2007

The Importance of Human Factors when Assessing Outsourcing Security Risks

Carl Colwill
BT Design Security Risk & Compliance

Andy Jones
BT Security Research Centre

The Importance of Human Factors when Assessing Outsourcing Security Risks

Carl Colwill
BT Design Security Risk & Compliance, United Kingdom
carl.colwill@bt.com

Andy Jones
BT Security Research Centre, United Kingdom
Adjunct, Edith Cowan University, Australia
andrew.28.jones@bt.com

Abstract

The word is becoming increasingly interconnected and ways of doing business are evolving rapidly. Communications technology is ubiquitous and reliable and businesses are continuously seeking ways in which systems can be exploited to improve resilience, become more efficient and reduce costs. One way in which organisations seek to achieve this is by concentrating their efforts on core business processes and outsourcing non-core functions. However, outsourcing - and particularly offshoring - presents many security issues that must be considered throughout the lifetime of contracts. The scale of outsourcing and increasing technological and security complexity is making this task more difficult. Often neglected, or given low priority, are factors relating to the people who will be working on the contract. These factors will be driven by regional and cultural differences and will manifest themselves in differing security threat and risk profiles and risk management frameworks must be designed to recognise and cater for these variations. This paper is based on BT's extensive global sourcing experience and describes some of the key human factors that can impact significantly on the success, or otherwise, of secure outsoucing. The application of technology alone will not provide solutions. Security controls need to be workable in a variety of environments and need to be designed, implemented and maintained with end user behaviour in mind. New approaches need to be considered for building and maintaining trust and secure relationships between organisations over time. Ownership of security is required, as is a means of building understanding and empathy with the cutomers' need for security; this may only be effective in the long term rather than short term – and this in itself presents a major challenge in the outsourcing world with its high churn of personnel.

Keywords

Outsourcing, offshoring, human factors, security risk management, security risk assessments, design, security controls

INTRODUCTION - OUTSOURCING CHANGES SECURITY RISKS

In an increasingly interconnected world where communications technology is ubiquitous, reliable and increasing in capacity and functionality, businesses are continuously seeking ways in which they can improve resilience, become more efficient and reduce costs. One of the ways in which they seek to achieve this is by concentrating their efforts on core business processes and outsourcing other functions that are required to support the core business to other organisations. Organisations providing outsource capability – the suppliers - can now offer the same or similar services and functionality to a number of customers more efficiently or at a lower cost (or both). Customer call centres and software development, maintenance and support are examples of business and IT functions that are most often outsourced.

Another aspect of the global sourcing marketplace is that it is increasingly acceptable, and indeed commercially necessary, to outsource to overseas centres –"offshore" locations - where the cost base is lower than in the regions where the organisation carries out its major business. In deciding to adopt the outsourcing option, there are a number of other factors, including security, that need to be considered in addition to the capability of the service provider to meet the requirements of the business. Some commercial factors are obvious, but it is becoming increasingly clear that a range of less tangible regional, cultural, political and philosophical issues must be taken into account when identifying the potential risks.

In most outsourcing transactions, the customer transfers the responsibility for handling functions to the supplier. From the security viewpoint, information protection presents an obvious risk as the outsourcer is unlikely to be able to retain the same measure of control over sensitive information that it could within its own company or country; this may lead to data being exposed to theft or disclosure. Outsourcing also increases the number of people having access to assets within your organisation's boundaries and can exacerbate the "insider threat", particularly where they may be concerns regarding commercial espionage or national security. All security regimes will be dependent on human factors and Jaques (2006) highlights the importance of people in achieving acceptable levels of security

SECURITY RISK MANAGEMENT AND OUTSOURCING DECISIONS

As global sourcing evolves and matures, more comprehensive risk assessments are being adopted to facilitate business decisions. Some security considerations are usually assessed in detail before contracts are signed, partly because the expectations of the outsourcers' customers are increasing – especially in relation to data protection in an offshore environment. Political, Economic, Social, Technological, Legal and Environmental factors (PESTLE) are often quoted as essential prerequisites for any risk analysis before contracts are signed and work is transitioned. However, security input will tend to focus on the technological factor though all of the above factors have security implications for the contract and need to consider the people who will be involved.

