INTRODUCTION TO CYBER SECURITY FOR FENCING BUSINESSES

The purpose of this guide is firstly to raise awareness of issues surrounding cyber security, i.e. what it is, why it is important, and secondly to suggest practical low or no cost solutions that small fencing businesses can implement to secure their own information systems.

So what is Cyber Security?

The fences that we all manufacture and/or install provide a physical security barrier to protect our clients' assets from theft or malicious damage. We are all fully familiar with the concept of physical security. Cyber security can be likened to fencing in that it is also a means of protecting assets – in this case "information assets" - which are the back-office computers and devices and the information stored on them that our businesses use and rely upon each day.

This information will likely include employee, customer, supplier and wage records, contracts and tender information, bank account details, perhaps credit card details, trade and technical secrets, etc. For a business to function (and comply with the law) commercial and personal information must be stored securely so as to remain confidential and unaltered, and must be available for retrieval when needed.

Businesses know only too well the value of ensuring that their physical assets, e.g. their manufacturing machinery, continue to operate every day without interruption. This is why businesses maintain them and protect them with fences. Similarly, although few consider them with the same prominence, businesses also rely upon the continued and correct functioning of their information assets.

These vital business resources also require a fence, or rather a defence, to protect them. Cyber security refers to the protection of a business' vital information and the computer systems on which it is stored. And it's not just about protection from the many dangers of the internet. What about loss of information due to theft or damage to your IT equipment? What about hardware failure, flood, fire? What about human error, or malicious human activity (perhaps a disgruntled ex-employee)?

Cyber security requires consideration of any and all risks to the business' information assets.

Effective cyber security requires an Information Security Management System (ISMS). The BS IEC/ISO 27000 series of standards (often referred to as ISO27K) formally define the requirements for an ISMS, and contain best practice guidelines for implementation. That said, the standards are lengthy and wordy documents, and can be off-putting and ill-suited to small businesses. However, their key principles and controls can be adapted to suit an organisation of any size.

© European fencing Industry Association

What are the risks to an undefended business' and its information assets?

- **Loss of Confidentiality**: unauthorised disclosure of vital business information, including: sales, estimating, accounts, personnel records, Emails, trade secrets, product designs, company, employees or supplier bank details, etc.
- **Loss of Integrity**: corruption or unauthorised alteration of the same vital business information.
- **Loss of Availability**: loss of access to that information due to malware, theft, fire, flood, human error, vandalism, hardware failure, etc.

Maintaining the confidentiality, integrity and availability (easily memorised as "the CIA") is the key concern of information security and an ISMS.

Who is at risk, and what are the risks?

The principal risk in this inter-connected age comes from the Internet. Increasingly businesses depend upon the Internet to manage their livelihood, finances, supplies, relationships, etc. Unfortunately everything that is connected to the Internet is at risk of being hacked by cyber criminals. In fact there has never been a more dangerous time to be connected to the Internet.

> *Everything that we use today has a computer in it. And those computers can all be hacked*
>
> (Leo Doyle, Head of Indianapolis Division of Homeland Security's Cyber Defense Force)

> *The total number of things connected to the Internet exceeded the global population in 2008, and is forecast to exceed 50 billion by 2020*
>
> (Cisco Systems)

This increased risk is in part because the number of things connected to it has grown exponentially. Nowadays many of us will have a desktop computer, plus a laptop, tablet, or smart phone. More connected things means more risk. More importantly it is that the threat level has increased. Hacking may at one time have been the preserve of nerdy teenagers who hacked for fun, or for notoriety, poking a finger up at authority etc. Their targets were government departments, and the military etc, and certainly not small businesses.

Unfortunately cyber-crime has become more lucrative than traditional crime, and the vast majority of hackers are highly organised and sophisticated cyber criminals who are aggressively looking for vulnerable targets. Worse still, the UK law enforcement agencies, by their own admission, have neither the resources nor the expertise to fight this growing threat alone.

> *International gangsters are increasingly abandoning drug dealing and other high risk rackets in favour of cybercrime*
>
> (Adrian Leppard, Commissioner of City of London Police)

> *2013: Twitter hacked. 250,000 user names and passwords extracted*
>
> *2014: JP Morgan Bank hacked. 76 million personal and 7 million business records*

Businesses therefore must help themselves and the authorities to mitigate the risks of cybercrime by implementing cyber security measures within their own organisation. Despite news reports of famous hacks against large organisation, where millions of customer records have been stolen, many business owners still don't associate this with real crime, or at least not a crime that affects them.

