the missing link

the Information Security Officer

Michel Nolf
Information Security Officer, Certified CISM, CRISC

Business
Services
orange™

executive summary

In today's world, a growing number of companies contract out part of their IT to external suppliers in the form of cloud, outsourcing and even managed services. Whatever the method, the result is the same: someone else takes care of your devices or applications.

Many articles address the security issues of cloud services; however, few of us realize that the same arguments also apply to other kinds of outsourcing.

In this article, we will go through some of the challenges posed by allowing an "outsourcer"[1] to take over a part of your IT infrastructure. We will see that whatever the form – cloud, outsourcing or managed services – the challenge of managing risks and security in a heterogeneous environment remains the same. This challenge is often a show stopper, but a few good habits and timely requirements on the part of the outsourcer can help significantly.

Many aspects come into play with regards to outsourcing, beginning with the current security posture[2] of the client, all the way to crafting appropriate strategies to keep – at the very least – the same level of risk. The choices are many. You can choose a fully-dedicated environment in which you dictate your own views on security, or you can use a public environment in which you accept the default setup. Outsourcing can also be the perfect opportunity to increase your level of security and can even be the trigger for it.

Over the years, Orange Business Services has developed a deep understanding of outsourcing issues. We've run managed services for WAN, LAN, voice, call centers, security and telepresence for many clients in many industries, including banking, chemicals, insurance and governments. We've provided managed services for some, while taking over entire infrastructures for others. Based on our experience, we feel that a new role in the outsourcing arena is needed, especially for large enterprises.

The client and the outsourcer both run their own security departments. They also have their own business teams managing projects. Within each team, someone must understand the business being outsourced, the security requirements associated with it, and how all those aspects translate into the outsourcer's environment. The leading member of the outsourcing team must be able to identify potential gaps, run a risk analysis on those gaps and come up with solutions. We call this role the "Information Security Officer."

The Information Security Officer, because of his understanding of both the client and his own company systems, tools and processes, plays a pivotal role during the implementation of the project as the gatekeeper on security rules: guiding implementation teams; defining security processes, like user management; and acting as the final approver of the proposed infrastructure. The Information Security Officer also performs internal audits and facilitates audits requested by clients. He is the ideal person to perform risk assessments and even run full risk management programs. And, because of his deep understanding of both parties and of the design and operations of the security infrastructure, when incidents do occur, the Information Security Officer is the best person to help resolve them.

[1] Throughout this paper, the term "outsourcer" refers to the supplier or vendor of outsourcing services to a client.

[2] The security posture is a concept representing the level of security controls regarding risks that a company is willing to accept.

contents

today

It is widely acknowledged that IT is becoming more and more complex. The time is long gone when a single individual could pretend to master an entire technical solution. The Internet brought power to PCs and servers, relegating mainframes to historical curiosities. Decentralized applications or client-server models have become the norm. Smartphones and tablets are pushing mobile computing to a new era.

But technology is not the only sector that has drastically changed. The way we do business is very different now than it was ten years ago. Our partners in one area are often our competitors in another, and governments have a more prominent role through laws and regulations. Large multinational companies must address these changes and so must their clients and partners.

Cloud, too, is affecting the way we provide IT solutions and how we translate business needs into technical solutions. Everybody wants to pay less and have a flexible IT infrastructure that adapts itself to business fluctuations.

User behavior is changing, as well, through mobility. We go from meeting to meeting with our mobile devices in hand; we keep in touch with colleagues while in airports and on public transportation. People want to work from home and hotels just like they do at the office. They want to choose which devices to use without cumbersome permissions. And they want to communicate using all sorts of vehicles, like instant messaging and social media, sometimes challenging their own company's confidentiality rules.

In short, in the last 20 years everything has changed, from user behavior, to the way IT is implemented.

Somewhere in the middle, the Chief Security Officer (CSO) is assigned the task of managing the security risks associated with these changes and must come up with appropriate solutions to alleviate them. How does he do it?

