The

Case for

IT Security

Produced by
encription limited
encription house
95 Droitwich Road
Worcester
WR3 7JE
April 2007

SME Division

01905 754440
www.encription.co.uk

Introduction

The complexity and rapid innovation in IT produces many challenges to an organisation, but one of the most urgent, and yet most neglected, is that of IT and network security. Whether it is the network, the applications you run, the web site you sell through, the legal implications of IT and your use of it, or your staff, and the possibility that they may knowingly, or unknowingly, divulge confidential information.

Of course IT security attacks happen to other organisations, not to you. Most organisations make sure that their anti-virus is up to date, and that they have a firewall. But this is simply not enough, because the increasing use of the electronic transfer of information provides a challenge, not only to you, but also to the malicious hacker, who wants to find ever more ingenious ways to illegally access your systems, and steal your data for financial gain.

Every interface on your web site that can be seen by the Internet is scanned every 3 minutes by an external agency! At *encription* we inevitably find that the two weakest points in a system are nearly always the web site, because of the way in which it has been designed; unwittingly creating open doors for the malicious hacker, and your people, who simply do not recognize security attacks and threats.

Many organisations forget about security procedures, as a result of this we partner with Higgs & Sons, a long established firm of solicitors. Their pointers on what to consider when drawing up an acceptable use policy, or undertaking a web site review are included in this document.

Spending scarce budget on IT security as a preventative measure is not seen as a high priority, but the cost of recovery after an attack, if indeed recovery is possible, will be far more costly both financially and reputationally.

Information security is rising up the corporate agenda. In the public sector it is now a specific, auditable part of good governance, but it still does not get the attention that it now needs within the small to medium enterprise.

This document is aimed at the non-computer person, indeed the computer techie may find it boring, because they (should!) already know what is in here, but do they?

We have tried to avoid jargon and our objective has been to explain what types of attack can happen, what effect they can have, and how to deal with them.

We have tried to make it easy to read by using colour coding as follows:

	Advice
	Facts & Figures
	Examples & Case Studies
	Education
	Questions to ask yourself
	Comments

We hope that you find it informative and useful. If you would like to confidentially discuss any aspect of your information security, **encription's number is 01905 754440 or or visit our web site at www.encription.co.uk.**

Tony McDowell
Managing Director
encription limited
April 2007

The Case for IT Security

Online security attacks are nowadays regularly gaining media headlines. As a result, information security is often seen by organisations as worrying, but even harder to mitigate against. It is then left to the IT department (if there is one) to deal with, rather than being seen as something that can impact on the whole business – and that needs to be dealt with as such.

This needn't and shouldn't be the case **Sir Digby Jones**

With information security, we face another question – how do we make sure we focus on the real threats and don't respond to the latest hype or media headline? Frequently we see genuine intent and efforts to improve security undermined by attention (and investment) focused in the wrong places, assumptions that the IT department can sort it all out, and a lack of genuine business ownership.

Information security is integral to good business practice

The "Partner Chain"

Today all businesses and organisations have a "partner chain". The chain could consist of divisions/departments within the same organisation, external suppliers, clients, agents, Constituents and even Patients. In fact anyone who uses or supplies our information is in the chain.

As the use of IT develops within the partner chain, so does the exchange of electronic information, and the risk that it will be illegally accessed, compromised or used illegally.

Use of the partner chain demands a great deal of trust between the partners. A breach in one partner's information security might not only affect that partner, but may also affect all of the partners in the chain.

The security of your information is as important to you as it is to your partners

encription
ethical hacking services

Some Facts and Figures

ATTACKS ON IT SYSTEMS

- **On average PC's are scanned by outside agencies every 3 minutes**
- **97% of all web applications have serious vulnerabilities (SIM Group 2005)**
- **75% of all IT attacks are aimed at web based applications (Gartner Group 2004)**
- **Hackers use "software tools" to penetrate IT systems**
  In 1980 they had 20 tools
  In 2004 they had 21,311 tools
  Today a hacker can use in excess of 100,000
- **The Police National High Tech Crime Unit - NHTCU Report 2006 found:**
  89% of respondents had been attacked in the last year
  90 % believe e-crime is a serious threat to the survival of their business
  10 % said they would not involve the police if they were attacked
- **The majority of sabotage and data theft is perpetrated by internal staff**

encription
ethical hacking services

What the Audit commission found in 2005

ICT Governance arrangements in the Public Sector

- 96 per cent of organisations have developed ICT security policies
- 82 per cent now employ email filtering
- 85 per cent now employ staff with specific ICT security responsibilities

