

0 1 1 0 0 1 0 1 0 1 1 0 1 1 1 0 0 1 1 1 0 0 1 1

A guide to:
**Outsourcing
network security**



1
0
1
1
1
0
1
0
0
1
0
0

about dns

dns is a leading provider of information security services in the UK. Our sole focus on information security provides us with the experience and expertise needed to provide security solutions to a wide range of public and private sector organisations throughout the UK.

Headquartered in Scotland, with offices in London and operating throughout the UK and Europe, dns provides security services across the full security lifecycle ranging from setting strategy and policy to design and delivery of secure infrastructure, service support and 24/7 management.

contact us

head office:
83 princes street,
edinburgh eh2 2er

london office:
16 st martin's le grand
london ec1a 4en

t: 0870 085 8555
f: 0870 085 8556
e: info@dns.co.uk



our services



A guide to: Outsourcing network security

table of contents

1	Introduction
2	The case against outsourcing
2.1	It will cost too much
2.2	We want to protect our in-house team
2.3	We don't want to lose control
2.4	It's a sensitive issue internally
2.5	We're not sure how to go about outsourcing
2.6	We've got the technology
2.7	We've got things covered 8 til 5
3	The case for outsourcing
3.1	We must protect the business
3.2	We want to save money
3.3	We don't have the skills in-house
3.4	We're concerned about compliance
3.5	It's a better way of managing risk
3.6	We want to focus on core strengths
3.7	The threat from worms and viruses is constantly changing
3.8	We want protection 24/7
3.9	We want simpler reporting
3.10	We want experienced people
4	Checklist

A guide to: Outsourcing network security

1 introduction

Nationally and internationally, the growing trend is for organisations to outsource management of their network security to specialists. There are many reasons for this – everything from the growing threat of security breaches to compliance concerns, cost issues and the difficulty of sourcing skilled internal staff.

Understandably, however, this is not a decision that organisations take lightly. Until the realities of managed security services are clearly explained, giving responsibility to a third party for your network security may feel like you are outsourcing control. And there may be other issues of concern, such as justifying the investment and wondering how to go about the outsourcing process itself.

The aim of this document is to address the key concerns that clients often voice to dns about outsourcing and tackle some common misunderstandings. It also provides an objective account of the range of benefits available from outsourcing network security – and what to look for in the company you outsource to.

Outsourcing network security is a decision few medium-to-large organisations can afford to ignore. This document will help you to decide if it is right for you.

This document will help you to:

- Explore the reasons why organisations resist outsourcing – and decide whether they apply to you.
- Determine the benefits that outsourcing could bring to your organisation.
- Provide a checklist to help you choose the right outsourcing partner for you.
- Gain an overview of the whole outsourcing debate for discussion with your colleagues and business partners.

2 the case against outsourcing

There are seven main reasons why organisations sometimes feel reluctant to outsource network security. Some (or all) of them may be familiar to your own organisation.

2.1 it will cost too much

Cost is often cited as a key reason why organisations resist outsourcing. The irony is that, for those who do outsource network security, cost savings very quickly emerge as one of the biggest benefits. Cost analysis should involve far more than simply looking at the fee to be charged by the outsourcing partner.

A guide to: Outsourcing network security

It should also incorporate the significant cost savings that will accrue internally from saving on staff time. A TCO (total cost of ownership) analysis will often demonstrate a spread of other costs attached to internal network security management that senior management may not be aware of. These can usually be eliminated by outsourcing – thus creating huge savings.

2.2 we want to protect our in-house team

Unless it is a necessary objective, outsourcing need not lead to staff redundancies. It is, however, a process that creates an ideal opportunity for reviewing staff responsibilities. By removing the time-consuming hassle and distractions of daily security management challenges, IT staffing resources can be deployed in more productive roles – adding value to the company rather than allowing key personnel to spend all their time firefighting.

2.3 we don't want to lose control

This is a common misconception. Outsourcing security management does not mean that a company is outsourcing control. Control remains firmly with the client and not with the security partners. Their role should be purely operational, defending the network as instructed and reporting back in whatever form and frequency the client demands.

2.4 it's a sensitive issue internally

IT security flaws are often the 'elephant in the corner'. People within an organisation know there are weaknesses but for various reasons, the issue is never tackled head-on. This could stem from a desire not to be seen criticising colleagues or it could simply be because another task always seems more urgent. Organisations may be reluctant to face up to this reluctance and address the issue with help from a third party. Yet a reputable company specialising in network security will always be able to improve a client's defences.

2.5 we're not sure how to go about outsourcing

This is another common factor holding people back – and a fear of not knowing how to approach the outsourcing process can encourage it to stay rooted at the bottom of the priority list. The solution, clearly, is to take advice. Industry analysts such as Gartner (www.gartner.com) can offer a wealth of objective information to get you started. Then, when it comes to assessing potential partners, set up site visits with some of their existing clients to see how the service works in reality. And put comprehensive service level agreements in place to measure the ability and deliverables of the companies concerned.

