# Essential guide to information security

**Thinking in threes:**
Confidentiality, integrity and availability


© Managed Networks Limited 2012

Share this on Twitter Follow us on LinkedIn Follow us on Facebook

MANAGED NETWORKS

# Contents


| | |
|---|---|
| **Introduction** | **03** |
| **Thinking in threes** | **04** |
| 1: Starting with secrets | 06 |
| 2: Keeping it real | 12 |
| 3: Staying power | 17 |
| **Conclusion** | **22** |
| **Contact** | **23** |




© Managed Networks Limited 2012

# Introduction

Wherever you look there's another story in the media about information security. Whether it's £800m lost to state-sponsored hacking by an unnamed UK plc, or £90,000 fines for breaching confidentiality, there are big sums of money at stake. Government is taking cyber-security more seriously than ever before and so are regulators – the Information Commissioner's Office levied record fines in May 2012, and the European Union is proposing fines of up to 2% of turnover for data breaches.

Even if you don't get fined, poor information security can cost you money. Data breaches can drop your share price, lose you customers and trash your reputation. Hacking attacks can shut you down. Data loss and business interruption aren't just temporary inconveniences – 43% of businesses that suffer a disaster never recover.

Just because you have a firewall and take backups doesn't mean you're secure and protected. Information security (also called cyber-security or infosec) is a very broad topic; it touches every aspect of your business.

This e-book gives you the overview you need to understand what you should be doing.

If you would like to explore any of the topics in this e-book in more detail, please call us on **0800 783 6170** or email us at **infosec@mn.co.uk** for a no-obligation consultation.

**Data breaches can drop your share price, lose you customers and trash your reputation.**


© Managed Networks Limited 2012

# Thinking in threes





© Managed Networks Limited 2012

Share this on Twitter Follow us on LinkedIn Follow us on Facebook

# Thinking in threes

## CIA Triad

The security profession often uses the “CIA Triad” to focus discussions on infosec. This triad consists of:

1. **Confidentiality**
   protecting your information from unwanted disclosure
2. **Integrity**
   making sure your information stays accurate and complete
3. **Availability**
   keeping your data accessible and your systems working

We use this triad to remind us how broad the topic is, and how interwoven it is with all aspects of business operations. In this e-book we’ll look at each of these topics in turn.

## Risk Triad

The “risk triad” helps us think consistently about the risks we face and how to mitigate them:

1. **Threat**
   something that may affect the confidentiality, integrity or availability of our information
2. **Exposure**
   how vulnerable we are to that threat, and how likely it is to affect us
3. **Countermeasures**
   what we can do to reduce the risk from the threat

## Tools and Elements

Finally we need to think about the different elements of our organisation, and the tools we have available to protect our information – and our business – from the threats we perceive.

1. **People**
   the human factor; the origin of most threats and the best mitigation
2. **Technology**
   both problem and solution; the heart of the infosec issue
3. **Physical**
   door locks and CCTV; fire and flood; the virtual world depends on the physical world


© Managed Networks Limited 2012

MANAGED NETWORKS

Thinking in threes

# 1: Starting with secrets


© Managed Networks Limited 2012

We'll deal with Confidentiality first, as this is what most of us instinctively think of as information security. Confidentiality is about making sure that access to information is restricted to those who need it, when they need it. Not all information is confidential, and its sensitivity varies, but all businesses will have some information they are obliged to protect – like employee transcripts – and some they want to protect, like customer lists.

When thinking about confidential information it's important to work out what it's worth to you. That way you know what it's worth spending to protect it. Sometimes the value is positive – the information is worth something in the open market: research; market-sensitive financial information; prospect or customer lists. Sometimes it's negative – perhaps there's a potential fine for disclosure; perhaps release of the information would damage your reputation.