But there is less evidence of commitment to providing users with robust guidance and unambiguous statements about their responsibilities:

- only half of the organisations surveyed have initiated ICT security awareness training
- only one-fifth of staff have been provided with a copy of their organisation's ICT security policy
- only one-third of staff have been informed about the policy and what they must and must not do
- only one-third of staff knows where to find written procedures for reporting a security incident

ICT security is only as effective as the staff within the organisation and failure to communicate to users their responsibilities has led to:

- a significant increase in inappropriate use of the internet and email
- virus infections continuing to represent a major risk
- ICT fraud still being committed across all organisations

Organisations still appear to be complacent about the risks of newer technologies:

- two-thirds regard wireless technology as being a medium to low risk
- three-quarters regard PDAs (e.g. Blackberrys) as only medium to low risk.

There is no doubt that despite the best endeavours of organisations and their security staff, auditors and managers,
ICT abuse will continue to thrive.

Many organisations have responded to the range of risks they face by deploying more preventative measures, but there is still an alarming minority who fail to protect their information assets, whether through complacency or ignorance of risks

So what are the threats and risks?

There are daily, if not hourly, reports somewhere about the latest technology attack. It could be the schoolboy geek "just fooling around" or it could be organised and sophisticated crime and/or terrorism.

Phishing, man-in-the-middle, virus, worm, probably familiar words, but what are they?

Management is busy running and growing their organisations, so devoting valuable time and money to prevent an "unlikely" attack on information, is not a priority. It is only when disaster happens and business (and perhaps a partner's business) is brought to a standstill, that the threat is taken seriously. The cost of recovery after an attack, if indeed recovery is possible, is many times the cost of preventing it in the first place.

The majority of computer crime is not reported

The cost of an attack to an organisation depends upon the type and severity of the attack. Being unable to process customer's orders for two days may have less effect on a jewellery firm than it would on a supplier of crucial medical products.

A County Council in the UK estimates that the loss of its web site for one day would cost it £3million

A company who had their web site highjacked had £40,000 worth of orders stolen as well as considerable reputational damage.

Do you know what the effect and cost would be (financial or other) of:

- **Not having access to your information for 1,5 and 10 days?**
- **Losing your information completely and not being able to recover it?**
- **Someone gaining illegal access to your on-line banking?**
- **A competitor having access to your client list including sales details?**
- **Confidential employee or client data getting into the public domain?**

EXTERNAL RISKS
Types of attack

Viruses
A virus can take many forms, but the most common are Trojans, man-in-the middle and worms; generically known as viruses.

A Virus
A virus is usually a program (computer code) written by someone, often as no more than an intellectual challenge. As its name suggests, a virus only has one purpose, and that is to cause disruption and harm. There are many variants of a virus, and once in the system, it may start deleting everything it encounters, or it might find the email address book on the computer and send a copy of itself to everyone in that address book. When the recipient opens the message (supposedly from a known and safe source) the virus could start deleting everything on that computer, or simply flood the system with emails.

Trojan
A Trojan (Horse) looks innocent because it is disguised as something else, for example a free toolbar download a screensaver. The Trojan can remain dormant until the hacker activates it, or it activates itself at a specific date and time, at which point it will release malicious software also known as Malware.

Once activated the Trojan can be used to take control of the computer, steal information, or just corrupt the system.

Man-in-the middle
A virus that captures and re-directs data (mobile telephone and computer) to a nearby external receiver owned by the hacker.

A Worm
Like an ordinary virus a worm is computer code, which attaches itself to existing good code. It then goes on to create multiple copies of itself.

Originally the purpose of a virus was simply to cause disruption, not to mention gaining notoriety for its author. Since it has been discovered that there is value in stolen confidential information the objective of malware has shifted to stealing rather than disrupting.

In the first six months of 2006 anti virus software producer Symantec reported a 20% increase of malware designed to access rather than destroy confidential information.

