Managing Risk and Security in Outsourcing IT Services

Onshore, Offshore and the Cloud

Frank Siepmann,

CISM, CISSP, ISSAP, NSA-IAM, NSA-IEM

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20131023

International Standard Book Number-13: 978-1-4398-7909-2 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Contents

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Foreword

I think that Frank does a great job of discussing outsourcing and his insights for areas to watch out for. He is dead-on with many of his observations, having been working with outsourced environments myself for a number of years. I appreciate his frank observations (pardon the pun!) and direct style in approaching the issues—in other words, he calls them as he sees them. The information on the different countries, albeit somewhat lengthy, provides a great perspective as to what is going on in the world and why it is so important to know who and what country you are dealing with. I also like the way that he moves into the cloud from outsourcing and shows the similarities. The latter section describing the controls, comments, and questions mapped to ISO27002-type requirements is very good as well. I also like the way that the book finished up with anecdotes to illustrate that these issues are real.

—Todd Fitzgerald
Global Information Security Director
Grant Thornton International, Ltd.

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Preface

Since the early 1990s, outsourcing has had a large influence on various industries in the Western world. Outsourcing companies have attracted industry giants such as Ford, GE, and Siemens, just to name a few, with promises of better expertise and significant cost savings. Now approximately 20 years later, not all of those promises have been kept. Organizations have learned their lessons—outsourcing is not a silver bullet. Some political and economic dynamics have resulted in a shift in how outsourcing is perceived. One of the areas of concern with many outsourcing customers is the level of security and privacy of their data. Now with cloud computing becoming a standard in modern IT environments, the picture has become even fuzzier. Many security experts are raising the flag regarding security and privacy in outsourced cloud environments. This book was written with the intent to help the manager who is challenged with an outsourcing situation, whether preparing for it, living it day to day, or being tasked to safely bring back information systems to the organization. It provides guidance on how to ensure that security and privacy can be achieved during an outsourcing situation. I have worked in the consulting and outsourcing industry for more than 15 years, leading medium- to large-sized security organizations and teams. I learned over the years that many risks can be addressed when there is a much broader understanding of a situation than just the technical aspects.

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Many factors can play into the success or failure of an outsourcing initiative. This book provides not only the technical background but also some broad information about outsourcing and its mechanics. Organizations sometimes try to resolve their issues of an expensive, fragmented IT infrastructure by looking into outsourcing. If this is truly a valid strategy, then it is heavily relying on circumstances and individual factors specific to that organization. Yet there are some common pitfalls that should be kept in mind before jumping to the conclusion that outsourcing will provide cost savings and a smoother-running operation. One critical factor for a smooth-running IT operation is a governance framework, resulting in mature processes, an executable IT strategy, and an IT environment that is maintainable. Most organizations that lack mature processes have to support an IT environment that ranges from Windows to three different UNIX flavors. Those environments are usually not sustainable in the long run, outsourced or not. To believe that outsourcing such an environment would result in cost savings and better performance can very quickly turn into a big disappointment. Yes, a large outsourcing company will certainly have the resources to support the various platforms and technologies. However, the more individuals an outsourcing company needs to provide to support a customer's environment, the higher the cost will be. Labor cost is the expensive part of the outsourcing equation, even delivered from low-cost countries like India and China. The leading outsourcing countries in particular have a common trend: the cost of living is rising, resulting in higher labor costs, making cost savings a short-lived dream.

That cost savings and security traditionally do not go hand in hand should be no surprise to anyone. Let's be clear: cost savings can be achieved in outsourcing if security is done right. However, the typical large-scale outsourcing engagement does not have security as the primary objective, but cost savings.

Definitions

This book uses for the purpose of standardization, whenever available, the definitions set by the US National Institute for Standards (NIST). Particularly in the fast-moving market of outsourcing, companies have come up with their proprietary marketing terminology, trying

to distinguish themselves from their competitors. Looking under the "hood" of such proprietary offerings, they usually are easily tied back to the NIST definitions and standard industry terminologies.