**When thinking about confidential information it's important to work out what it's worth to you.**


© Managed Networks Limited 2012

# Risks

The biggest risk to confidential information in your business isn't shadowy hackers or even physical burglary; it's your own staff. If your information has a high positive value – if it could be sold to a competitor, for instance – then you may need to worry about insider theft, but the main cause of confidentiality breaches is negligence.

Negligent release of confidential information happens every day; in some cases, it even makes the front page of the papers. The consequences can be very real: the Information Commissioner's Office can fine you up to £500,000 for breaching consumer confidentiality, for instance. The proposed EU regulations on data breach are even more stringent, and could result in fines of up to 2% of global turnover.

There are hackers out there actively trying to steal secrets; whether they're after yours will depend on how valuable your confidential information is. For most businesses, this is a far less probable threat than employee mistakes, but you shouldn't ignore it entirely. Remember, too, that the easiest way for a hacker to get the information he wants isn't to penetrate your IT security… it's to phone up and ask for it.

You do also need to think about viruses and malware, but we'll talk about these when considering integrity. There are real risks here to confidentiality as well, but the countermeasures are the same in both cases.

## So how do you preserve confidentiality?

**The proposed EU regulations on data breach are even more stringent, and could result in fines of up to:**


**of global turnover.**


© Managed Networks Limited 2012

# Countermeasures

## People

Have a clear policy about what information is confidential and who is supposed to have access to it. Make sure staff are aware of and constantly reminded about the need to keep confidential information secure.

Organise your information so that confidential and public information are segregated; that way there's no excuse for mistaking one for the other. Grade your confidential information sensibly, so that you focus your attention on the most valuable; if you over-secure, staff will find ways around your security measures in order to make their jobs easier.

Put proper management structures in place; make sure users with access to sensitive information are properly supervised. Where you can, make sure that no one person has access to everything; that way it would take people acting in concert to breach your confidentiality from the inside. Have proper procedures around information release for example, double-check destination fax numbers and ensure someone is there to receive the document, or use only signed-for delivery services for posting CDs or memory sticks. Supplement this with technologies like encryption, and where possible stay away from physical or postal transmission of information in the first place.

Make sure you have effective access control. Simple things like better password rules, frequent reviews of users' permissions and proper employment exit procedures all make life much harder for hackers and don't require any sophisticated technology.

Ensure staff are aware of "social engineering" – train them not to give out confidential information or network access passwords until they have properly verified the requestor's identity and need to know. Ask them to watch out for strangers and not let people 'tailgate' them into the building.

Train your staff to ask questions of strangers. Just because someone looks official doesn't mean they should be there. People are often shy of confronting others, especially in shared-access buildings; they must be reassured that it's their duty to do so. Make sure they're aware of shoulder-surfing and tailgating: reading over someone's shoulder and following someone through a controlled entrance, respectively. These are easy things to test, and you should do so.

**Train your staff to ask questions of strangers. Just because someone looks official doesn't mean they should be there.**


© Managed Networks Limited 2012

## Technology

Use technology to support your policy, not instead of having a policy. Many breaches happen because users fail to use the technology available to them; encryption for example – make sure you invest in training as well as technology.

Defend your perimeter – put in a proper firewall and make sure it's professionally managed. Lock down access from the outside to what is necessary and make sure you log activity and check the logs frequently.

Construct your network in layers, with your most sensitive information at the centre of a series of defences – for instance, don't put your public website on the same server as your confidential files. Make sure no services or systems have more access than they need.

Use encryption wisely; without careful thought it can either give the illusion of security or lock you out of your own data. Talk to your customers and suppliers and agree procedures between you for exchanging sensitive information securely.