The CSO must understand the legal frameworks of all the various countries in which his business operates. In some cases, security certifications are required to run the business; in others, they are necessary to forge a relationship of trust between partners and clients. The CSO also needs to master a variety of technologies, including WAN, LAN, servers, PCs, tablets, operating systems, databases, enterprise applications, internal applications, etc., even coding and scripting languages. He needs to know how IT systems are developed and tested and how they could be attacked. The CSO is constantly warned of attacks and vulnerabilities via mailing lists, and he has to know if the warnings apply to his environment. But all of this knowledge is useless in developing a sound security policy if he doesn't first have a good understanding of the way business is done in his own enterprise. The CSO must adapt his security strategies to the risk appetite of his enterprise and ensure that all technical solutions support the way his business is run. He must also be aware that no single solution will solve every issue.

is the CSO superman?

Most people would agree that these requirements are too many and too difficult for a single individual to master. Fortunately, most CSOs can rely on teams of experts for help. System administrators will translate high-level policies into technical procedures. Network experts will comply with the security rules of the company. Internal auditing will check for compliance. And, at the end of the day, a full set of technical and business experts will also help the CSO make educated decisions and translate them into technical or business countermeasures.

However, this picture is of an ideal world. In reality, people who support the CSO have their own constraints and goals, and those are not always aligned with the security and risk management targets. Users want to have access to internal systems and confidential information from anywhere. Developers need to roll out their applications on time to support new products and will do what they need to do in order to make that happen. Security is very often not considered, no matter what the company's policies are. As a company relies more and more on external suppliers to manage a part of its IT[3], every player should be aware and aligned with the strategic security view of the CSO. This was a difficult task when the CSO had to rely on internal resources for IT management, but it becomes a real challenge when IT is externalized to one or more parties.

[3] Companies pretending that they do not outsource at least part of their IT are hiding the truth from themselves: what about their WAN, their phone lines and their Internet providers? Outsourcing can be a simple Web server to full IT outsourcing.

how to secure an outsourced project – the client aspects

knowing the current situation

Before starting an outsourcing project, it is best to evaluate the current security controls and the risks that they mitigate. This will allow you to duplicate the controls that are working and replace those that are not, in order to maintain the same level of risk. In very rare instances, the current situation is unknown or too complex to be understood. In those cases, outsourcing can be the catalyst to improving security and setting the foundation for a good security approach for critical business processes.

In all cases, internal security policies, regulations and local laws are critical in painting a precise picture of what the business's overall security should look like in an outsourced environment.

Outsourcer management is often neglected. Some companies outsource different parts of a project to different suppliers. For example, they outsource a telephony infrastructure to one company and the WAN to another. When they do this, the company must ensure that the same level of security is requested and delivered by both outsourcers. Establishing clear communications between the various outsourcers and also between the internal departments that deal with the outsourcers is critical. Although this sounds straightforward, when an incident occurs or a large set of changes are requested, problems that could have been avoided often surface. We've found that when Information Security Officers are part of regular security meetings with clients, those issues are often circumvented.

responsibilities

The RACI model, a relatively straightforward tool that can be used for identifying roles and responsibilities during an organizational change process, is well known but rarely used. A RACI matrix, however, is not only crucial in an outsourcing project, but should be completely explicit. Outsourcing companies deal with IT, not with business, so blurred areas can be common and must be avoided.

understanding what is outsourced

As mentioned above, the as-is state of security controls must be understood before an outsourcing project is undertaken. In addition, you also need to be aware of the processes that will be affected by the outsourcing project.

For example, how do you control access management if you do not receive notice of persons leaving the company or changing roles? And how do you prove to your own auditors that the process is fully managed?

The incident management process is, of course, also affected. You must ensure that security incidents are detected by your outsourcers, that they are correctly evaluated, and that they are reported to you in a suitable timeframe. Incident management can have very diverse impacts, including legal and operational. Therefore, you need to ensure that the outsourcers' obligations are clearly stated and determine whether or not the outsourcers have any legal constraints that are incompatible with your business.