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

3

Before You Decide to Outsource

The question "What are the risks?" is not easily answered and has more aspects to it than just from a security perspective: for example, how agile does my IT need to be to support our business? Companies that need flexibility in how IT supports their business will have a hard time finding an outsourcing company that actually can (and I mean not one that only commits to it in their Statement of Work) keep up with their demand for the ever-changing IT infrastructure. Reality is that changes to the IT infrastructure have now another bureaucratic layer, when outsourced, in the form of Service Level Agreements (SLAs), contract terms, change orders, and so forth. This is widely underestimated and maybe even ignored by managers that make the final decision to outsource or not.

Outsourcing is like giving up a hand-tailored suit that fits like nothing else. Most companies will not achieve this "right fit" by outsourcing parts or all of IT. It might result in a more mature IT environment with less cost, but it needs to be understood that this will be more akin to the suit off the rack with some slight modifications than the handmade IT-Armani suit that every chief information officer dreams of.

Security and Privacy Impacts

When outsourcing business processes or IT, security is impacted at various levels. Information that used to reside in a controlled environment, physically as well as logically, is passed on to a third party that is now entrusted with protecting the information against unauthorized access and corruption (intentionally or unintentionally) and with making it available to the business whenever it is needed. To add to these requirements, now your organization needs to make sure

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

that the outsourcing company is trustworthy and executes as agreed on in the contract both parties signed. Critical pieces of information that ensure that your organization is competitive (e.g., the Coca-Cola recipe) or your personnel files with Personal Protected Information (PPI) are now accessible by the outsourcing company's personnel. Information that is protected by laws and regulations in various states and countries around the globe becomes an SLA with the outsourcing company. The level of criticality of particular information is maybe passed on to the outsourcing company in a signed contract, but down the road the information is just one piece among many. Furthermore, the outsourcing industry has adopted a model of cascading outsourcing that has resulted in some of the services not being provided by the original outsourcing company but by a third party that the outsourcing company has contracted to provide certain services to the outsourcing company. This third party might have another fourth party that provides services to them involving your data. It is very unlikely that those additional service providers understand your requirements for security and privacy of the information that you entrusted to the original outsourcing company. This results in a situation where nobody can understand the complete picture anymore. Information that should have been hosted only in the United States suddenly winds up in India or other countries. With the introduction of cloud-based outsourcing offerings, this situation has now become even more complex since many cloud service providers (CSPs) use technologies that allow for cloud bursting, which can mean that additional cloud resources are added from other geographical regions. Cloud bursting can also mean that your private cloud suddenly has resources added from a public cloud. The visibility to the information owner is taken away more and more.

Secure Communication

The sooner you think about secure communication in the outsourcing deal, the faster you get one of the biggest information leakage areas under control. Communication is going to take place at various levels of the organizations and in various formats. Phone, e-mail, instant messaging, paper, and videoconferencing are just some of the modern ways that we use to communicate with each other. The problem is that

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

those ways of communicating are not always secure. Particularly after the revelations of Edward Snowden, who was not the first, pointing out that globally there are governments eavesdropping on all forms of communication. The PRISM program is probably the most famous, controlled by the National Security Agency (NSA) however, it is not the only program in place. I say this because with outsourcing deals the communication takes place at a global level. Only if both endpoints and the communication channel are secure can the information that is communicated stay secure. Secure can mean it stays confidential, or the integrity of the information stays intact, or the communication can take place and is available to you.

Telephones

The telephone is one of the oldest forms of communication. In the early days of telephone service, so-called party lines were in place. A couple of neighbors shared one phone line. It was expected that when a party realized that the call was not for them, they would hang up. So much for that theory. In reality human curiosity resulted in neighbors sometimes listening to each other's conversations. Not to mention that the operator who had to manually patch calls through could easily listen in to calls. Nowadays we have telephone service nearly everywhere. Landlines are dying a slow death with a generation of college graduates simply relying on their mobile phones and having no need for a landline anymore. Times have changed, but not human curiosity or the fear of missing out on a detail that could be terrorism related or in some cases be used for corporate espionage. So-called signals intelligence (SIGINT)-gathering systems are capable of gathering information from satellite communication, microwave links (as used by telephone companies to bridge long distances), wireless services (cell phone service) and cordless phones. ECHELON is one system that performs SIGINT by collecting and analyzing worldwide communication. The ECHELON network is operated on behalf of five countries (Australia, Canada, New Zealand, the United Kingdom, and the United States) according to the UKUSA Security Agreement.* ECHELON was originally created to monitor

* http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml.