**Use technology to support your policy, not instead of having a policy. Many breaches happen because users fail to use the technology available to them.**


© Managed Networks Limited 2012

MANAGED NETWORKS

## Physical

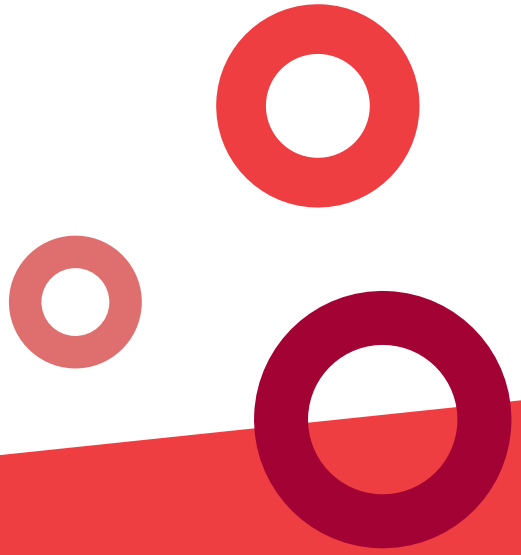
Don't ever forget about paper. Use policies to restrict printing, especially of confidential documents – you can tie this to environmental commitments to reinforce it – and control distribution of documents. Make sure staff who deal with confidential paper documents have and use lockable filing cabinets (and look after the keys properly) and have access to a shredder. Make sure that all confidential paper is shredded as soon as it's no longer needed. Enforce a clear desk policy to prevent sensitive documents being left out in the open.

Lock things up; make sure your servers are in a controlled environment – better still, move them into a datacentre, which will have much better physical security than your own offices. Don't leave USB keys and removable hard disks lying around – even if you've encrypted the data on them, it's better not to risk the one chance that someone forgot to encrypt, and in any case these things cost money in themselves.

Make sure your premises are secure; as with all security, organise your protection in layers so that an intruder faces a number of obstacles rather than a single checkpoint.

Take special care of laptops. Many data breaches result from theft or accidental loss of laptops, and the cost of the breach is many times the cost of the device itself. Combine policies: never leave your laptop unattended, hide it away at home and so on; technology: encryption, GPS tracking / phone home services, password lock whenever the lid is closed; and physical security such as security cables – almost all laptops have the relevant locking slot now - or lockable desk drawers.

**Make sure your premises are secure; as with all security, organise your protection in ayers so that an intruder faces a number of obstacles rather than a single checkpoint.**




© Managed Networks Limited 2012

MANAGED NETWORKS

## Thinking in threes

# 2: Keeping it real

Integrity is used in the security domain to mean keeping your information in step with reality; in other words, not just preventing data loss or corruption, but also ensuring accuracy and timeliness. As ever, there's much more to this topic than just protecting your data from external threats. You need to think about the whole range of information you maintain – not just documents and folders, but databases, staff lists, asset registers…


© Managed Networks Limited 2012

# Risks

## Another set of three:

Loss and corruption are the obvious risk, whether arising from intentional external agency, simple hardware failure or the whole range in between. Don't forget that one real issue with data loss or corruption is knowing that it's happened. The more data you have, the harder it is to tell if it's all still there, and all correct. Think of the damage a disgruntled employee could cause by going back and changing the details of historic orders, or changing the text in electronic copies of contracts. The main risk to businesses from viruses and malware remains the deletion or corruption of information – whether deliberate or as an accidental by-product of the impact of the virus on your systems.[1]

Loss of currency is the second of our three. Information that's out of date can be worse than information that's missing. If you have no phone number for a key contact, that's an obvious absence that can be remedied. If you have a phone number, but it's out of date, you won't know until you try calling it - at which point it may be too late. Think about supplier price lists, shipping and billing addresses, product specifications – these are all data, which can be dangerous if out of date. Bear in mind also that it's not good enough just having the up-to-date information; you also have to know where to find it. If you have multiple copies of a customer proposal on your system, how do you ensure that everyone is using the correct version?

The final risk is inaccuracy. It sounds simple, but as well as being present, and current, information needs to be right. It's all very well protecting it against inadvertent deletion or deliberate corruption, but this is only worthwhile if the right facts were recorded in the first place. Accuracy is both validity and completeness – the truth, the whole truth and nothing but the truth.

