening in the Central and Eastern Europe¹⁵?

An important number of international corporations have slowly been making their way towards CEE countries in the past years. After the fall of the communism in that region, Central and Eastern Europe has shown an increasing attractiveness for foreign investors, not the last among types of investment being outsourcing, and in particular IT services. The following developments further show the opening of the region towards the Western IT investment.

¹⁵ Central and Eastern Europe/European region is also referred to as “CEE” throughout the text.

What countries are CEE?

There are different views as to what is Eastern and Central Europe. For the purpose of this paper, the classification by the Central & Eastern European Business Directory will be used a rather extended classification, which lists Central European countries (Czech Republic, Hungary, Poland, Slovakia, Slovenia) and Eastern European countries (Balkan countries: Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Macedonia, Montenegro, Romania, Serbia; Baltic countries: Estonia, Latvia, Lithuania; strictly Eastern European countries: Belarus, Moldova, Russia, Ukraine). Some of the researched papers also consider the Caucasus republics (Armenia, Azerbaijan and Georgia) as well as Central Asiatic republics (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan) in the context of CEE countries; since these are former Soviet Union countries, they are indeed culturally close to the rest of the Eastern Europe, so the inclusion is correct in the cultural context – geographically, though, these countries are situated on the Asian continent.

- Skype's development center is located in Tallinn, *Estonia* (King, R.) Same city hosts HireRight and the largest office of eBay.

- *Belarus* saw an increase in outsourcing, with IBA Group¹⁶ (specialized in SAP and Baan implementations) and EPAM Systems (which does software development for the US health insurance and healthcare market) as two of the main players on the market. Small-sized, Belarus faces a relatively limited internal demand for IT specialists, which leaves the labor force open towards offshore programming. Belarus has a "reputation as the Silicon Valley of the former Soviet Union", according to MW2 Consulting's CEO, Uwe Weinkauff, in *Radkevitch, U.*)

- The *Czech Republic* was situated on third place in the top of the most attractive offshoring destinations in 2005, according to a study by EIU (Economist Intelligence Unit) cited in *Pruitt, S.* Commerzbank of Germany outsourced its data processing to Prague (*Tagliabue, J.*). Accenture's main center in Central Europe is located in the Czech Republic (starting 2001), but they have expanded to the capitals of *Slovakia, Hungary, Poland* and *Romania*.

¹⁶ IBA Group was founded in 1993 as a partnership between Minsk R&D and IBM, which withdrew as shareholder in late 90s but remained main customer.

- Pilot Software, US-based strategy management software company, outsources software design projects to the Moscow (**Russia**) vendor Auriga (*OOPB association*).
- The Dutch electrical conglomerate Philips operates a shared service center near Warsaw, **Poland**.
- In 2006, Morgan Stanley decided to open a technology center in Budapest, **Hungary**.
- Google started working with a research lab in Krakow, **Poland** (*Swaine, M.*) and then purchased it.
- The first CEE outsourcing summit took place in July 2007 in Kiev, **Ukraine**. The summit, named *Silicon Valley Open Doors 2007*, hosted 18 countries in the Central and Eastern European region¹⁷, as well as partners from Western Europe, Asia and the United States (*Silicon Valley*).
- The Unit, and IT service provider from **Lithuania** worked with IT in the car industry (Fiat and Mitsubishi)¹⁸
- Sciant, a Swiss IT services vendor, has its main development center in **Bulgaria's** capital Sofia (*OOPB association*)

Wages

Eastern Europe is a particularly attractive option for outsourcing from the Western European companies, due to closeness – both geographic and cultural – and also to lower wages. According to a study conducted by McKinsey (*Hoch, Kwiecinski and Peters*), between 2000 and 2004 the compound annual growth rate of wages was between 1% (Russia) and 15% (Hungary), with Slovakia, Bulgaria and the Czech Republic around 11-12%, Romania (8%) and Poland (3%). As an observation, in the latter years, as more countries in the area became members of the European Union, the wages showed a more pronounced increasing trend as the quality of life slowly improved.

¹⁷ For a detailed list of the participants, as well as for the subjects that were discussed, visit the official website of the summit at <http://www.cee-outsourcing.com/>.

¹⁸ As cited on the company's webpage (http://www.unit.lt/unit/our_clients.php)

In the 2006 Global Outsourcing Guide, CIO magazine analyzes some of the countries that provide IT services for outsourcing Western companies. In the Central and Eastern European area, Hungary, the Czech Republic, Poland and Russia are considered overall “challenging”, but with rising wages for the first three (as they became members of the European Union) and with poor infrastructure and security under the risks chapter for the latter. Also mentioned, as “emerging” and with lower salaries (an average of \$5,000 - \$10,000 for an entry-level programmer with 2 years of work experience), are Ukraine (with a significant increase in the IT sector, but with English not spoken as widely as in other countries in the region), Bulgaria (which acts on a smaller scale due to a reduced workforce, but with IT workers experienced in complex technologies) and Romania (with the most IT professionals per capita in Europe, according to a study by Brainbench cited in the CIO magazine guide).