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

the military and diplomatic communications of the Soviet Union and its Eastern Bloc allies during the Cold War in the early 1960s. The European Parliament formed a committee during 2000 and 2001 to investigate ECHELON and issued a report in 2001. The report stated that the ECHELON is used in a number of contexts but that evidence indicates that ECHELON stands for a signals intelligence collection system. This investigation uncovers an interesting situation with the UK, which is part of the European Union (EU) and is also actively involved with ECHELON. It is suspected that the five member countries have divided up the monitoring responsibilities.

- **Australia** eavesdrops for communication that originates in Indochina, Indonesia, and southern China.
- **Canada** used to monitor the northern portions of the former Soviet Union and conducted sweeps of all forms of communication that could be picked up from embassies around the world. After the Cold War era ended, the focus shifted to monitoring satellite, radio, and cell phone traffic originating from Central and South America to track drugs and nonaligned paramilitary groups in that region.
- **New Zealand** is targeting the western Pacific with listening stations in the South Island at Waihopai Valley and on the North Island at Tangimoana. Locals hold regular protests against the listening posts, demanding that they be closed down.
- **United Kingdom** is responsible for monitoring communication in Europe, Africa, and the European part of Russia. There have been cases in which companies located in non-ECHELON participating countries suspected that the ECHELON system was used to provide UK- or US-based companies a competitive advantage by passing recorded information to companies in their countries.
- **United States** monitors most of Latin America, Asia, Asiatic Russia, and northern China.

The report issued by the EU also concludes that ECHELON was capable of eavesdropping on and analyzing telephone calls, faxes, e-mail, and other data traffic that traverse via satellite transmission, microwave links, and public-switched telephone networks (carrying Internet traffic during the early stages of the Internet revolution). It has been suspected

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

for quite some time that ECHELON is used not only to protect the national security of the five member states but also for industrial espionage. Germany's national intelligence agency, Verfassungsschutz, has warned German businesses and the German industry community against ECHELON since June 1999, when it recommended that German companies encrypt all important information—encode it to prevent ECHELON stations from picking up the communication and using it to their advantage. The Verfassungsschutz even issued in 2008 a brochure* to German companies providing guidance on how to protect sensitive information, not mentioning ECHELON but clearly stating that communication can be eavesdropped on.

e-Mail

In the early days of e-mail communication, the e-mail servers exchanged the content of e-mails in clear text across the Internet. Since these early days, this has changed, and many e-mail servers now offer secure transmission of e-mails via the Transport Layer Security (TLS), the successor of the Secure Sockets Layer (SSL) protocol. This allows for secure communication between e-mail servers. To check if TLS is in place, you can inspect the full-header of an e-mail that contains the server handshake part. If the header contains a line like this (or similar—the keyword is TLS), "(version = TLSv1 cipher = RC4-SHA bits = 128/128)," then TLS version 1 was used to secure the communication from one e-mail server to another. One caveat to the above line, the RC4 cipher† is no longer considered secure, and an e-mail server should not use the RC4 stream cipher algorithm anymore. A prominent victim of the weakness of RC4 was the Wired Equivalent Privacy (WEP) protocol that is nowadays considered highly insecure. Too often individuals (particular auditors) seem to check only for the word TLS in the header of an e-mail and do not actually pay attention to the actual cipher that is being used. With computing power doubling every two to three years (see Moore's

* http://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-spionage-und-proliferationsabwehr/broschuere-4-0806-wirtschaftsspionage (in German).

† http://www.schneier.com/blog/archives/2013/03/new_rc4_attack.html

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

law*), a weak crypto algorithm can easily result in no obstacle at all after just a couple of months or years.