The typical outsourcing security model puts the emphasis on the customer (outsourcer) to impose the following on the supplier:

- build multiple levels of physical, IT and personnel vetting security requirements into policies, processes and procedures;
- mandate security training and awareness programmes;
- mandate security and compliance audits;
- impose severe penalties for security breaches.

These are all facets of good business practice but should not be seen definitive solutions to all security issues; periodic review and variation may be required for different suppliers in different parts of the world.

Effective security risk management requires ongoing assessments of risk, implementing appropriate controls and measuring compliance to requirements. In reality, driven by the increasing scale and scope of sourcing, many security assessments involve performing a one-off risk analysis that subsequently drives all sourcing business decisions - well before all the factors, and the complexity of organisational and people interactions, can be realistically understood, let alone reviewed effectively over time. The creation of an environment of ongoing secure operations and trust over time can prove very troublesome, even when things appear to start off well.

THE IMPACT OF CULTURAL AND SOCIAL FACTORS IN OFFSHORING SECURITY

A European survey on the impact of globalisation on business risk highlighted that 57% of respondents cited problems stemming from cultural differences (Copeman, 2007). The need to consider cultural and social implications when drafting contracts is not new (Pruitt, 2004). For example, standards of privacy could be considered looser in the Indian subcontinent because of its close-knit societies where, say, reading someone else's e-mail would not be considered much of an intrusion. The implication is that this more relaxed attitude toward privacy could have serious consequences when it comes to protecting corporate data and specific contractual security requirements are required to address this. A survey on the impact of globalisation on business risk highlighted that 57% of respondents cited problems stemming from cultural differences (Copeman, 2007).

However, once contracts have been signed, there is a great potential for the relationship between the customer and supplier to be driven solely by service level agreements (SLAs) and the pressure to increase productivity. Treating outsourcing as a procurement issue rather than a relationship issue can encourage an adversarial approach (Muir, 2006). Cultural implications and the impacts on individuals are often ignored and even if considered initially, may be given lower priority over time as the supplier organisation becomes treated as just one source of input to the outsourcer's organisation. It is also important to consider two levels of cultural implications that impact on individuals: the regional culture (usually derived from religious, philosophical, social and historical factors – and this can vary significantly within the political boundaries of a single nation); and the supplier's organisational culture (derived from the founder's philosophy, organisational myths and the nature of work conducted). Note that the latter now provides some levers for the security community: most large companies offering outsource services have adopted, or plan to adopt, international standards such as ISO27001

– which can help instil a security component to organisational culture. Cultural differences will also impact on attitudes towards risk: some companies will be willing to work with far lower risk thresholds (i.e. making operations and decisions more 'riskier') in an attempt to gain business advantages. This is often seen in offshore health and safety topics but this can also lead to cutting corners for security. Different educational systems will also have a bearing on attitudes, outlooks and the process for acquiring knowledge, e.g. the occidental 'analytical' approach compared to the oriental 'holistic' and 'philosophical' approach.

Global sourcing also highlights the language differences that can cause problems of misunderstanding and misinterpretation at all levels – from the wording of the contractual security requirements down to the day-to-day briefings employed at the work face. There are many versions of English! Even where there is no conflict over the explicit meaning of the wording, per se, the implicit perceptions and expectations behind them will differ - driven by the history of security approaches and issues within any given company and country. There are regional attitudes and propensities towards different types of crimes and the means of protecting against them, for example, Indian companies have traditionally focussed on physical security and expect low levels of crime – but the situation is changing, driven by the rising importance of India as a global IT provider and changing crime patterns and global threats. However, the lack of long-term experience of (and more importantly a thorough understanding of the reasons behind) critical security controls such as physical and logical access logging and analysis, can lead to a 'lip service' or 'veneer' approach. The importance, and implications to overall levels of security protection, of even basic differences in perceptions and expectations has been borne out by the authors' experience of audits focussed a given subset of controls but targetted at variety of companies across different countries; there are many different approaches and responses, and many lessons to be learned to ensure effective understanding, implementation and maintenance.