Internal incidents must also be considered. To analyze internal incidents, the security department may need information that is in the hands of outsourcers. You should ensure that your security team can access those logs within a reasonable timeframe and identify the individual(s) within the outsourcers' organizations who can understand the issues and take the correct actions.

the outsourcer: constraints and challenges

challenges

When developing products and services, an outsourcer will select a set of security controls – technical, physical and organizational – that will apply transversally to all of the outsourcer's services. This approach creates a baseline for all of the outsourcer's clients. Trustworthy outsourcers create a strong baseline and spread the cost of security throughout its client base.

You should understand your outsourcer's baseline and request additional security if your project or business requires it. The outsourcer will then develop a personalized service that satisfies your needs.

At Orange, we've already developed a complete offering with very strong physical security controls. We see the role of the Information Security Officer as primordial: he understands the business of the client and the operational environment of the outsourcer, and he can run risk analyses to determine if a specific environment is overkill or not.

In addition, many clients want guarantees regarding their outsourcer's security organization and operations. Security certifications can and do help in that regard. However, the certifications of the outsourcer must correspond with the needs of the client – it is useless from the client's perspective to have an outsourcer with an ISAE 3402 certification for remote access facilities if the client is not using that service.

legal issues

Legal obligations are a very touchy subject for outsourcers. Before entering into any outsourcing obligation, you should consider these questions:

- does your outsourcer manage private data? How?
- will your data be traveling between different regions of the world, having very different regulations?
- how can you access logs if your outsourcer manages them? How do you investigate specific instances? Are you certain that your outsourcer can and will maintain logs for your required timeframe? What happens at the end of the contract? Log retention and access deserve careful attention

If the outsourcer is providing you with a "standard" service, you must ensure that all of your legal requirements and obligations are met: you remain accountable in the face of the law.

Last, but not least, outsourcers may be subject to local laws that conflict with your business purposes or may impact the confidentiality of your data. If this is the case, you must ensure that the outsourcer is aware of this situation and puts in place mitigating controls.

audits

There are two kinds of audits in an outsourcing environment:

- audits performed by the client
- audits performed at the request of the outsourcer to obtain a security certification

client audit

When implementing an outsourcing project, you may subject the outsourcer to an internal and/or external audit. The requirements of the auditors must be clearly understood. When an environment is to be outsourced, extra controls may be requested. Some controls may disappear, some may be replaced. This means that when building the project, you must ensure that the outsourcer is able to provide the auditors with the correct information. If you are using a third-party auditor, you must request from the outsourcer the right to disclose sensitive information.

You may not always have the right to audit an entire outsourced environment. The shared environment is usually guaranteed by international certifications; however, if you've had a dedicated service built, it may or may not be included in the scope of the certifications. You should clearly state before signing any contract if you require the right to audit and which part of the outsourced services you desire to audit. The Information Security Officer can help to define these requirements at the beginning of the project and all the way through the audit cycle.

There are two forms of auditing. This first one, the "paper audit," can provide you with some basic assurances. During this audit, the Information Security Officer will align your security controls and policies with the outsourcer's policies and certifications. This simple approach is sufficient for non-critical outsourcing projects; however, more critical ones will require a physical audit. The rights and the conditions to perform this type of audit must be included in the contract.

security certification audit

Auditing has several drawbacks: each client must pay for the audit and each audit introduces a disturbance. Outsourcers will have a difficult time managing all the requests coming in from their clients: each takes time and resources and introduces disruptions within the audited environment. To avoid this and to reduce costs, outsourcers often apply for security certifications, such as ISAE 3204 and ISO 27001. These certifications provide proof to clients that the outsourcer competently manages security. The client should then ensure that the scope of the outsourcer's accreditation matches his needs. Sometimes, the accreditation covers only a small part of the outsourcer's environment and gives a false sense of security to clients. Also, the client should ensure that the certification is an international standard and that the auditors providing the certificate are reputable firms.