Information security awareness

Various studies have repeatedly raised the question of treating security as a cost instead of something that could add strategic value (and thus being able to translate into revenue). Only 37 percent of the almost 8,000 respondents in 50 countries in a study by CIO, CSO and PriceWaterhouseCoopers (*Holmes, A.*) say that they have an overall security strategy as of the end of 2006. The study underlines the importance of having C-level security positions and mentions that only about a third of the companies participating in the research have created this type of position.

There have been considerable efforts from the European Union towards increasing education and awareness concerning information security, with two underlying aims: enhancement of development of the information society and promotion of trust in online services.

In the **European Union**, ENISA conducted a study (*ENISA and PwC*) with the help of PriceWaterhouseCoopers, which concluded that despite the acknowledged high importance of information security (half of the participants in the study consider it a “high priority” and another 30% think it constitutes a “very high priority”, as opposed to 4% giving it a “low priority”), many managers in the EU find it difficult to justify significant expenditures on awareness programs for employees. For any programs addressing the issue, there does not seem to be a post-program evaluation to quantify the benefits and compare them to the costs. Since the awareness training is viewed more as a compliance requirement by three quarters of the respondents, as opposed to a security issue, the budget for it is treated as overhead rather than as an investment.

An interesting observation can be made on the initiative of information security training taken by large number of companies in the European Union, in the view of the lack of regulations to specifically require member states to conduct this type of training (the companies do pursue the training because they consider it important in view of achieving compliance with the existing legislation).

Advantages of outsourcing to Central and Eastern European countries

- Due to closeness to the regular outsourcers (compared to India, for instance), CEE offers a more attractive *time zone*; smaller time zone difference seems to improve communication.
- In addition to the geographical nearness, this part of Europe also shows a *cultural closeness*, which means minimal socio-cultural differences among the countries here and their Western clients.
- Although CEE is more expensive than India, it is still a *cheaper skilled labor force* than the option of *not* outsourcing (*The rise of nearshoring*).
- Due to the close ties to Western Europe and to the status of EU members of many countries, also from traditional reasons, Eastern Europe is *more regulated* than some of the Asian outsourcing destinations. This factor shifts some of the responsibility towards the vendors, since they have to comply with the internal regulations before even establishing an SLA, but it also adds to the amount of paperwork to be prepared with virtually any event.

The top IT outsourcing country at present is not European: What's happening in India?

The CIO Magazine's study on the global state of information security (*Holmes, A.*) refers to the absence of even some of the routine security tools and policies in Indian companies, like access control software or security guidelines for external business partners. One in every five or six Indian companies had issues concerning extortion, fraud and intellectual property theft during the past year, a number that is from twice to four times larger than the percentages found in the rest of the world.

PriceWaterhouseCoopers' specialists suggest conducting risk assessments and background checks if doing business with an Indian partner. An article in the Network World (*McMillan, R.*) describes a data breach that took place at the beginning of 2006 in the Florida Department of Management Services database. According to this source, the breach had been caused by the service provider that subcontracted part of the human resource management applications to a company based in India.

- The high number of multilingual workers, with English, French, German and Spanish either known, or otherwise easy to learn at a high proficiency level, makes EEC show comparatively *fewer language barriers* than its competitors on the outsourcing market (*Hoch,*

Kwiecinski and Peters). According to a comparative analysis done by eCODE¹⁹, Romania is the most multilingual country in Europe, after the Netherlands, for potential business-process outsourcers (*The rise of nearshoring*).

- With countries that are members of the European Union, NATO, or both, the **political environment** in the region is relatively **stable**, and in addition the government shows a **stronger commitment** to the industry.

- Many companies consider the work performed in the countries of Eastern Europe to be more **scientifically intensive** (*Pruitt, S.*) than that which is produced in other markets

- Due to **reliable infrastructure** already in place there is a relatively low risk coming from this direction. (*Ferguson, T.*)

- Researchers also point out the strong **engineering talent** in the Central and Eastern European countries, also software programmers that show more **flexibility** than some of the other offshore locations because they are willing to work (*OOBP association*)

Shortcomings of outsourcing in the CEE region

- The legacy of communism is shown mainly in **unexpected delays** and **excessive bureaucracy**, with the latter being widely a cause of annoyance as an investor has to tour various institution in order to receive a needed document or permit. In addition, Eastern Europeans have been known for years as taking long socializing breaks while at work.

- The relatively **high level of corruption** may create unplanned additional costs with the pretended reason of generating savings, all through CEE, although this trend has decreased with the EU ascension.