Another issue that must be taken into account is that of acceptable business practice. Practices that are considered illegal and abhorrent in the Western World, for instance the giving of substantial gifts, are common and accepted practice in other regions. In fact it is often difficult to carry out business in some countries unless the 'wheels have been oiled' and the relevant parties have been remunerated in some way for their input or their consent. Carrying out business in a region where practices that we find unacceptable are the norm may cause significant problems when trying to establish the cultural values that we understand and find acceptable may prove challenging. In this environment, additional consideration should be given to the way in which organisational ethics are promoted and the way in which staff are trained and rewarded.

It must also be noted that most people responsible for writing contracts and security requirements will have little or no experience of the country in which they will be applied. It is often difficult for Westerners to understand some of the cultural, religious and societal pressures, e.g. the caste system and hierarchical society implications in India where orders are expected to be obeyed and the rules required by customers at work will always tend to be less important than behaviour ingrained over countless generations.

POLITICAL, LEGAL AND ECONOMIC FACTORS

Political and legal systems vary significantly. Although often treated at a macro level for supplier due diligence assessments as part of the sourcing bid process, these factors also have implications on the personal level and often need to be complemented by specific training to overcome ingrained attitudes and behaviours. The way in which business is conducted and the perception of contract and liabilities (and their importance) varies across regions and cultures. Data protection can now generally be handled adequately by standard model clauses but attitudes towards intellectual property rights (IPR) can vary significantly between western and Asian countries. Even within the West, there are significant differences between the laws in the UK and the USA and, to some degree, the rest of Europe. It is important to remember that local laws will always take precedence over the outsourcer's home country legislation. There are also other practical issues that impact on security levels: e.g. the ability under local privacy laws and to obtain information for effective background checks and vetting of employees, e.g. criminal records and academic qualifications.

The presence and power of the state will also feature in the way individuals think and act and where the requirements of the state may override any contractual requirements. The outward face of recently liberalised nations (from both societal and economic perspectives) should not hide the true level of control that the state still exerts. It is usually wise to assess the risk of regional government interception of confidential information and communications; the use of data encryption may be restricted (to forms easily decrypted by high-capability agencies) or prohibited completely.

Preconceptions and stereotypes may also apply. Security requirements imposed by Western companies on Asian suppliers, for example, could be seen as attempts to exploit differences in, and attitudes towards, the maturity of the legal environment and are based on assumptions that tighter control (and imposition) than would be allowed in the parent country will be acceptable offshore, e.g. frequent body searches of all staff. This may prove counterproductive to developing relationships and empathy.

Economic implications are usually viewed by outsourcers as opportunities to get the best deal. However, they should also be viewed from the perspective of the supplier's people, especially the value of money. Job income, though relatively low by Western standards, may, quite literally, be matter of life of death for some families and it must be remembered that in such cases the power of money (even relatively small sums) can be a powerful coercion factor. There are many allegations (often 'scare stories' in Western media) about offshoring security breaches, but real incidents do happen (BBC 2005, 2006).

CREATING TRUST AND GAINING 'BUY-IN' TO SECURITY REQUIREMENTS

There are many definitions of trust but from a basic security perspective it relates to creating confidence and assurance that personnel will not abuse the responsibilities, access, authority and knowledge given to them to perform a given role. In an outsourcing context, the focus of attention for the customer is to ensure (or enforce) trust by presenting measures such as rigorous employee vetting requirements. However, it must be remembered that most high-impact security breaches, e.g. fraud, tend to be perpetrated by senior executives (Wilding, 2007); often these people will have no not directly involved in your specific contract. It can also be argued that, on a personal level, trust must be earned not imposed. If trust cannot be achieved at the individual level, experience shows that it will be difficult for organisations involved in an outsourcing relationship to operate together at a business level (Winn and Bickerstaff, 2007).