Unfortunately the opposite is true, as the main purpose of these large-scale hacks from banks, utilities, and retailers etc. is to obtain information about individuals and businesses to be used in further malicious activities. Names, addresses, contact numbers, etc are as valuable as currency, in fact quite literally as hackers sell this information on to other malicious actors in a growing dark market.

> *Small businesses are under the misconception that their networks and data are safe because they don't have anything of interest to cyber attackers*
>
> (Corey Nachreiner, Director of Security Strategy at

The buyers of this stolen information use the names, numbers and other information in a series of cleverly crafted personalised attacks. They may impersonate a known contact, e.g. a person's bank, by phone or Email and try to get the victim to reveal their banking passwords, or send them Emails containing malicious attachments which, if opened, will install malware onto their systems. Ultimately cyber criminals are after your money, and they are numerous, determined and resourceful. They are not interested in 'you' as such – it is not personal – they are just looking for vulnerable targets.

For that reason small businesses are increasingly being targeted due to their lack of cyber security awareness and protection. Whilst small businesses may not yield value in themselves, they can be invaluable as a 'stepping stone' to more lucrative targets, e.g. their own customers. Perhaps you work with utilities, schools, local authorities, the MOD or CPNI. If you have no cyber defences you may find your systems being used as a 'backdoor' to someone in your sales or supply chain.

How many of your customers would continue to buy from you or suppliers supply you if they thought that THEIR private information on YOUR systems was being compromised?

There are also important legal reasons for protecting information: the Data Protection Act 1998 requires businesses to manage data responsibly and to store it securely. The MD of an organisation is responsible, and can be held accountable for, the information stored on their systems howsoever obtained, i.e. even if placed there innocently by an employee or deliberately by a hacker.

Consider the implications of unlicensed downloaded music, film, or even pornography finding its way onto your computer systems. Unlikely? It probably is if you have strong cyber defences which include managing who can access what on the internet and within your internal network.

If however you have a number of staff with unrestricted and unmonitored access to the internet, alarm bells should be ringing!

The internet is a vast and dangerous place and everyone that is connected to it is at risk, and particularly small businesses whose perceived lack of cyber awareness and protection makes them a vulnerable soft target. All businesses are custodians of their customers', suppliers' and employees' commercial and personally sensitive information, and bear a commercial and legal responsibility to treat that information responsibly. Fencing businesses more so as they are perceived as being a part of the security industry – its no good making a superb job of a client's fence whilst abandoning his commercially sensitive information to the fates. Cyber security is an expected facet of our industry, i.e. commercial and moral imperative.

Implementing a basic Information Security Management System?

Information security, just like physical security or safety in the workplace, is essentially about risk management: identifying what is at risk; the level of risk; and finally implementing controls to mitigate the risk. Fortunately, most managers working in the fencing industry will be familiar with risk assessments, as they will likely be reading or writing them on a regular basis in order to protect the safety of their employees in the workplace.

An information security risk assessment serves the same purpose, i.e. protection, and adopts exactly the same principles and methodology. That is, it first considers the likelihood of an event occurring, in this case a loss or corruption of information; and secondly considers the severity of that event upon the organisation. Severity could refer to the time a computer or IT system could be offline whilst it was say being cleaned of a virus, or data restored, or it could refer to the cost (including time and disruption) of restoring it to its former state.

The likelihood multiplied by the severity give a risk rating – the higher the rating the greater the risk - as illustrated in the following table, whose format should be familiar to fencing businesses.

			RISK RATING = Severity x Likelihood				
			Severity				
			5 Severe	**4** High	**3** Medium	**2** Moderate	**1** Low
Likelihood	**5**	Almost Certain	25	20	15	10	5
	4	Highly Likely	20	16	12	8	4
	3	Possible	15	12	9	6	3
	2	Unlikely	10	8	6	4	2
	1	Highly Unlikely	5	4	3	2	1

The next table illustrates whether action is necessary dependent upon the risk rating. Where the risk level is considered unacceptable, the organisation takes action by implementing controls to mitigate or eliminate those risks.

Risk Level	Risk Rating	Actions
Low	1-6	= No action needed
Medium	8-12	= Action to be taken to reduce risks (controls)
High	15-25	= Urgent action required.

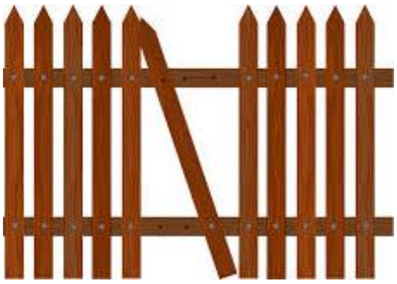
The worked examples on the following page illustrate side-by-side an extract from a traditional fencing risk assessment (considering a manual handling operation) and an extract from an information security risk assessment (considering the information on an accounts department desktop computer).