EXTERNAL RISKS
Types of attack

Viruses can be introduced into a system in a variety of ways. They can be hidden in an email attachment. They can be picked up when visiting apparently innocent web sites. They can be resident in a disc containing some free software obtained from "a friend". The latest technique is to hide a virus within an image, such as a logo or picture on a web site.

- **Do you control what can be loaded into your system and by whom?**
- **Are all external media (DVD's etc.) scanned for viruses before its contents are loaded into the system?**

HACKING

Hacking is when someone attempts to gain unauthorised access to computer systems.

Most hacking attacks are opportunistic, but once a vulnerability has been found the attack can quickly become purposeful, with the intent of seeing what disruption can be caused or stealing and using confidential information. Hackers have automated programs which trawl the Internet looking for vulnerabilities without the hacker even being at his/her computer. Once found the hacker can then decide how best to exploit the vulnerability found by their automated process.

Organisations that fail to fix security vulnerabilities in their network are more likely to become the target of a hacker

Phishing

The computer industry can always be relied upon to dream up new words and acronyms, and phishing is a classic example, just think of fishing and you will understand.

Phishing is an attempt to obtain confidential information, and usually comes as an email (no attachment) from an apparently bona-fide source; for example an apparently genuine email from HSBC Bank saying that they have carried out a system upgrade and need you to confirm your bank account details including password. Many people actually respond to this.

The information obtained may be used to buy goods using the victim's bank account details, or it could be used to open a bank account in a false name and launder money. The results are nearly always financial and/or reputational loss.

EXTERNAL RISKS
Types of attack

Keystroke Monitoring
Keystroke logging is another form of malware. Once installed the malware computer code can record every keystroke made. This information is then sent back to the Hacker who runs it through more programs to try and identify meaningful words from the string of characters. If a string of characters like l-l-o-y-d-s-t-s-b is found the program will highlight it and the hacker will explore further expecting the next keystrokes to be user name and password; the consequences are obvious.

Illicit use of an organisations computer system
Recently there has been an increase in attacks which are purely for financial gain. An example is “adware”. Adware is computer based advertising which whenever anyone clicks on it; the author of the adware is paid a fee by the advertiser. Several copies of the adware may be hidden within the computer.

Another example is where an organisation’s web site is “cloned” and an identical copy of the site is made. Visitors to the genuine site are then, unknowingly, re-directed to the cloned site and any financial transactions go into the bank account of the hacker rather than the organisation for which it was actually intended

Denial of Service (DoS)
A DoS is the flooding of a web site or computer system with false access attempts. The result is that the system or web site starts to run more slowly or in extreme cases ceases to operate at all.

Regularly do an Internet search on your own organisation to make sure that there are no “cloned” sites and/or that your organisations name is not being used illegally

Spam
Spam is unsolicited junk mail sent via email. As well as being annoying, and time consuming to handle, it is also a security threat, because it can include phishing attempts or cause denial of service if there is a lot of it.

Do you have an acceptable use policy for the Internet and emails?

EXTERNAL RISKS
Your Environment

Most organisations take far more care over the security of their environment than they do of their data. Burglar alarms are fitted, CCTV may be used, and visitors signing-in-books and badges are required. But the advent of the hacker has introduced new external and perimeter threats.

It is now possible for a hacker to be up to 150 metres away from your premises, and using specialised equipment to detect, and then compromise, any wireless networks in use. Having done this it would be possible to gain access and ultimately full control of your networks and IT infrastructure.

The security key (called a WEP key) that is distributed with many wireless base stations may be identical to that used on other wireless stations from the same manufacturer

Many Hackers have a list of the most common security WEP keys

Make sure that any wireless base stations are fully encrypted and that the security key and password are changed regularly

War Chalking/Driving
There are groups of hackers who when they find an un-encrypted wireless point, "chalk" the external wall of the building with special symbols to inform other hackers that it is available

Hackers use all sorts of ways to hack including acting as a courier with a parcel for someone at the company. The person of course does not exist, but the parcel is left at reception, or hopefully within the department where the hacker is trying to penetrate; for example accounts. The parcel may sit there for some length of time until it is returned to the sender, also bogus of course , or opened. If it is opened, it doesn't matter, because it can be disguised a desk ornament

The parcel contains sensitive electronic equipment which will capture all of the computer and wireless traffic, and forward it on to a nearby receiver owned and operated by the hacker.