It is easy to assume that the people working for the outsource supplier will, with suitable 'carrot and stick' inducement, buy into the outsourcers' requirements or face sanctions. Senior management within the suppliers will readily accept, and sign up to, customer requirements but in reality it is difficult for them to speak for all their staff particularly in larger companies where there is a large churn of people at the lower levels. It must also be recognised that, as with all humans, the real motivation to change behaviours and outlooks will come from within not without and may require specific intervention, i.e. targetted education, and not just another missive from the top. Imposition rather than education and negotiation may not be effective in the long run. Sasse et al (2007) highlight a range of issues related to people factors that impact of the acceptance of security requirements.

Employee loyalty is an oft-quoted Holy Grail and an important concept for secure outsourcing. It can be argued that companies with a large percentage of long-term personnel see more buy-in to security, not for security's sake, per se, but for the very survival of their company and thereby their own future. The situation in sourcing suppliers is typically very different, e.g. it is well known that a high level of loyalty is unlikely in a call-centre with deskilled jobs, short contracts and 40% churn of staff. There are also two levels of loyalty to be fostered: to the employer (the outsource supplier who actually pays the employee's wages); and to the employer's customers (the outsourcer), who may seem to be less tangible entity and far removed from any considerations of reward.

EDUCATION – SECURITY TRAINING AND AWARENESS

A common theme for human factors and security is education. Training and awareness are important but must be seen from a realistic perspective. Sasse et al (2007) highlight that awareness and education can prepare the ground but changing people's behaviour involves breaking old habits and establishing new ones via targetted training. To be truly effective, this crucial topic needs to be more than regurgitating the outsourcers' or the suppliers' security policies but a *process* of building understanding, preferably empathy and ownership, and developing knowledge of situations that may cause security threats and risks and the behaviours and reactions required. For example, it is important for operatives to know how to recognise and respond to social engineering attempts when their job is designed to help the foreigner on the end of the phone.

The scale of recruitment by suppliers is also a factor that can cause problems: some outsourcing service providers in India and China are growing rapidly, hiring thousands of new employees in a month; this requires significant training in the supplier's standards, let alone the supplier's customer's. Effective education in the customers' expectations also has a cost and the need to provide appropriate outsourcing security training budgets has been highlighted (Schwartz, 2005). From BT's experience, this will usually also include the outsourcer providing appropriate training material (e.g. security Computer Based Training (CBT)) and onsite training personnel.

THE IMPACT OF COMPLEXITY

All organisations are a mixture of socio-technical systems, with each component, including every human being, having vulnerabilities that are open to accidental or malicious exploitation. Complexity will compound security vulnerabilities and the potential scale of impact, and therefor increase risks – often in a subtle or intangible way that is difficult to model or assess. System complexity is increasing rather than decreasing and security requirements, both technical and procedural, are becoming more demanding on people. This has become a significant feature of global sourcing environments e.g. customer specific information confidentiality markings, the use of a variety of security tokens, userids and passwords for gaining physical and logical access, etc. From the outsourcer's perspective, there is sometimes a view that the more security controls that are implemented, the more secure the environment. However, the opposite may be true. The situation may be further compounded: one given supplier may be providing services to many companies from different parts of the world and there may be little consistency, and probably some notable contradiction, in the total set of security requirements they are attempting to implement. Sometimes this can be also exhibited at a micro level with different projects from the same customer (but sourced from different divisions within the same company) where conflicting requirements are presented. In these environments humans will undoubtedly make errors and gaps in layers of protection will appear which can lead to accidental security failures let alone exploitation by those with malicious intent.

Security may also be unintentionally placing hurdles in the way of productivity, which is key in the mind and the objectives of most on the receiving end of out-sourcing contracts, especially where time is precious and meeting the targets is essential. This can only result in lip service being paid. Sasse et al (2007) confirm that when security mechanisms create an unreasonable physical or mental barrier they will be bypassed if they affect remuneration. Improved design of controls, with participation of the people affected, is becoming a key topic.