Safety Risk Assessment (Fencing)		**Information Security Risk Assessment**	
Activity	Manual handling	**Asset**	Accounts Dept Desktop
Who is at risk	• Employees • other site workers • site visitors	**What is at risk**	• Accounts, banking and personnel/payroll records • Word documents • Excel spreadsheets • Email
Hazards	• Bodily Injury (back, limbs, hands, feet) • Trips and falls • Damage to adjacent property	**Hazards**	• Unauthorised access (cyber or physical) leading to loss, corruption or disclosure of confidential records • Malware infection • Computer hardware failure • Theft of computer • Fire, flood
Risk Rating	Severity 3 x Likelihood 3 = 9 (Medium)	**Risk Rating**	Severity 5 x Likelihood 3 = 15 (High)
Controls	• Lift with mechanical means where possible • Never lift anything that you feel is too heavy for you • Share heavy loads between persons of similar build and strength • Wear appropriate PPE • Observe good manual handling techniques (ensure all staff trained) • Keep working area free from obstructions • Exclude unauthorised personnel from the working area	**Controls**	• Implement user access controls so that only authorised personnel can access the accounts computer. • Protect with a strong password (screen lock) • Ensure internet access via a properly configured firewall • Mirror the accounts data on secure secondary storage media. • Antivirus/malware protection • Regular security updates to OS • Regular backups, & ensure backup media stored securely • Bolt or chain desktop computer to desk. Lock doors and windows at night.
Residual Risk	Severity 3 x Likelihood 2 = 6 (Low)	**Residual Risk**	Severity 5 x Likelihood 1 = 5 (Low)

The example above should illustrate that undertaking an information security risk assessment, just like a safety risk assessment, requires little more than common sense, and does not need to be completed by an IT expert. All risk assessments are subjective, i.e. there is no ‘one size fits all’. Each business will store different information in a different IT configuration, may be subject to different risks, and will likely have a different risk attitude.

A large organisation with many staff each having well defined roles may need to do a security risk assessment for each computer that they use, as each may contain unique data which needs to be the subject of different levels of risk and controls. That may seem a daunting proposition.

However for a typical small business in the fencing industry, with relatively few staff each necessarily adopting a number of roles, the risks and controls will be very similar for all of their computers. So it is highly likely that a business can achieve a good level of information security by undertaking a single information risk assessment covering all of their IT systems, and implement the same set of risk controls universally throughout the organisation.



It is important to stress that no information security solution will protect against ALL eventualities, just as a fence will not necessarily prevent all attackers. Each business must balance the cost of the remedy against the benefits. For many businesses the ideal fence is one that is just strong enough to make a would-be intruder look for a more vulnerable victim elsewhere. This is the same for information security, although in fact most controls neither require IT expertise nor any significant cost to implement.

The balancing act for small businesses will likely be between the need for security and the need for utility, i.e. staff getting their work done. For example there is no point in trying to enforce passwords of such complexity that no-one can remember them and so writes them down on a post-it note stuck to their monitor. Information security controls must be practical and not obstruct the business' core activities to the extent that users seek ways to bypass them.

Some practical and simple controls may include:

User Access controls: try and limit access to computers, programs and/or data only to those staff that need to use it. Restricting access will reduce the likelihood of data corruption by an inexperienced user, and data theft and disclosure by a malicious actor. There are technical ways to restrict access to each user on a file by file basis, but for the most part a password will do the trick. That is a password on the computer itself for log in, and a password on any programs, e.g. accounts, that have that facility.

Password controls: an intruder will penetrate any high security fence with automated tools and sufficient time unobserved, and so it is with passwords. They are not unbreakable, but a strong password can make it difficult for a would-be hacker, who will hopefully be put off and look for a more vulnerable victim elsewhere. Passwords are one of the most effective security controls and cost nothing at all to implement.

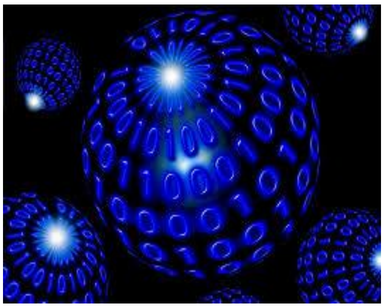
The first principle of passwords is that any password is better than no password. So always use a password where the facility is available, and always change the default password, i.e. the one that came with the device from new (typically username "admin" and password "password"). Secondly never use your name or any other phrase, number or combination that can easily be guessed. Third, never use an English word that could be found in a dictionary - some hackers use automated password cracking tools which literally try every single word from a digital dictionary. Fourth, configure the screen saver to password lock the computer when unattended. Fifth, never write your password down nor disclose it, verbally or by Email, to anyone who does not have the correct authority. Finally, never use a single password for all applications/websites etc, Your bank' website can be relied upon to be secure, but that is no use if your password is obtained from another less secure site, e.g. an online retailer.