- There is also a **lack of certification authorities** (*Levina, N. – former USSR*), which makes it difficult to assess the actual level of knowledge and capabilities in the IT sector.

- Even with a high number of technical experts, there is a chronic **lack of prepared managers**, especially qualified **project managers**.

- Countries in the region have experienced a tendency towards the so-called “brain drain”, with IT specialists driven towards other countries where the pay is higher (*CIO’s ABC*). This constitutes one of the shortcomings of nearshoring in particular, where, due to the limited distance between the provider and the client, there is a faster increase in wages in the field

¹⁹ The European Centre for Offshore Development is a group of independent offshore outsourcing consultants based in UK (<http://www.ecode.org.uk/>)

where the particular provider's country is specialized (it's one of the reasons why IT wages in Eastern Europe are increasing faster relative to the ones in Asia).

The legacy of communism

In a way, the countries of Central and Eastern Europe constitute a paradox. On one hand, their citizens are reminiscent of communist practices and express worries about their phone conversations being taped and archived (they are, indeed, in most countries of the area). On the other hand, people are not aware that their government is usually applying the exact same form of control over ISPs (*Daniel, D.*). This leads to a relatively dangerous mentality especially in the non-technical people, which in turn can determine negligence in a position inside a service provider company (which, just as is the case in the United States and Western Europe, does not function with technical staff only). From the point of view of human resources, the work force in the region has a solid educational background (*IT Business Edge article on "Soviet heritage"*), with the traditional orientations towards engineering and scientific degrees that easily take IT functions and adapt to the new requirements.

Recommendations for common outsourcing issues

- The most important factor towards a rewarding outsourcing contract is **knowledge** of the common practices, culture and legislation of the targeted country.
- Before actually outsourcing a database or service, the company needs to strictly **classify the existent data** into common and sensitive and have clearly stated standards and guidelines on handling it; these standards should also appear on the SLA.
- During the set up of the **service level agreement**, the outsourcer needs to make sure that the service provider will abide by the SLA even if the legislation in the respective country is not as information-protective as the outsourcer would want it to be.
- The **roles and responsibilities** of the service provider should be clearly stated in the SLA, together with **rules about inspection and audit**. Some experts (*Twing, D.*) also suggest creating a venue for legal disputes, establishing penalties for breaches of security policy and requiring nondisclosure and non-compete agreements from the vendor employees.
- Only the employees that need access to data should have it, and only as much as they need to be using at that moment, according to the **principle of least usage** (*Coro, A.*).

- The vendor's *applied security policies* should be subjected to close research from the outsourcer; preferred policies are strict, starting from the hiring process and going to the actual enforcement. In the optimal case, the vendor will also monitor the traffic in and out of the establishment and any other possibilities of information theft (for instance, by restricting the usage of USB devices).

- There is also the *risk of privilege abuse* (Coro, A.) from either internal or external sources (a data breach committed by an authorized user testing the limits of the security system). If a database, for instance, doesn't contain protection against easy ID and password discovery (which should be specified in the SLA if the vendor doesn't already have a strict protection), then this makes obtaining access privilege that much easier.

Central and East-Europeans are open to new businesses and conscious that – to make it simple – the more businesses they service, the more opportunities will open for them. In order to overcome the *specific* issues of outsourcing to CEE, an international company would need to become familiar with the main characteristics (IT-qualified work force and level of knowledge, range of salaries, reliability of infrastructure, existent legislation²⁰) of the country that will be chosen as service provider. After the decision was taken to outsource to country X, the company needs to understand that there *are* cultural differences that *will* appear in the relations with the vendor country, but with some knowledge about what to expect²¹, these would show an insignificant effect on the work.

²⁰ For countries that are European Union members, relevant EU directives will apply as well

²¹ One of the most reliable sources on general information about a country is CIA's World Factbook (<https://www.cia.gov/library/publications/the-world-factbook/index.html>). As far as specific, non-number, issues go, a good start point would be the Wikipedia (http://en.wikipedia.org/wiki/Eastern_Europe) articles on the country, for an overview of cultural characteristics and a set of links to national webpages for further research.