In the United States and in Europe, the governments are actively discussing the storage of information about communication that takes place using e-mail, social media, or telephone. The approaches that the EU and the United States are pursuing vary. The EU approach in general only requires the storage of envelope information of an e-mail but not the actual content of the e-mail. The actual interpretation and implementation of the EU directive have varied by country. The United States, on the other hand, has implemented measures that go beyond what the EU has defined. After the 9/11 attacks, a shift took place in how anonymity and privacy of e-mails are handled in the United States. Intelligence agencies have been using intelligent software that can screen the content of millions of e-mails with relative ease (e.g., NSA's XKeyscore† goes even beyond e-mails). Civil rights activists heavily criticize the practice of screening e-mails. Agencies such as the US Federal Bureau of Investigation conduct screening operations regularly. The American Civil Liberties Union and other organizations alleged that Verizon illegally gave the US government unrestricted access to its entire Internet traffic without a warrant and that AT&T had a similar arrangement with the NSA. In 2008, Congress passed the FISA Amendments Act of 2008 (FAA) granting AT&T and Verizon immunity from any prosecution. According to a whistleblower (William Binney, a former NSA employee), the NSA has collected over 20 trillion communications, including many e-mail communications.

Mobile/Cell Phones

As already mentioned in the telephone section, governments around the world are spying on wireless and wired communication, no matter where you are. Since the new millennium (potentially earlier), companies like ThorpeGlen, VASTech, Kommlabs, and Aqsacom sell so-called passive probing data-mining services to governments around

* http://www.merriam-webster.com/dictionary/moore's%20law

† http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

the world, according to a *London Review of Books* article.[*] For example, ThorpeGlen, a UK-based vendor, provides mobile phone location and call records via its data-mining software. The sky seems to be the limit when it comes to analysis of data gathered: a target's community of interest, a single person swapping SIM cards, or even throwing away phones—no problem.

Smartphones

The success of smartphones around the globe is unprecedented. Particularly the younger generation has adopted this new technology, using it wherever they can: e-mail, text (SMS), one-time access code applications, and so forth. Unfortunately, smartphones have become the target not only of criminals but also governments, which want to control any information that might go against the regime in that country. Western countries use "government spyware" on smartphones, too. One company that has tapped into this market is Gamma International, a UK-based company marketing a spyware called FinFisher, under the description "IT intrusion and remote monitoring solution." FinFisher is supposedly only offered to law enforcement and intelligence agencies to covertly monitor criminals. However, according to researchers, it has been used by repressive regimes, for example, by the Bahraini government to spy on dissidents. According to some analysis, a demo version of the FinFisher software was in some cases reverse-engineered to a certain degree removing the demo mode limitations. FinFisher is available in versions that work on mobile phones of all major brands. FinFisher has the ability to take control of target smartphones and capture even encrypted data and communications. Using "enhanced remote deployment methods" it can install software on target smartphones.

FinFisher is, at the current time, the crème de la crème of spyware for smartphones (and computers). However, many other security issues might put your sensitive information at risk. For example, in late 2012 a research team at the University of Leipzig, Germany, discovered that the SSL implementation,[†] used by many applications on the popular Android platform, is insecure.

[*] http://www.lrb.co.uk/v30/n16/daniel-soar/short-cuts.

[†] http://www2.dcsec.uni-hannover.de/files/android/p50-fahl.pdf.

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

In another case, free smartphone applications that were using an advertisement framework to generate revenue for the usage of the application were introducing malware through the advertisement framework.*

Many other threats make smartphone platforms potentially unsuitable for highly sensitive data.

BlackBerrys

Probably still the most secure smartphone platform available is the BlackBerry. Even Research in Motion (RIM), the manufacturer of BlackBerrys, had to give in to demands from the Indian government (and others) to allow it to eavesdrop on communication taking place using the BlackBerry encryption. RIM demonstrated in August 2012 a solution developed by a firm called Verint that can intercept messages and e-mails exchanged between BlackBerry handsets. This solution makes encrypted communications available in a readable format to Indian security agencies. Many experts doubt the validity of the claim of the Indian government that it uses the eavesdropping to identify terrorism. It is suspected that the Indian government uses the intelligence gathered from the business-to-business communication (this is the only communication that RIM had encrypted) for other purposes.