Are your staff aware of security risks?

EXTERNAL RISKS
Your Environment

At one time it was believed that computer equipment became obsolete every five years, today it is more like two or three years. This results in equipment, especially PC's (Desk Tops) being replaced frequently. What do you do with them? You could donate them to a good cause, you could take them to the recycling depot, or you could decide to try and sell them. But what have you done about the data which was held on the computer?

If you simply deleted the files using the delete function within Windows all you have done is delete the index link that lets the computer find the correct data quickly and accurately. The data still exists on the hard drive, or wherever it was stored, and can be accessed easily by someone who knows how.

Many old discarded PC's are turning up in markets in Africa.
One man who thought that he had disposed of his PC safely (he took it to a Council tip) discovered that his old PC had been bought by a hacker in Africa with the specific intent of seeing if they could find any useful information on the PC. They did and he lost several thousand pounds from his bank accounts

There are different methods available to ensure that data is not retrievable depending upon what is going to happen it.

Computers no longer required by the ministry of defence are "wiped" twelve times and then the hard disc has holes drilled into it

INTERNAL RISKS

A CBI report in 2005 showed that greater use of technology by organisations could reduce costs, increase productivity, and automate routine procedures. In order to achieve this employees must be given access to the systems and often the Internet.

Technology enables information to flow quickly and effectively within an organisation as well as to and from the partner chain, resulting in better informed and more empowered employees.

67% of respondees to the CBI report saw a measurable increase in employee job satisfaction

With such power and knowledge the disgruntled or dishonest employee can become a dangerous enemy.

It is very easy to download confidential information onto a USB stick or a PDA. If an employee does not take care of, or willingly divulges a password, then access for the hacker is simple. Even worse, employees use post-its above their desk to remind them, and others, of their "confidential" password(s).

Of course the Hacker, given time, can crack most passwords; some even use social engineering (see below).

TIME TO "CRACK" A PASSWORD
The following is based on using one small (1.5 GHz) PC

Less than 6 characters (abcde)	1 minute
6 Characters (abcdef) lower case	50 minutes
6 Characters (abcDEF) upper & lowercase	2.2 days
8 Characters (abcDEF12) upper & lowercase number	67.8 years

Hackers are patient people

PASSWORDS

Should be a minimum of 8 characters
Should contain both upper and lower case
Should contain at least one number AbcDe12F

SHOULD BE CHANGED EVERY THREE MONTHS

INTERNAL RISKS

Social Engineering

In order to obtain sensitive information, including passwords, hackers and criminals may make direct contact with your employees. This can be via the telephone, via email, face-to-face and even via fax. An urgent telephone call from a supposed irate senior manger to a secretary or receptionist, may quickly gain the "senior manager" the information they require.

An email from "IT" declaring that a policy to change all passwords has been taken, and in order to maintain their service the user needs to email back with their current password and the new one they want to use. This is really "phishing".

An employee in the accounts department of a large organisation was responsible for VAT reclaims. The person concerned calculated the VAT to 3 decimal places, but only rounded up using 2 decimal places moving the balance electronically to their own bank account

Budgets are always tight, and spending money on IT security, when the organisation has NEVER had a problem, is not considered a high priority.

When the IRA campaign of terror started in London many financial institutions considered disaster recovery, but thought it to be too expensive when measured against the risk. The likelihood of an attack was remote and certainly would not affect them, until it actually happened!

When the City of London was bombed one weekend the disaster recovery companies could not cope with the enquiries on the Monday, and today disaster recovery is seen as essential by any good organisation. Indeed most auditors demand it.

Employee Errors

Training is one of the first things to be cancelled/reduced when budgets are tight, but the lack of training leads to employee errors.

Such errors had considerably less impact when systems were paper based, but an error made electronically can have a multiple knock-on effect, literally within milliseconds. Employees who divulge sensitive information, because they have not been trained, are a liability, but whose fault is that?

SO WHAT TO DO?