**It sounds simple, but as well as being present, and current, information needs to be right. It's all very well protecting it against inadvertent deletion or deliberate corruption, but this is only worthwhile if the right facts were recorded in the first place.**

[1] The risk from spyware – viruses and malware designed to breach confidentiality – is very real, and has had some high-profile exposure in the media recently. It's often associated with the term "Advanced Persistent Threat" which implies a sophisticated human agent specifically focused on using a variety of techniques to compromise your confidentiality. However, at the time of writing in May 2012 relatively few businesses are likely to be targets of an APT and most freely-circulating malware is aimed either at stealing consumers' log-on details to retail bank accounts and web services or at taking control of machines so that they can be used in spam and denial-of-service attacks.


© Managed Networks Limited 2012

# Countermeasures

## People

Don't give any one person complete authority to make changes; make sure at least two people are involved, and check each other's work. Where you can, rotate people around so that habitual mistakes or omissions are identified. This also helps detect fraud and means that several people would need to collude in a deliberate act of sabotage or theft, which is always less likely than if someone can act alone and unsupervised.

Have policies for checking data, including reviews of historic information as well as new entries. List the key documents you expect to have for each client, for instance, and make sure someone checks they're all present and correct on a regular basis.

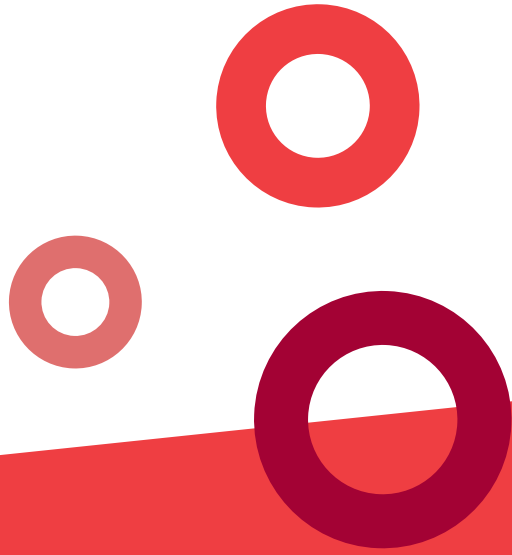
It sounds obvious, but make sure people save their work frequently, using a new name each time for important documents. Even in this time of reliable technology and background provision for the retention of previous versions, this kind of discipline is useful and protects you against unforeseen technology problems.

Make sure you have clear version control policies and document naming conventions in place; ensure everyone knows where to store the latest version of a document and what to do with previous documents. Have a clear policy for identifying versions and for communicating changes to those who need to know about them.

Establish a change control policy; make sure that changes to your systems (computer or paper) don't happen without planning and approval, and that there is proper testing before any changes are used in your live environment. Make sure the implementation of changes is accompanied by backups and a clear record of how things were done before, in case you need to revert.

Teach your staff good computer hygiene – make sure they know how to identify suspicious email attachments; how to tell a phishing email from a legitimate one, and what to do about it; how to check if a website is secure and is what it says it is.

**It sounds obvious, but make sure people save their work frequently, using a new name each time for important documents.**




© Managed Networks Limited 2012

## Technology

Make sure, where you can, that your systems have effective data validation. This is obvious for databases, but you can also implement it in spreadsheets, intranets and many other systems. Remember to check for completeness as well as accuracy, and think about sense checks – for example comparing the size of the current transaction to previous transactions with the same customer.

Review your access controls frequently; make sure people have no more rights than they need to do their jobs. Often people are granted greater privileges as a "quick fix" under deadline pressure, then the enhanced rights are never withdrawn. Six months later they accidentally delete a folder they shouldn't even have been able to see…

If your systems permit it, enable 'snapshots' or 'volume shadow services'; these provide background retention of previous versions of files and folders, and make it easy to recover from accidental deletion or mistaken changes. Of course, you need to make sure that the rights to do this recovery are controlled, too.

