



Can Outsourcing Lead to Bad Security?

An onslaught of internal and external security breaches over the last couple of years has forced organisations to rethink their security strategies.

Dwaine van Vuuren
Global Security Practice Lead
Dimension Data

This document explores the history of security outbreaks and the role outsourcing suppliers can play in coping with the advent of increased risk. It also provides recommendations on the proposed content of an outsourcing contract and guidelines for the selection of a partner.

July 2006

Contents

1. Introduction	3
2. History of security outbreaks	3
3. The challenge	3
3.1 Outsourcers deal with short-term issues	3
3.2 Lack of internal expertise	4
3.3 Increased threats	4
3.4 The network becomes a new target	5
4. Security shift	5
5. Outsourcing security	6
6. Outsourcing recommendations	6
6.1 Considerations for outsourcing security	7
6.2 Choosing an outsourcing partner	7
Glossary of terms	9

1. Introduction

Customers and outsourcing suppliers who engaged in the outsourcing boom three to five years ago are now facing significant security challenges.

When these contracts were signed, information security was not of paramount importance. There was no onerous legislation to comply with, and the debilitating virus outbreaks we suffer today were unknown. Globally destructive self-replicating worms and spyware were unheard of, and users were not faced with today's proliferation of mobile communication technologies or devices.

At that time, the typical organisation's network would be relatively simple, with a minimal number of entry points. The focus for both parties would be on cost-cutting, efficiency, connectivity service levels and agility. Information security was a simple equation: Security = Firewalls + Antivirus = IT Department.

The idea that more than 850 million people worldwide would be using instant messaging and peer-to-peer protocols to swamp organisations' networks with private conversations, shared music, movie and porn downloads in the not too distant future, seemed far-fetched.

2. History of security outbreaks

In almost all outsourcing contracts, information security was buried under all the legalese and traditional service options as a vague one-liner, usually with reference to the maintenance of Firewalls and AV. In fact, for all intents and purposes, information security as we understand it today was beyond the scope of the contract.

The reason for this is that before the advent of the Internet, e-mail and e-commerce, the closed nature of corporate networks made security a relatively simple affair. The classic security defence model revolved around defending a "trusted" internal network from the "untrusted" outside (ie everything else).

The demarcation line between these two zones of trust was called the "perimeter" and security products such as Firewalls, VPNs, etc., were implemented on the perimeter to enforce the trust differentials. A DMZ was set up on the Firewall for public-facing data. This represented the "Protection" security model when security was relatively uncomplicated.

3. The challenge

With the advent of the Internet and e-commerce and the explosion in popularity of these media, the "Protection" model worked for a short while, but then became increasingly powerless against viruses, Trojans, worms, application level attacks and malicious code entering the network perimeter through e-mail, file transfers, Web pages, P2P networks and VPN links.

3.1 Outsourcers deal with short-term issues

The first wave of virus outbreaks before Blaster et al were deemed to be infrequent occurrences. The outsourcer dealt with the diagnosis and clean-up exercises accordingly, as requested by the client. On subsequent occurrences the outsourcer would automatically start dealing with the issues, even when the issues were not related to their scope of work.

An example of this would be a WAN or LAN network outsourcer who would have to deal with virus issues at the endpoints, because they were considered to be a bandwidth or connectivity or infrastructure problem. The possibility that these issues would keep recurring - or that they would keep getting worse - was never even considered. The outsourcers were focused on service and their main aim was to resolve the issues of the day.

But this short-term fix of a growing problem would lead to a security crisis for organisations. These issues became more pressing and frequent as corporate networks became more complex; as they connected to more partners and suppliers and therefore had to make use of more contractors and the problems began to escalate. Security outsourcers started to deal with these issues as part of their normal business process and as a result, the client lost all visibility of the nature of the problem.

Organisations did not receive regular reports from outsourcing suppliers as to the frequency, scope and impact of the security incidents. Therefore, organisations were unaware of the looming issues. In fact, in some cases where internet abuse and viruses were sapping WAN bandwidth, the solution to the problem offered by outsourcers was merely to add more bandwidth. This may have suited many WAN outsourcers as they could then bill the client for the additional bandwidth.