A guide to: Outsourcing network security

2.6 we've got the technology

Technology has advanced to such a stage whereby there are highly sophisticated software and hardware options for managing an organisation's security. **dns** makes full use of these. However, some organisations can fall into the trap of believing that this technology is enough on its own. It's not. Failsafe security also requires human analysis (see 3.10).

2.7 we've got things covered 8 til 5

Because standard business hours in the UK are 8am to 5pm, there is often an assumption that management of security services is not required outside these hours. It's an easy assumption to fall for but a wrong one. The threat to security is global. The Asian-based hacker does not work British business hours – nor for that matter do most British hackers. And if you wait until 8am for your staff to restore a system that has been attacked overnight, your network could be down for hours during the crucial 8-5 period.

3 the case for outsourcing

Our experience tells us that there are ten key drivers that lead organisations to embrace outsourcing of their security management. Some of them mirror the inhibitors already listed, others address different issues.

3.1 we must protect the business

This is clearly the key issue at the heart of network security – protecting your organisation from malicious threat. This is the main driver for many. Organisations can no longer afford to take risks with security. An expert third party will bring that additional tier of expertise to guarantee protection.

3.2 we want to save money

One of our clients (a large public sector organisation) estimates that they would need 8-12 full-time staff to do the work carried out on its behalf by **dns**. And that's only one of the cost savings that can be achieved through outsourcing. For instance, without 24-hour outsourced security, an organisation can start work in the morning only to discover its entire network has been taken down by a malicious attack overnight. We've probably all seen it happen. Then there are longer-term issues to consider. The cost savings available through protecting your data, reassuring your clients and meeting all compliance demands can make the difference between an organisation in trouble and an organisation that is thriving.

A guide to: Outsourcing network security

3.3 we don't have the skills in-house

Organisations usually don't have the necessary skill sets in place and recruiting the right people makes no sense financially. Selecting a partner to provide expert operational support therefore emerges as the logical solution.

3.4 we're concerned about compliance

Given the fall-out from the Enron scandal, this is a particularly big concern for US companies – and an increasingly important issue for the UK too. Security management is not just about protecting your network from malicious threats (essential though that is). It's also about meeting regulatory standards and providing tangible reassurance to your customers, suppliers and staff that the network is secure. A good managed security service will fulfil all compliance requirements.

3.5 it's a better way of managing risk

Risk management is an issue that a good network security specialist will be able to advise you on. Allowing your outsourcing partner to focus on this issue is invariably more time and cost-effective than attempting to manage it in-house. A third party is able to bring a level of expertise and a third-party perspective that will reduce both risk and cost.

3.6 we want to focus on core strengths

Outsourcing enables your IT team to focus on core issues. Security management is a time-consuming, challenging responsibility that often eats heavily into the time of employees and distracts them from other priorities. Compartmentalising that responsibility and removing the demands on staff for operational activities creates a helpful demarcation line that will deliver time and cost savings.

3.7 the threat from worms and viruses is constantly changing

As anyone reading the papers will know, the global threat from worms and viruses is increasing exponentially. Keeping on top of the rapidly-changing nature of these threats requires full-time expertise of the type that is usually only found with specialist managed security service providers.

A guide to: Outsourcing network security

3.8 we want protection, 24/7

Mirroring one of the inhibitors already covered in this paper (see 2.7), working hours are another driver towards outsourcing. The threat to network security is global; it never stops. Yet most organisations in the UK shut up shop in the evening, leaving their network vulnerable to attack throughout the night. dns Managed Security Services is manned 24 hours a day – something that few organisations could afford to do or would be prepared to manage internally.

3.9 we want simpler reporting

A professional managed security service will provide you with a centralised reporting service that keeps you fully up-to-date with the levels of threat to your organisation and what is being done to combat it. The clarity and simplicity of the data will keep you informed and in control without eating into your time. The reporting service is typically provided through a real-time ‘dashboard’ (a secure website) that can only be accessed by your nominated managers.

3.10 technology is not enough

Hardware and software is not enough on its own. Installing a bank of ‘whining devices’, whirring away in the background of your building, may provide reassurance at one level but, without 24-hour analysis from an expert team, it will not be enough to eliminate all threats. Effective security management requires people on the ground who are able to identify trends and spot behavioural threats. This is one of the big advantages you receive from a 24-hour service manned by experts.

4 checklist

To help you decide if outsourcing is appropriate to your organisation, here is a checklist of relevant questions. If you reply ‘no’ to more than one of these questions, outsourcing is almost certainly worth considering.

- Do you have the skills in-house to provide a failsafe managed security service?
- Are your IT security people fully on top (on a weekly basis) of the changing threats of viruses, worms and the behavioural patterns of malicious attacks?
- Do you have staff working to protect your network round the clock, 24 hours a day, or does the human element of the security blanket clock off with everyone else?
- Are your IT staff struggling to concentrate on key projects because of the growing demands placed on them by security threats?

A guide to: Outsourcing network security

- Are you confident that your current network security arrangements fulfil all compliance criteria?
- Have you carried out a total cost of ownership (TCO) study to work how much you are paying to manage your security internally?
- To find out more about the **dns** Managed Security Services (MSS), simply get in touch through the contact details listed on page two.