Many third-party products exist which can scan your systems and folders regularly to detect unexpected changes or unexpected activity. Used appropriately they can help detect – and in some cases prevent – both data loss and intrusion.  All of these systems will need careful selection and calibration, though, and are not substitutes for proper procedures and defences.

If you do nothing else, make sure you have effective anti-virus deployed throughout your organisation and that it is updated frequently. Consider using different anti-virus scanners in different places, since all of them will have a different list of viruses that they detect. Remember that most infections these days arrive either by email or from web-browsing; make sure you scan email and monitor or scan web activity; there are also cheap and effective ways of blocking access to websites containing undesirable, dangerous and illegal content.

If you have a lot of important data in document files, consider using a document management system – like Sharepoint – in place of basic folders and shares. This will give you greater control over security, better data validation, the ability to automate a range of integrity protections and certainty that people are using the latest versions of files. You can also integrate scanning and filing of paper documents, allowing these to benefit from the resilience you build into your computer systems and making them searchable.

Backup your data. This seems obvious, but so often we find that people's backups are inadequate, incomplete, untested or just plain absent. Make sure you get your backup off-site, too. Backups are your last line of defence in recovering from data corruption, so you need to retain them as well as making sure you take them regularly.


© Managed Networks Limited 2012

## Physical

Remember that not all of your important data are stored on your computer systems. You need to think about protecting paper as well. This means, if you're not going to scan it all in, making sure it's filed properly, and that access to the files is properly controlled. Not only is unfiled paper vulnerable to confidentiality breach, it's hard to find – and data that you can't find is as good as missing for most purposes.

Protect your equipment from environmental risks. If your servers aren't kept cool, clean and dry, they'll fail sooner and you'll lose data. If they're not kept in a restricted-access location, anyone could switch them off, or pour something over them by mistake. Remember that this applies to any device holding important data – all the more reason to keep documents off local hard drives, but also a reminder to look out for removable hard drives and network attached storage boxes; these are another "quick fix" that often becomes a permanent feature.

Replace your equipment regularly, before it fails. It may seem expensive, but the cost of equipment is far lower than the value of the data it contains. Remember that hard drives are mechanical devices with high-precision moving parts. A typical server hard drive, for example, spins at up to 15,000 rpm, 24/7/365. That's nearly eight billion revolutions per year. The outer rim of the disk inside the drive will travel 189 thousand kilometres in that time – nearly eight times round the Earth. It's hardly surprising that eventually they wear out.


**The distance the outer rim of a hard drive disc travels in a year - that's nearly eight times round the earth.**


© Managed Networks Limited 2012

MANAGED NETWORKS

Thinking in threes

# 3: Staying power


© Managed Networks Limited 2012

Availability, the last part of the triad, is about keeping your systems working, and your business trading, no matter what happens. Business continuity planning – the formal discipline behind availability – is a vast topic in itself; this section, therefore, really is a summary of a summary and we suggest you also have a look at our other white papers on the topic.

The key steps to remember in business continuity planning are:

1. **Absorb**
   try to cope with issues and failures without interruption
2. **Adapt**
   deal with reduced capability
3. **Recover**
   return to full functioning

In each step, what's important is that you identify the risks, plan carefully and test your plans. It's equally important that you fit your plans to your circumstances, needs and capabilities. It's far better to have an affordable, workable plan that reliably recovers from a major disaster within three days than to try for a four-hour recovery and fail.

The risks are numberless, and will vary from case to case. Be careful to think rationally about the real likelihood of each risk; don't spend money protecting against high impact but low probability risks until you've protected yourself against the lower impact things that are almost certain to happen.


© Managed Networks Limited 2012

# Risks

Because this topic is so broad, in this section we've chosen just to list out some of the things to think about under each heading.