To quote Sir Digby Jones again

Information security shouldn't be seen as an inhibitor to business growth, but as an online challenge to be tackled and overcome….. Organisations need to understand that effective security is inseparable from good business practice [and governance]

Carry out a risk assessment

- Identify what assets you are trying to protect and identify where they are
- Identify which systems, staff and assets are involved in the reception, transmission, storage and processing of information
- Identify which staff and partners have access to and control of the information
- Identify the elements that are critical and try and calculate the cost of them not being available
- Identify the potential threats to, and vulnerabilities of, those critical elements

SO WHAT TO DO?

Make sure that you have up to date security policies and procedures

Information governance is now an integral part of good governance. Sound policies and procedures are essential to its delivery.

The elements of a good security policy include:

Confidentiality and Privacy
Access
Accountability
Authentication
Availability
Information technology system and network maintenance policy

In the event of a virus attack or IT disaster

What happens?
Who takes control?
Who does what?
What contingencies are in place?
What are the recovery procedures?

SO WHAT TO DO?

Make sure that staff are trained
Everyone in your organisation should understand what constitutes a possible social engineering attack, and the effects of a virus. All computer users should know what your acceptable use policy is, and be aware of the need to protect confidential information, especially passwords. They should also understand the procedures and boundaries for contact with the IT department and external suppliers/contractors

In one organisation 90% of the employees were persuaded to divulge their passwords in exchange for a free pen

SO WHAT TO DO?

Introduce a Computer Use Policy & Web Site Review

In conjunction with our legal Partner, Higgs & Sons, we have produced guidelines on how to carry out a review of your web site to ensure that it conforms to the latest legislation. Higgs & Sons has also identified points to be considered when drawing up an Acceptable Use and Email policy, here they are:

Computer Use policy Checklist of Issues to Consider

Please note this list highlights some of the points that should be considered when drafting a Computer Use Policy. The list highlights generic issues without regard to the specific commercial issues that may face your business. Depending upon how you use IT in your business, some of the issues will be less important than others. ***This list is not definitive and specific guidance should be sought.***

1. Introduction

a. Describe the general background to the policy, highlighting the importance of IT security to the business, what use is acceptable and why.
b. Explain that the policy may change from time to time to reflect changes in technology and the way the firm uses its IT facilities.

2. General Duties

a. Set out general duties in respect of the legal and proper use of the IT facilities.

b. The IT system may contain large amounts of confidential and/or commercially sensitive data. Accordingly set out a general duty of confidentiality.

c. General prohibition on unauthorised copying, processing and distribution of material and use of the IT system for any illegal purposes.

d. Set out general duties in respect of content (e.g. material must not be defamatory, offensive or obscene).

e. Set out a general duty of care when sending email (bear in mind that email is generally a less formal means of communication than a letter and can easily be copied to a large number of recipients at the touch of a button; employees should therefore take care to ensure the accuracy and content of emails).

SO WHAT TO DO?

Introduce a Computer Use Policy & Web Site Review

3. Use of Email

a. All outgoing email to contain your standard email notice/disclaimer.

b. Set out the firm's standards (for example, the firm's reference and approved form signature to be included on all outgoing email; email to be checked by a senior colleague before sending; hard copies of all emails to be retained in the firm's manual filing system).

c. Encourage employees to consider who should be copied in on an e-mail. The ease with which this can be done means there is a temptation to copy e-mail to large numbers of users even where this may not be relevant or useful. If an e-mail does need to be copied to several users, encourage the use of BCC, blind copies, to protect the identity and email address of other recipients in the group.

d. Set default settings on user's inbox so that the preview window is closed to minimise the risk of a virus being introduced through an email automatically opened in a preview window.

e. Agree with the customer that email is an acceptable form of communication.

f. Consider whether email is the most appropriate means of communication in the circumstances, having regard to the content and time frame. Particular care is needed if an email contains highly confidential or sensitive information. It is good practice to confirm safe receipt when sending particularly important or time sensitive information.

g. Remind users that email may be used in evidence and could become part of a legally binding contract. Further, under the Data Protection Act 1998, individuals who are the subject of the email have a right of access to that and related messages. Consequently, care is needed as to content and should always be checked by a senior colleague if in doubt. Be clear about who in your organisation has authority to bind the firm to contracts. The same rules and procedures should apply to contracts entered into electronically.

SO WHAT TO DO?