Obtaining access to accreditation reports is not easy: the documents are confidential and require a good understanding of the outsourcer's infrastructure and processes. The Information Security Officer can be an ideal resource to provide this information, however.

the missing link

This paper discussed the need for businesses and outsourcers to collaborate in the development and implementation of IT security. Security entails controlling, mitigating or managing risks, and someone must take responsibility for this.

At Orange Business Services, we specially train our consultants to be Information Security Officers, who act as a link between your business and your outsourcers to ensure that your security requirements are understood and integrated and that risks are eliminated or properly managed.

audit facilitator

The Information Security Officer is a critical component of audits. When you request an audit, the outsourcer must ensure that all resources are available at the time of the audit. The scope of the audit must be understood and agreed. The Information Security Officer may perform the audit of the outsourced environment himself, or he may act as a facilitator between you and your chosen auditors.

This role of facilitator is “natural” for the Information Security Officer. Not only does he understand the project and the outsourced environment, but he also has a good understanding of your business, the reasons behind the audit and what is really needed. By being a part of Orange Business Services, he also knows who to contact for the necessary information, either inside the project team or within the organization.

This three-way knowledge – the project, the client and Orange – puts the Information Security Officer in an ideal position to drive audits smoothly and ensure that security controls are in place.

security meetings

The Information Security Officer participates in security meetings with his clients. This ensures that all findings, corrective actions and requests are correctly pursued. He also contributes his understanding of the outsourcer and of the timeliness and feasibility of his clients’ requests.

processes

Many processes must be defined to facilitate the efficient collaboration between businesses. Our processes touch security areas, like user management and incident management, since any failure in those areas could have a dramatic effect for both the outsourcer and the client in an outsourcing project.

risk management

Risk management is a pillar of security management. The Information Security Officer is in the ideal position to identify and highlight risks that you may not be aware of. Additionally, many assumptions can be tested during the risk analysis program. Throughout the life of the outsourcing project, many changes will occur: new services will be implemented or you may contract with new partners. The world of security will also evolve: new technologies will be developed and new attacks will be deployed.

The Information Security Officer will be fully aware of how each of these changes might affect his clients' security solutions. He will assess the impact on the security of his clients' data and present correct and verified information regarding any new risks. He will also suggest solutions and potential mitigation actions.

conclusion

Whatever part of your IT or process is outsourced and whatever type of management (managed services, full outsourcing or the cloud) you prefer, the Information Security Officer is the only one who can ensure that all security aspects are fully considered and met. He is the only one with a 360° view of the project, your business and the outsourcer's company. This view allows him to provide you with the unique guarantee that your requirements are perfectly understood, that audits will be executed correctly and that incidents will be correctly and efficiently managed.

Having an individual Information Security Officer in an outsourced project guarantees that security will be managed in the way that you want it to be managed. At Orange, the Information Security Officer is also part of a community, which provides you with many more advantages. By sharing knowledge and experiences, solutions to specific issues are presented and improved throughout the community, so all of our outsourcing customers benefit from the experiences of others. The community also provides an efficient communication path with other departments. The net result is a set of security best practices and a continually enhanced role of the Information Security Officer.

about Orange Business Services

Orange Business Services, the Orange entity for business, is both a telecommunications operator and IT services company dedicated to businesses in France and around the world. Our 20,000 employees support companies, local government bodies and public sector organizations in every aspect of their digital transformation. This means we're at hand to orchestrate, operate and optimize: mobile and collaborative workspaces; IT and cloud infrastructures; connectivity (fixed and mobile networks, private and hybrid systems); applications for Internet of Things, 360° customer experience and big data analytics – as well as cybersecurity, thanks to our expertise in the protection of information systems and critical infrastructures. More than 2 million businesses in France and 3,000 multinationals place their trust in us. See why at: orange-business.com or follow us on Twitter @orangebusiness

Business
Services

orange™