## External Risks

Fire; flood; civil unrest; terrorism; earthquake; power interruption; public communications network failure; major events; logistics disruption; vandalism; theft

## Staff Risks

Industrial action; pandemics; mass absenteeism (e.g. large sporting events); loss of critical individuals ('key man' risk); travel disruption; sabotage; negligent or deliberate data breach; theft; fraud

## Infrastructure Links

Hardware failure; virus/malware damage; DDoS or other system compromise; communications link failure; software defect;

Before you think about countermeasures to these risks, and whatever other risks you identify, you should ensure that you understand your business properly – how its different functions are interdependent, who the key people really are, how important each system is and how long you could do without it. There is a number of useful mind-mapping and workshop tools you can use to help you do this.


© Managed Networks Limited 2012

# Countermeasures

## This is just a sample:

### People

Make sure that all key roles and activities are covered by more than one person; consider job rotation or job-sharing. At the very least make sure you have a buddy system so that everyone knows who is going to cover for whom. Where you can, try to assign critical roles to people who take different routes to work and live some distance apart.

Encourage flexible working arrangements – you can use technology to enable this. Not only does this help with staff retention and comply with legislation, it's an essential component of your ability to absorb travel disruption or movement restrictions.

Paper doesn't need power; it doesn't need sophisticated technology to decode or update it; it can withstand considerable punishment in transit; it's extremely cheap per megabyte. These are all good reasons not to overlook paper records as part of your business continuity strategy. If you print off your accounting daybooks at the end of each day and take them home, for instance, then you'll always know who owes you money, and whom you owe, even if all your systems are off-line tomorrow.

**Where you can, try to assign critical roles to people who take different routes to work and live some distance apart.**


© Managed Networks Limited 2012

## Technology

Build resilience into your systems at every level – duplicate key components, have multiple communications paths. Spread your systems across multiple servers, and your data across multiple disks – use reliable technologies like RAID to reduce your risk of data loss. Protect your servers against power outages with uninterruptible power supplies.

Backup your data; if you can, do this automatically and continuously to another location. Better still, have parallel systems in another location ready to fire up if your primary systems are off-line or damaged. All of this costs money, but is increasingly available as a commoditised service that you can rent rather than having to make your own investment.

Ensure you have effective remote access provisions – from simple things like enabling smartphone access to email through to a full remote desktop. This enables staff to work from anywhere, even if they can't get to the office. Unlike many aspects of business continuity planning, the added value benefits of remote working – like flexibility, and the opportunity for staff to do extra work from home – justify it on their own.

Make it possible for staff to use their own kit to access your systems, provided you can do so securely. This gives you a much bigger pool of hardware to work with and makes it much easier to adapt if you lose your main office.

## Physical

If you have multiple office locations, leverage them. Make sure it's possible for staff to work from any of your offices, and that your data and systems are distributed between them.

Think about your exposure to natural risks: don't put your servers in the basement – they flood – and don't put them under the roof – they leak. If your building's next to a fuel depot or a power station, then you need to raise the priority of getting at least critical IT systems off-site.


© Managed Networks Limited 2012

# Conclusion

As you'll have seen from this brief overview, there's a lot to know and a lot to think about. You can make a big difference just by making some simple behavioural changes, but if you want to make sure your business is secure and protected, you need professional help and advice.

Managed Networks specialises in providing secure, reliable IT to SMEs. Why not contact us for a free no-obligation consultation to see how we can help you meet the challenges of confidentiality, integrity and availability now and into the future.