Some outsourcers deployed IDS technology in the networks as a first proactive step. But they soon realised that this would not be a complete solution. What accelerated the scope creep was that all the new infections and problems were originating from within their clients' own trusted networks or from the clients' own trusted users. The outsourcers were managing the networks and/or users and therefore they had to assume the responsibility.

3.2 Lack of internal IT expertise

To exacerbate matters, organisations had scaled back their IT resources as part of the outsourcing contracts. The fact that security was not an important issue three to five years ago, coupled with loss of visibility of the growing risks, meant that there was seldom a consideration to have an IT security competency within the clients' staffing complement. The clients' IT staffing complement gravitated towards procurement and "outsourcer relationship managers".

3.3 Increased threats

It took the disruptive outbreaks of Blaster (aka W32/Blaster, LovSan, MSBlast, W32/Posa), SoBig, Nachi, Sasser and others to bring the security crisis to the top of the corporate agenda. Almost every corporation affected by these viruses rated the threat from malicious code as priority number one on their risk/threat management agenda. Many corporations were infected from within their own trusted network or from their own trusted users - this in spite of aggressive antivirus, IDS and other traditional security investments made by these organisations.

The reasons for this were the following:

- ▲ There were "zero day" attacks with no known signatures. IT managers would arrive at work in the morning to find that they had already been infected the evening before, for example, by the Far East, before antivirus or mail vendors released signatures.
- ▲ Contractors and workers with laptops that were infected elsewhere, infected the internal network when they connected to it.
- ▲ External VPN or remote access/wireless connections that terminated in the network core (bypassing DMZs and Firewalls) introduced infections.
- ▲ Traditionally "trusted", e-Commerce and business partners were used as launch platforms by malicious code to attack the customers' resources.
- ▲ Branch networks, that were not under the strict control of the central IT department or outsourcer were used as launch platforms against the central network and other branches.
- ▲ Patch management was not proving scalable as a defence mechanism due to the effort and frequency of the updates required and the shrinking window of vulnerability.

This cast into stark relief the fact that the traditional approach to protection and detection no longer applied.

The wave upon wave of mass network worms and virus outbreaks in 2004, tagged among the security community as "The Year of the Worm", were far more sophisticated and were starting to wreak havoc. Blaster and Sasser were so devastating that IT departments and outsourcers alike could no longer sweep compromised security issues under the carpet. The media were having a field day with the issue while the implications for organisations were dire. Finance departments, for example, could not access their mail or systems and point of sale systems were being brought down. It became apparent that bold new initiatives in network security would be needed to overcome the crisis.

3.4 The network becomes a new target

The last eighteen months have also seen a shift in the perception of the security issues that face networking infrastructures. For the first time, networking products have made it to the SANS Top 20 Vulnerability list, with Cisco's IOS getting specific attention. In the past there was very little attention paid to the possibility of security vulnerabilities in network infrastructure equipment being exploited. The demonstration given at the BlackHat symposium in 2005 has also contributed to the new perception of network infrastructure as being subject to security issues previously only dealt with in relation to servers and desktop computing resources. The research firm Gartner recommends that enterprises that run Cisco IOS pay close attention to IOS vulnerabilities, treat them seriously, and follow the guidelines within advisories to upgrade to a newer version of software at the earliest possible opportunity.

In the event of buffer/heap/stack overflow vulnerability exploitation, Gartner recommends that enterprises take immediate action to shield their network by implementing a layered defence, including network-based intrusion prevention technologies, to block exploits while executing normal test-and-patch deployment processes. The sheer amount of Cisco equipment installed, the many versions of IOS involved, the difficulties of upgrading IOS and the IOS vulnerabilities already out there or yet to be discovered present a major challenge to network administrators and security professionals. This is an aspect that needs to be reflected in outsource contracts, or if handled in-house, the amount of effort required should be recognised and planned for.

4. Security shift

All these developments resulted in widespread realisation that traditional Firewall and Antivirus technologies, as covered in original outsourcing contracts, were not able to withstand emerging threats such as self-replicating worms, port 25 (mail), port 80 (web), P2P exploits and Spyware, amongst others. And to compound the external threat, internal IT assets that were infected were infecting other internal assets.