Sources

Beckett, Helen – “*Outsourcing options in Eastern Europe*”, Computer Weekly, January 31, 2007

Blau, John – “*SAP targets Eastern European midmarket*”, InfoWorld, May 31, 2006

Bradbury, Danny – “*Nearshoring: Looking closer to home*”, Computer Weekly, June 21, 2005

Coro, Ariel – “*9 Tips for Outsourcing Securely*”, in <http://www.sourcimgmag.com/content/c061120a.asp>

Daniel, Diann – “*As the outsourcing market grows, so do the security risks. What can you do to decrease the threat?*”, CSOonline.com, May 29, 2007 (<http://www2.csoonline.com/exclusives/column.html?CID=32812>)

Ferguson, Tim – “*Eastern Europe new favourite for outsourcing*”, ZDnet.com, December 11, 2006

Ferguson, Tim – “*European companies to look East*”, December 8, 2006 (<http://management.silicon.com/itdirector/0,39024673,39164600,00.htm>)

Germain, Jack M. – “*The Security Implications of Outsourcing*”, CIO Today, May 16, 2006

Hoch, Detlev; Kwiecinski, Michael; Peters, Peter – “*The overlooked potential for outsourcing in Eastern Europe*”, Mc Kinsey on IT, Winter 2006

Holmes, Allan – “*The Global State of Information Security 2006*”, CIO magazine, September 15, 2006

King, Rachael – “*The Outsourcing Upstarts*”, Business Week, July 31, 2007

Leigh, John – “*Managing outsourcing security risks*”, in <http://www.securitypark.co.uk/article.asp?articleid=24963&CategoryID=1>

Levina, Natalia – “*Off-shoring to Former Soviet Union: Understanding boundary-spanning practices*”, New York, December 10, 2004

Levina, Natalia – “*Sources of vendor production: Cost advantages in IT outsourcing*”, Massachusetts Institute of Technology study, October 1, 1999

Levina, Natalia; Ross, Jeanne W. – “*From the vendor's perspective: Exploring the value proposition in information technology outsourcing*”, MIS Quarterly, Vol. 27, No. 3, pp. 331-364, September 2003, September 1, 2003

Locher, Margaret – “*Outsourcing in Eastern Europe*”, CIO Magazine, February 1, 2007

McMillan, Robert – “*Offshoring cited in Florida data leak*”, Network World, March 24, 2006

Ortiz, Sixto (jr.) – “*Can Outsourcing Skilled IT Help Compromise Security?*”, General Information, Vol. 27, Issue 44, pp. 30 in print issue, Nov. 4, 2005

Pruitt, Scarlet – “*Report: Eastern Europe to challenge Asia in outsourcing*”, Network World, February 16, 2005

Pruitt, Scarlet – “*When outsourcing, don't forget security, experts say*”, Computerworld, September 21, 2004

Radkevitch, Ulad – “*Belarus attempts to become the Eastern European Bangalore*”, Outsourcing Center, March 1, 2005

Rapoport, Michael – “*Companies Pay A Price For Security Breaches*”, Wall Street Journal, June 15, 2005

(da) Silva, J. Schwarz, Dr. – “*Future Internet research: The EU framework*”, ACM SIGCOMM Computer Communication Review, Volume 37, Number 2, April 2007

Sims, David – “*Eastern Europe ICT, CRM Report Finds 'Large Growth'*”, TMCnet, October 22, 2007

Swaine, Michael – “*Why the next big thing in software may come from Eastern Europe*”, Dr. Dobb's portal, May 7, 2007 (<http://www.ddj.com/architect/199300084?pgno=1>)

Tagliabue, John – “*Eastern Europe Becomes a Center for Outsourcing*”, New York Times, April 19, 2007

Twing, Dan – “*Reviewing the security aspect of outsourcing: Outsource the work but stay in control of the security responsibilities*”, Network World, September 7, 2005

*** - “*ABC: An introduction to outsourcing – CIO.com*”, CIO magazine (<http://www.cio.com/article/40380/8>)

*** – “*Computer security threats classification*”, CACI Information Assurance (<http://www.caci.com/business/ia/threats.html#Malicious%20Threats>)

*** - “*Information Security Survey 2007*”, Informationweek Research & Accenture, July 2007

*** – “*Information security awareness initiatives: Current practice and the measurement of success*”, (research carried out by for ENISA by PriceWaterhouseCoopers), July 1, 2007 (<http://www.enisa.europa.eu>)

*** - “*Outsourcing definitions*” Offshore Experts (http://www.offshoreexperts.com/index.cfm/fa/map.outsourcing_definition)

*** - “*Securing your business information - Strategies for outsourcing security measures*”, Cisco Systems Inc. whitepaper, June 24, 1905 (<http://www.cisco.com/go/security>)

*** - “*‘Soviet Heritage’ Makes Eastern Europe an Outsourcing Contender*”, IT Business Edge, December 5, 2006

*** – “*Technology Investment Conference - Silicon Valley Open Doors 2007*”, (<http://www.svod.org/node/487>)

*** – “*The Bangalore experience goes Baltic*”, Offshore Outsourcing Best Practices association, June 11, 2007, <http://www.oobp.org/Outsourcing+News/628.aspx>

*** – “*The Rise of Nearshoring: Budapest, Tallinn and Warsaw*”, The Economist (print edition), December 1, 2005

*** - “*The ROI of outsourcing*”, NaviSite Inc. whitepaper, 2005 (<http://www.navisite.com>)