Introduce a Computer Use Policy & Web Site Review

4. Personal Use of IT Facilities

a. Set out the extent to which use of the firm's IT facilities for private use is acceptable.

b. An email sent from the firm's machines will probably identify the firm as well as the individual, so whenever the individual is using the firm's email for personal use, the email should make it clear that the individual is acting in their individual capacity.

c. Encourage individuals to mark personal emails as such and to direct incoming personal email to a personal folder. This may be important if you intend to monitor incoming email, having regard to the individual's right to privacy.

d. Set out procedures to reduce the risk of introducing a virus onto the firm's system from personal use (for example no unauthorised downloads; no unauthorised use of personal software; care when opening email from an unknown source).

e. Explain that any personal use of the firm's IT facilities must not interfere with the employee's job.

f. Where appropriate, include sections in respect of Blogging[1] and re-iterate that users must not publish or offensive, obscene or defamatory material.

g. Consider the extent to which an individual is permitted to use their own IT equipment during office hours bearing in mind that it will be difficult to monitor private IT systems in the way that it is possible to monitor the firm's system.

5. Use of the Internet/ Internal Intranet

a. Set out the extent to which users are permitted to access the internet/ intranet and the purposes of access.

b. Make it clear which parts of the internet/intranet are not to be accessed and state that employees are not to attempt to access such parts.

c. Set out the firm's policy on downloads and subsequent use of downloads.

[1] A "Blog" or web-log is a personal log similar to a diary published on the internet.

SO WHAT TO DO?

Introduce a Computer Use Policy & Web Site Review

6. Copyright and Intellectual Property

a. Explain that most information on the internet will be protected by copyright and that unauthorised copying is an offence.

b. Explain that all software must be licensed. Set out the firm's policy on introducing new software on to the firm's system. Explain that you may undertake a software audit and the sanctions for introducing pirated or unlicensed software on to the firm's system.

7. System Security

a. Re-iterate the importance of security and duties of confidentiality.

b. Set out the firm's policy on the use of passwords.

c. Stress the importance of only up/downloading information from a known, reputable source and perhaps subject to prior authorisation.

d. Warn employees not to respond to Phishing[2] or other security risks and what action they should take if they are concerned about an email.

8. Working Remotely

Be aware that working remotely imposes a greater security risk and set out the firm's procedures for reducing those risks, for example

a. The importance of keeping laptops and hand held devices secure and out of sight when not in use;

b. Ensuring the screen can not be overlooked when in use;

c. Where there are adequate alternative provisions to allow secure access to work related documents, discourage employees from emailing business related documents to private email accounts to enable the employee to work on the document from home.

[2] Phishing is the term given to email sent from an apparently legitimate source used to try to persuade individuals to surrender sensitive information, for example, an email supposedly from a high street bank requesting confirmation of account details and passwords. The perpetrator may then use the information causing potentially serious loss and damage.

SO WHAT TO DO?

Introduce a Computer Use Policy & Web Site Review

9. Monitoring Communications

Be aware that there are restrictions on employer monitoring of email and telecommunications. There is an extensive amount of legislation in this area. Consequently, if you do intend to monitor employees or intercept communications, specific, professional advice should be sought. Failure to comply with statutory requirements may render any evidence obtained this way as inadmissible in subsequent legal proceedings.

10. Data Protection Act 1998 ("DPA")

This imposes various (and in some cases, onerous) duties and obligations on those who process "personal data" (namely, information relating to living, identifiable individuals). In most cases, the employer will be primarily responsible, but will also have a duty to ensure that employees are acting in accordance with the provisions of the DPA. The implications of the DPA are extensive and specific, professional advice should be sought.

11. Disposal

Refer to the firm's policy on safe and proper disposal of obsolete or damaged equipment bearing in mind you may be subject to other legislation in this area (for example, WEEE and CoSH regulations).

12. Compliance with the policy

Confirm that any breaches of the policy will be taken very seriously and set out sanctions for non – compliance.

SO WHAT TO DO?

Make sure that your websites are legally compliant

Web Site Legal compliance considerations

A web site not only needs to be secure it needs to be legal

A typical area of vulnerability will be an organisation's website. All too [illegible] attention is given to the security relating to a website, although this is an obvious and very public target for external attacks. Remember also that a website must meet certain criteria and legal requirements. If you are reviewing the security implications of your website, this provides an opportune time to consider legal compliance.