AUDIT AND COMPLIANCE

The outsourcer's customers are now demanding assurances that their outsourced information and operations remain secure. Security requirements and controls should therefore be designed to facilitate audits and the implementation of effective governance and compliance regimes. Onsite audits of supplier facilities are an essential part of ensuring ongoing outsource security but should not just be seen as an opportunity to wield the big stick. Supplier security engagements can be used as learning opportunity to test not just compliance to standards and controls (and acquire appropriate tangible evidence and assurances) but to test understanding of requirements and the rationale behind them and to capture company and regional factors and differences. Audits therefore present significant opportunities for education (and reinforcement) on the customer's security culture and philosophy . Based on its experience, BT now employs a full time supplier security relationship manager in India. The main role of this person is to build alliances with the supplier's senior management responsible for security and risk management and to facilitate migration to effective security cultures. BT also provides opportunities to those people responsible for conducting outsourcing risk analyses and recommending security requirements to participate in overseas onsite audits to see the impact of their work and appreciate the implications for effective implementation. Once again this has cost implications.

POTENTIAL SOLUTIONS

There are a number of measures, taking into account human factors, that can be implemented in order to improve the likelihood of effective and long-term outsource security. At a basic level, the following should be considered:

- employ a common security language – use international standards and security controls , e.g. ISO27001, rather than re-invent the wheel each time;
- create basic 'building blocks' for your own specific security requirements that are understood globally with all your suppliers, i.e. not just technical and procedural components but awareness. (NB it is necessary to avoid conflict or repetition with global standards);
- design security controls that integrate the tasks in hand and the people responsible for these tasks. Sasse et al (2007) identify five key design principles that should feature in all designs.
- be sensitive to cultural issues when developing policy and requirements (this should not mean the dilution of corporate, legal or regulatory requirements – or customer expectations - but to be cognisant of the impacts of implementation);
- use risk management and compliance reviews as a learning opportunity and compare cross-region and cross-company results for explicit and implicit lessons;
- involve those responsible for creating security requirements and controls in supplier engagements and reviews.

More importantly, outsourcers and suppliers need to recognise that a wide-ranging set of security vulnerabilities can exist stemming from the complexity of technological and human interactions which cannot be solved by contracts alone and may be further impeded by short-term business visions and priorities. Risks will therefore vary and require periodic review.

Other obvious, but frequently ignored steps that can be taken to improve the likelihood of success are the introduction and maintenance of an ongoing programme of training and awareness. While this is often poorly implemented in the organisation that is outsourcing, the potential effect is slightly mitigated by loyalty, cultural understanding and staff working to protect their jobs, it is vastly more important in outsourced, offshore environment. There is nothing new in this type of programme, however, even in the UK in organisations that have a good record on security, it is often not well implemented. When a culture of security understanding and awareness has been created through the use of training and awareness programmes, it is essential to carry out a process of reinforcement to ensure that staff have a heightened sensitivity to any potential security issues. Sasse et al (2007) emphasise the importance of organisational behaviour and 'citizenship' – involving the informal aspects of work roles and relationships that can be managed via personal 'psychological contracts' negotiated with employees, rather than depending on a 'command and control' approach.

CONCLUSION

New approaches need to be considered for building and maintaining trust and secure *relationships*, i.e. not just relying on the traditional 'customer' and 'supplier' security model. However, these may only be effective in the long term rather than short term as they will be dependent on communication, feedback and a new level of openness on real security threats and issues. Ownership for security is required and a means of building empathy with cutomers' need for levels of security; this is facilitated by education and understanding. However, time may not be on the side of those attempting to implement new approaches, especially with high staff turnover and the resultant frequent changes of personnel within contracts.

Greater simplicity rather than complexity is needed. This requires ensuring that security controls are workable in a variety of environments and can be bolted together. This has major design and cost implications and moves further away from a simple 'lift and shift' approach to outsourcing. Such controls will need to be developed with end user participation – sometimes this may mean the involvement of those 'untrusted' targets for the security controls. Variations in design and/or implementation may also be necessary for effective local implementation, but this may add to the complexity of the customers' compliance regimes.

Periodic security risk management and compliance frameworks should be augmented to create a means of recognising, capturing, assessing and testing human factor implications and, in turn, feed back into security requirements, vulnerability, threat and risk assessments and contractual clauses.

However, all of this must be balanced against commercial realities and priorities: the costs of even more investment in security assessments and the implementation of controls (often for the sake of less tangible or long-term benefits) may be difficult to justify in many companies.