Instant Messenger

It is not a well-known fact that instant messaging (IM) predates the Internet. Early versions of instant messaging appeared already in multiuser operating systems like Compatible Time-Sharing System (CTSS) and Multiplexed Information and Computing Service (Multics) in the mid-1960s. Later when network connectivity became more widely available, some new protocols came up, some of them using peer-to-peer protocols (e.g., talk, ntalk and ytalk) and others having a client-server architecture (e.g., Internet Relay Chat [IRC]). Many IM solutions followed. However, America Online (AOL)

* http://www.csoonline.com/article/732204/bogus-ad-network-marks-new-twist-on-android-malware.

offered the first IM that had huge success, with millions of users still using it today. The AOL Instant Messenger (AIM) has been leading the way for modern IM solutions (Google Talk, Yahoo IM, Microsoft Messenger, etc.) offering not only a text chat function but nowadays also voice chat, video chat, and file transfer function. As useful as IM solutions are—boosting productivity, particularly for teams that are geographically dispersed—they also carry a high risk if they are implemented by using one of the public IM offerings (Yahoo, AOL, Microsoft, Google, etc.). The following could be considered the top five risks and liabilities:

- **Malware infections through IM**—IM networks have been used to deliver large numbers of phishing links (i.e., URLs) and file attachments containing malware. Even if your computer is not the direct target of an attack, the user around the globe could not run antivirus software on their computer and would get infected with malware.
- **Compliance issues**—In the United States alone there are more than 10,000 laws and regulations related to electronic communication and records retention. Some of the well-known ones include the Sarbanes–Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and SEC 17a-3 requiring that certain exchange members are required to create records in a certain way. For example, in December 2007 the Financial Industry Regulatory Authority (FINRA) issued to member firms in the financial services industry a clarification stating that the terms *electronic communications*, *e-mail*, and *electronic correspondence* may be used interchangeably and do include electronic messaging as instant messaging and text messaging. This ruling states that companies that are required to be in compliance with it record IM and text messages since many IM communications fall into the category of business communications, which must be archived and retrievable according to SEC 17a-3.
- **Requiring additional ports**—Unfortunately, due to the nature of IM, running behind firewalls, or on networks using network address translation (NAT), the programmers of some

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today

IM applications have been creative in keeping a communication channel open to the IM server. This sometimes involves the User Datagram Protocol (UDP) network protocol. UDP is not known for its security and allows for spoofing of communication sources.

- **Social engineering**—Just like the traditional form of social engineering, IM has been used to claim the identity of someone to gather information. Sometimes the IM name varies by only one character, using the limitations of character sets. For example, I and 1 or O and 0 are often swapped for each other to create an IM name that on the first glance looks like the name of a trusted person.
- **Leakage of confidential information**—IM applications usually use communication protocols that are in plain text, making them vulnerable to eavesdropping attacks. Another area of concern is that many IM protocols are not peer-to-peer protocols but traverse through servers of the company offering the free IM solutions. There have been many speculations why this is being done since it creates a cost overhead for the company offering the free service to the public.

IM has been widely used by outsourcing companies; however, the risks that the usage of IM introduces must meet up with your risk appetite and compliance requirements.

Letters and Parcels

The old-fashioned way to transport information from point A to point B, using a carrier that provides tracking of your shipment, can give you a false sense of security. Yes, you know where your letter or parcel is; however, tracking does not help much when the letter or parcel has been delivered to the wrong address and the signature is completely unreadable or no signature has been recorded. In most cases international shipments require additional paperwork, such as customs forms that need to be filled out. In some countries, parcels or larger envelopes are routinely opened and inspected. Those inspections serve different purposes, depending on how stable the regime is in a certain country.

Managing Risk and Security in Outsourcing IT Services: Onshore, Offshore and the Cloud
Frank Siepmann
ISBN 9781439879092 (Print)
Excerpt for IT Today