There is no single law on websites, but rather, relevant provisions are scattered throughout multiple sources of legislation and case law. Highlighted below are various matters of which you should be aware.

Employee Considerations

A computer use policy is essential otherwise employees make their own decisions on what is acceptable and what is not

As described earlier in this document, employees can represent a serious security threat to your business. It is therefore vital that you implement a carefully drafted computer use policy setting out the ways in which employees are permitted to use the firm's IT system. In the absence of specific guidance, employees will be forced to make their own subjective judgments as to what constitutes acceptable use. At best this can lead to inconsistencies and difficulties in bringing disciplinary action against employees who engage in appropriate use. In some cases, an employee's misguided behaviour can expose the firm's IT system to serious security threats and other legal liabilities.

Please note that as an employer, you may be held liable for the wrongful or negligent acts of your employees under the principle of vicarious liability.

All employees should receive training on your policy appropriate to their use of the system. You must also consistently enforce the policy.

Here is a checklist of matters you may wish to consider including in a policy.

LEGAL COMPLIANCE CHECKLIST

Corporate Information

What must be displayed on your web site?

You may be aware that in accordance with various pieces of legislation you are required to display specific corporate information on the website. This includes any company name, registered office address and registered number. Unincorporated businesses are still required to supply certain information including an address for service, VAT registration number, and in the case of some partnerships, the names of the partners.

This list is not exhaustive and for further information, you are advised to seek specific advice.

SO WHAT TO DO?

Make sure that your websites are legally compliant

Intellectual Property ("IP")
Who owns your web site?

Intellectual property is a very valuable commodity in an ever expanding market. In order to retain its value you need to protect your interests. Do you own the IP in your website? How is this dealt with in your website development agreement? Many businesses do not realise that the IP in their website may be owned by the site developer. This can cause difficulties if the business seeks to engage the services of a different developer or contracts a third party to undertake website maintenance; or if the business is ever sold.

There may be copyright and other IP rights in the content of the site. You should ensure that your business owns or is licensed to use the content. You should not assume, for example, that having the right to publish photographs in a hard copy brochure automatically gives you the right to display those photographs on your website. Copyright notices and fair use policies should be included on the site to explain to others what information they are permitted to download from the site and restrictions on their use of that material.

Domain Name
Are you using someone else's name?

Is your domain name the same as or similar to anyone else's corporate or trading name or to a registered trade mark? Use of such a domain name may infringe the third party's rights and could result in a claim against you for trade mark infringement, or in the tort of "passing off".

Equally, if you become aware that a third party is using your name or infringing your rights, you should take action swiftly to prevent further infringing use. The longer that the third party uses the name (thereby establishing their own goodwill and reputation in the name) the more difficult it will be to bring a successful action in future.

It is possible to register several similar domain names with different extensions, for example, .co.uk, .com, .org and so on. You may consider registering several variations of your name, or perhaps common miss-spellings of your name, with a view to ensuring those domain names will not be available to your competitors in future.

Domain name registrations typically last two years, after which time they must be renewed. You should ensure renewal dates are diarised and not missed. Failure to renew the registration means that the domain name becomes available for third parties (including your competitors) to acquire.

SO WHAT TO DO?

Make sure that your websites are legally compliant

Trade Marks
Have you obtained necessary permissions to use trade marks?

If you display any third party registered trade marks on your website, you must obtain the owner's specific consent. Displaying marks without consent can constitute a Trade Mark offence.

Similarly, you may consider registering your brand as a registered trade mark. Doing so will assist you in protecting your brand and preventing others from using it without your authorisation.

Data Protection
You probably need to be registered; are you?

The Data Protection Act 1998 ("DPA") protects any information relating to living, identifiable individuals. This may include photographs of individual employees or customers, a customer testimonial, or even an email address. Any personal information that you collect through the website either by the individual supplying information to you (for example, on an order or enquiry form) or information that is passively collected through the use of cookies or scavenger software will be protected. The implications of the DPA for website owners are extensive.

If you process information on behalf of a third party, or if you engage the services of a third party to process information on your behalf (for example third party IT consultants, providers of book keeping and payroll services or providers of an occupational health or pension scheme) that party will be acting as a Data Processor under the DPA there must be a written agreement in place between you.