REFERENCES

BBC (2005) http://news.bbc.co.uk/1/hi/world/south_asia/4619859.stm

BBC (2006) http://news.bbc.co.uk/1/hi/world/south_asia/6044402.stm

Copeman, S, (2007) Strategic Risk, Risk without frontiers

Jaques, R, (2006) Human factor essential for IT security: People and processes more important than technology, vnunet.com, 26 Oct 2006, http://www.vnunet.com/vnunet/news/2167357/human-factor-essential-security

Muir, D, (2006), Computer Weekly, Why, when and where to outsource

Sasse et al, (2007)Human Vulnerabilities in Security Systems, DTI Cyber Security Knowledge Transfer Network, 2007http://www.vnunet.com/vnunet/news/2167357/human-factor-essential-security.

Scarlet Pruitt (2004), IDG News Service, Companies often forget about cultural differences that may affect security.

Schwartz (2005), IT Compliance Institute, Organisations Neglect Human Factors in Security.

Wilding, R, (2007) Insiders are the biggest enemy, Strategic Risk, September 2007.

Winn, E and Bickerstaff, R, (2007) Computer Weekly, Pull together for outsourcing success

COPYRIGHT

Increasing security in the physical layer of wireless communication

Luke Golygowski
School of Computer and Information Science
Edith Cowan University
lgolygow@student.ecu.edu.au

Abstract

This paper introduces a concept of increasing securing in the Physical layer (PHY) of wireless communication. It gives a short description of current status of wireless standards and their security. Despite the existence of advanced security protocols such as IEEE 802.11i or WLAN VPNs, wireless networks still remain vulnerable to denial-of-service (DoS) attacks aiming at PHY and Data Link Layers. The new solution challenges the problems with the currently defined PHY and Data Link layers. The concept introduced here, holds a promise of descending with some of the security measures to the lower layers of the TCP/IP and in this way not only increases security but also efficiency and performance. In addition this model would reduce management overhead and security architecture complexity. The proposed solution is dealing with: encryption implemented as part of modulation techniques as well as authentication procedures partially deployed within the first two layers of Open System Interconnection (OSI) protocol stack. The introduced model attempts to solve problems related to DoS that is focused on Data Link Layer, eavesdropping and man-in-the-middle (MITM) attacks. Additionally, there are presented some ideas for future research in the area of protection from malicious activity aimed at the PHY Layer – e.g., jamming attacks, as well as other security issues such as eavesdropping prevention by use of physics laws and tunnelling as another layer of protection to ensure privacy and signal robustness. The potential deployment of this technology embraces Wireless Local Area Networks (WLANs) as well as the emerging IEEE 802.16e (mobile WiMAX) standard. In this paper there are considered and analysed practical needs, defined necessary steps and set priorities. In the final part, there are presented challenges concerning the research and there is established a background for the consecutive papers.

Keywords

Modulation, cryptography, TCP/IP, OSI Layers, PKI, Wireless DoS attacks.

INTRODUCTION

In its core design, the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack was not meant to be secure. It was supposed to remain operational in case of geographically dispersed disaster (Ciampa et al 2005). It was developed in times of political unrest and cold war. TCP/IP goal was to assure communication even after nuclear attack (Thomas et al 2004). However, since it was an extraordinary invention capable of completely changing the world, it was quickly released to the public. The academic circles were the first that could experiment with the new technology (Boswell et al 2003). Soon after that, it became a germ of the Internet. The potential of TCP/IP was impressive. There was created a great number of new services taking advantage of the new protocol stack (Boswell et al 2003). Despite its great functionality TCP/IP was soon proved to be missing security measures. Apart from ordinary users Internet begun to host a new black hat community of crackers (Pipkin et al 2002). Since then, members of this group keep exploiting flaws in the design of the TCP/IP protocol stack. Due to a great number of new malicious code, exploits, etc, in order to keep functionality of Internet services secure, scientists and organizations were forced to conduct intensive work in the area of security.

After release of IEEE 802.11i, there was introduced a new term in wireless communication - Robust Security