A detection and response strategy within the perimeter was now required to supplement the ailing protection strategy. Many enterprises were also not aware that their insurance policies did not provide cover against malicious code attacks. Other companies who tried to buy coverage found there were few policies being written that protected against digital attacks.

The security industry experienced a very busy year in 2004. There was much piloting and testing of IPS and other appliances to solve specific problems. During this exploratory phase a key issue for outsourcers and their customers was the question of who was going to take responsibility for paying for the implementation of the technology once they were satisfied with the tests/results.

The biggest error made by organisations and outsourcers (and some technology providers and systems integrators who were also none the wiser) was that they thought that deploying this technology would solve their issues.

What they did not realise was that they were only solving particular issues, in much the same way as they had done when they invested in Firewalls, VPNs and antivirus software. While IPS appliances, Application Firewalls, host-IPS, desktop Firewalls and IDS were being installed, no-one considered the fact that security needed to be a holistic process involving people, process and technology.

Outsourcing contracts were modified to include the provision and management of additional security hardware at strategic points within the network. These measures repeated the mistakes of the past. They catered for short-term challenges, but did not make provision for long-term issues.

5. Outsourcing security

In response to growing concerns about security and the ever-increasing complexity of the management of these newly-installed point devices, many companies turned to the same companies who managed their existing network infrastructure, or to the emerging band of managed security service providers. This seemed the logical response for any company seeking to offload the complexities of security management and to alleviate the need for highly-priced technical talent.

The problem was that most of the contracts contained clauses in the fine print absolving the service provider of liability and accountability for security incidents. Many such contracts promised little more than notification of events which could not be confirmed as false positives. This level of service put the onus on the customer to respond to and resolve the incidents reported. In many cases, this caused extreme distress to unprepared clients in their hour of need, especially when these same service providers were able to assist in the incident response for additional hourly fees.

Outsourcing security has been a hot topic of debate for some time. There is a strong argument for both sides and no sign of consensus on the horizon. The facts are simple, yet overwhelming for many and include the following:

- ▲ Addressing security and IT risk is not optional.
- ▲ Legislation and liability are driving security to the top of CIOs' priority lists.
- ▲ There is a real awareness of the problem in bridging the gap between business people and the technologists.
- ▲ Technology is ever-changing; therefore security is a moving target.
- ▲ Good security resources are difficult to find and costly to hire and retain.
- ▲ Outsourcing security does not transfer accountability or liability to the service provider.

Regardless of whether organisations choose to outsource or go in-house for security, the challenge lies in getting executive support and alignment between the business units and the security function. At worst, these relationships are adversarial and conflict between groups results in a decrease in productivity. At best, the security officer understands the business and is able to communicate the threats to business operations clearly and show that effective risk management actually enables the business.

Many enterprises make the mistake of outsourcing their security as part of a generic outsourcing agreement before obtaining this alignment. The outsource then leads to a false sense of security or a "tick in the box".

6. Outsourcing recommendations

Organisations that simply cannot afford the investment in resources (both people and technology) need to be sure of the services that they are buying and specifically what exclusions are in their outsource contract. Frequently, outsourcers offer low bids to secure the business and then try to make up for it in change or out-of-scope orders.

It is a fact that organisations will need to continuously adapt their security practices to suit the ever-changing environment. Threats, vulnerabilities and mitigation procedures have changed dramatically over the years and organisations must be able to adapt their contract and the underlying security architectures used to keep pace.

If organisations have questions about the service level commitments or the verbiage in the contract, they should consult a trusted advisor. A technology partner, independent auditor or legal counsel can help them navigate the complexities. For international and multinational organisations, it is important to seek advice on compliance requirements in every individual country in which the organisation is conducting business, and to find out how their service provider is addressing those requirements. Once organisations understand what the outsourcer intends to do, they need to figure out how to fill the gaps.