This report has already considered the concept of a Partner Chain, and it is likely that Data Processor Agreements are required between the partners in the chain.

Further, it may be necessary to implement an Information Handling Policy. This document explains to your employees and others the ways in which you process their information. The DPA is particularly important in the context of employees, as you are likely to retain significant quantities of personal information, including potentially sensitive information such as sickness absence records.

Privacy Policy
You need one

There are strict legal requirements under the DPA which are aimed at protecting your customers' privacy with regards to the information that they provide to you. Displaying a carefully drafted privacy policy on your website will assist you in complying with your obligations under the DPA.

SO WHAT TO DO?

Make sure that your websites are legally compliant

Terms and Conditions of Sale
If you sell through your web site, then you need them

Where goods are sold through a web site, there is a host of legislation designed to protect customers, promote confidence and support the growth of E-commerce. You must display terms and conditions on your website and these will not only protect your customers, but also ensure you are placed in the most favourable position possible in the event of a dispute. The terms should comply with all relevant legislation and should be kept under review to reflect changes in legislation from time to time.

Links to Other Sites
Do you have permission?

There are a number of considerations to bear in mind if your website includes links to other sites (for example links with distributors and other organisations in the Partner Chain). You should obtain the consent of the owner of the site that you intend to link with and enter into a specific written agreement with them. You may need to include a disclaimer to protect you against any defamatory, offensive or other infringing material on the linked site and obtain an indemnity from the linked site so that in the event that a third party brings a claim against you in relation to the linked site you have a corresponding claim against the owner of the linked site.

Disability Discrimination
Your web site must be accessible to those with disabilities

The Disability Discrimination Act 1995 ("DDA") outlaws discrimination on the basis of disability. Websites must be accessible to all and if your website is not set up in such a way as to make it accessible, this can amount to discrimination in breach of the DDA. By way of example, does your website include text alternatives to pictures? Does the site support the use of Screen reader or screen magnifier software for visually impaired users? Dyslexic users may benefit from clear text and fonts or the use of particular text formats such as Easy Read. At best, failure to comply with the legislation could mean excluding potential customers; at worst it may result in claims leading not just to significant financial consequences, but also damage to reputation.

The above set out some of the general legal considerations that may apply to your website and IT system. We are able to provide a review of the legal issues relating to your website and to provide assistance in drafting all required documentation. For further information, or to discuss your specific requirements, please contact us.

Independent Advice

Independent advice can save time, money and reduce the risk of an attack

Independent Legal Advice

At encription limited we consider all areas of security from internal to external, including legal considerations. We also believe in specialisms, which is why we partner with Higgs & Sons for the provision of legal advice to our clients. Higgs & Sons has been established since 1875 and are one of the largest legal firms in the Midlands.

If you need legal advice on any aspect of IT you can either contact Higgs through us or go directly to Higgs & Sons at

www.higgsandsons.co.uk
01384 342100

Independent Advice

Independent advice can save time, money and reduce the risk of an attack

It is impossible for your own internal IT department and/or the vendor who installed your network and IT infrastructure to be objective in testing for security vulnerabilities. They will have pre-conceived ideas and take things for granted.

What is the alternative?

Ethical Hacking (penetration testing)

Ethical = Morally Correct
Hacking = Penetration of a computer system to gain control over its data and programs.

An ethical hacker is an independent external consultant who is engaged by an organisation to try and break through their perimeter and IT security. The ethical hacker uses exactly the same techniques and tools as the malicious hacker, but their intent is different.

The ethical hacker finds security vulnerabilities, exploits them to see what effect breaching can achieve, and then reports to the client on how to fix them, or fixes them on the client's behalf.

Ethical hacking tests the network, IT infrastructure, web site, environment and staff.

At **encription** our consultants have extensive experience of all aspects of IT security. All of our consultants are a minimum of CEH (Certified Ethical Hackers) and work to BS7799/ISO27001 standards. As a company we are ISO9001:2000 regsitered.

We operate across all industries and organisations including Public Sector, Building Societies, manufacturing, law firms and accountancy practices. We also work with UK police forces. We are UK based and can offer:

Consultancy in security standards and procedures
Ethical Hacking
Social Engineering
Perimeter Testing
Security awareness training

You will find out more on our web site or call us:

www.encription.co.uk
01905 754440