You can call us on **0800 783 6170** or email us at **infosec@mn.co.uk.**

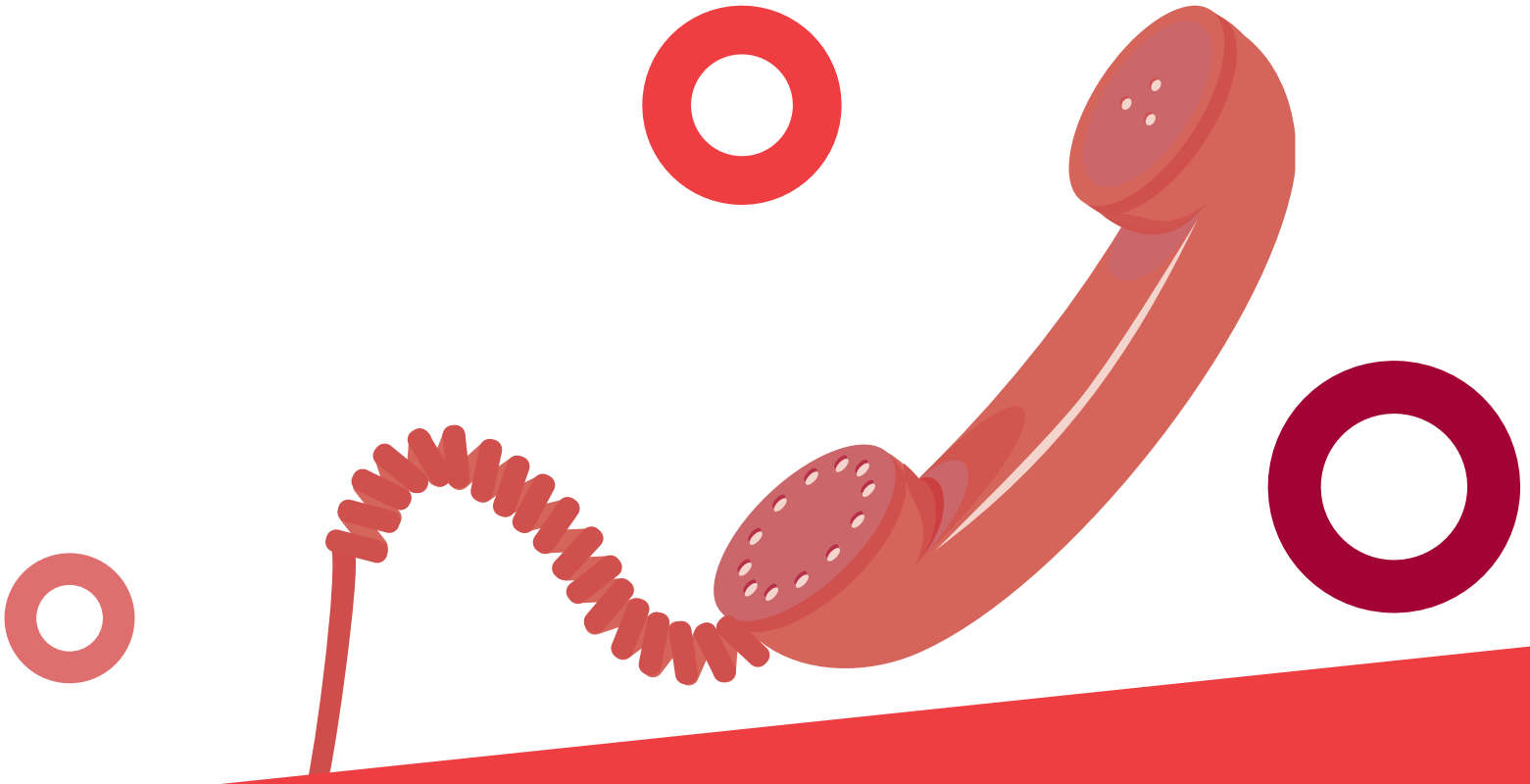

© Managed Networks Limited 2012

# Contact

**London Office**

6-8 Bonhill Street
London
EC2A 4BX

t: +44 (0)20 7946 8000
t: +44 (0)20 7946 8001
w: www.managednetworks.co.uk




© Managed Networks Limited 2012