6.1 Considerations for outsourcing security

Organisations should consider the following points when outsourcing security (either in its entirety or as part of a bigger infrastructure outsource contract):

- ▲ Note that compliance is the responsibility of the company, not the outsourcer.
- ▲ How does the service organisation's purchase enable them to better manage risk?
- ▲ What are the terms of the agreement? Check SLAs, limitations and exclusions. Organisations need to know exactly what they are getting for their investment.
- ▲ Be prepared to respond when incidents occur – this means that organisations need an incident response plan and someone to deal with the response. The contractor must support post-incident review.
- ▲ Verify that the outsourcer is compliant with all relevant legislation and verify the security procedures and best practices deployed by the service provider.
- ▲ Define security-related roles and responsibilities clearly and completely and specify clear security objectives in the SLA for integrity, confidentiality, availability, accountability and use control.
- ▲ Appoint a security officer, even if it is initially in a secondary role. The security officer should have a direct reporting line to an executive who is empowered to address tough questions and make decisions that impact the risk exposure of the company.
- ▲ Retain the ability to monitor and audit the outsourcer's environment to independently verify fulfillment of all the objectives and expectations.
- ▲ Ensure contract terms are flexible enough to allow for changes in a rapidly changing threat landscape, and to avoid being blocked by the organisational walls that outsourcing erects and the difficulty of anticipating all the contingencies in a contract.
- ▲ Measure contractor performance through security metrics such as number of incidents, time taken to respond to incidents, best practices, benchmarking, etc.
- ▲ Even if an organisation is using best practices frameworks such as the ITIL or CoBIT for SLAs, do not rely on these for security - use security specific frameworks such as ISO 17799:2005.
- ▲ Customers need to try and include infrastructure "Security Assurance Level Agreements" with their standard SLAs in outsourcing contracts in the future, and minimise the number of people managing the network components.
- ▲ The outsourcers' goal is to lock down and standardise to gain efficiencies and then sweat the assets. This is diametrically opposed to the adaptive nature required by modern day secure infrastructures.

6.2. Choosing an outsourcing partner

As applications such as Telephony, P2P and Microsoft Live Messaging rapidly converge onto the network infrastructure, security becomes more complex and important. In addition, the industry is faced with strong convergence of networks, systems and security management as companies like Microsoft and Cisco embed more security functionality into their OS and networking fabrics.

Network Access Control (NAC)¹ and other "Integrity Architectures" are emerging to take their place in the self-defending network of the future, which means configuration, identity and asset management are going to play larger roles in future managed, secure infrastructure. Also, infrastructure components themselves are subject to security vulnerabilities². Now the proactive "Assurance" management of those devices themselves becomes as important as managing standalone Firewalls and IDSs. This implies that enhanced configuration, security and patching management are going to play increasingly important roles in infrastructure management.

¹Cisco's self-defending programme

²CiscoGate: <http://secure-o-gram.blogspot.com/2005/11/ciscogate-landing-page.html>

All this means is that careful deliberation needs to be given to the partners used in outsourcing contracts. Organisations cannot have a situation where multiple parties manage the same devices to achieve their respective goals. This can defeat security objectives because too many people are involved.

Many MSSPs will insist on full device control to provide their services. This scenario was suitable for standalone Firewalls and IDS/IPSs, but will need consideration when the Firewall/IDS/IPS functionality becomes embedded into standard routers. The question of who will then manage the router bits and who will manage the security bits in that device becomes an issue.

Just as applications are converging onto the network, and security is converging into the network and applications/OS, outsourcing functions will converge. Customers will increasingly seek out systems integrators and outsourcers who have skills in network management, desktop and branch office life-cycle management, systems management and configuration management, in addition to world class security expertise. This may very well spell the demise of the boutique security shop or niche-managed security services player, over time.

Glossary of terms

AV	Audio and Visual
CIO	Chief Information Officer
CoBIT	Control Objectives for Information and related Technology
DMZ	Demilitarised Zone
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ITIL	IT Infrastructure Library
LAN	Local Area Network
MSSP	Managed Security Service Provider
OS	Operating System
P2P	Peer-to-Peer architecture
SLA	Service Level Agreement
VPN	Virtual Private Network
WAN	Wide Area Network