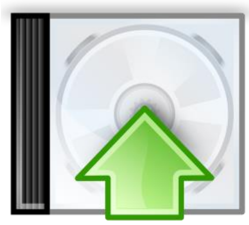
Passwords must be difficult to guess, which means that they should be fairly long (at least 8 characters). Longer is better, but they must also be memorable, or they will likely be written down. Why not make one up from the first (or any) letter of each word from a line of your favourite song, or perhaps join three random words together? If a password policy requires numbers, try substituting a 1 for an ‘i’ or a 5 for an ‘s’ etc.

Email: the majority of Emails sent these days are unsolicited: at best advertising punts, although all too common they contain highly dangerous malware. Always be wary of an Email with an attachment, particularly if sent from a stranger. Generalised greetings or content can also signify danger. Never click on, open, nor forward suspicious Emails – delete them without reading.

Firewall: a firewall is an essential tool in the information security armoury. Typically a firewall blocks unauthorised access to your systems from the Internet, whilst allowing users on your systems to access the internet. Many common routers have them built in (check whether yours does – and if so ensure that you change the default user name and password). Windows also has its own firewall which should also be enabled.

Anti-virus/malware: malware is a generic term meaning malicious programs designed to infect your IT systems. At one time we only had viruses to worry about. Nowadays viruses are just one example of a growing number of threats, including Worms, Trojans and Keyloggers (further explanation below). There are said to be 80,000 new malware variants released every day, and so it is vital that every business invests in suitable anti-malware software, installs it on every computer and mobile device, and ensures that it is updated daily.





Backup: regular backups are ESSENTIAL to information security. A business cannot possibly protect its computers and data against every eventuality but, if it makes regularly backups, it can at least restore it following a serious incident, e.g. theft, fire, flood, virus, etc. Backups should ideally be kept off site, e.g. The Cloud. Remember, backups are copies of the original data, so backup media must be securely stored and protected in the same way as the original data.

Social Media: these sites are renowned for being monitored by cyber criminals as a source of useful information for hackers. User posts can reveal names or images of key staff, and of the premises, that could be used to gain unauthorised entry to your systems. Perhaps an ID card could be forged, or the location of valuable IT equipment disclosed. If Social Media is used for marketing then restrict its use to the marketing personnel only. Otherwise it is a dangerous and costly distraction and should be banned as a matter of policy.

Internet use: unrestricted use of the internet is a recipe for disaster - online shopping, gaming, video/music streaming, and other non-work related web distractions not only waste time, and therefore cost the business money, but can lead to dangerous malware being installed on your systems. Many apparently ‘free’ online services and websites contain tracking programs and other malicious software. Remember, if you are not paying for the product, YOU are the product! Implement an internet use policy to control how it is accessed.

Physical security: shouldn’t need much explanation as it refers to familiar fences, gates, locks, cages, etc. What we all do! In making a cost-benefit decision about physical protection of IT systems, businesses should consider the whole cost. That is, not only the couple of hundred quid or so it costs to replace the hardware, but the cost of the business interruption and disruption associated with restoring the data and programs before getting the staff member, department or company back up and running again.

Updates and patches: during the life of a software program it is common for users to discover vulnerabilities, i.e. bugs or errors in the software. Hackers exploit these vulnerabilities to compromise their victim’s systems. Market-leader Microsoft, for example, releases weekly security patches for its Windows family of operating systems. It is important that your computer systems are configured to receive security and other updates automatically, or you may otherwise be leaving a ‘back door’ open.

Portable devices: employees must be prevented from bringing their own devices into work and connecting them to the company’s systems. And likewise they must not be able to copy and take information away. Information that is off the business premises may not be able to be protected, particularly if copied to a home computer. DVD and USB ports can be easily disabled on most computers.

WiFi: If you need WiFi for your business, e.g. for sales staff laptops, then ensure that you use a password on your wireless router or access point so as to prevent unauthorised access to your systems. Don’t allow staff to connect their own personal mobile phones and devices to the company WiFi system. When staff are ‘on the road’ they must avoid connecting their WiFi equipment to unsecured public WiFi networks such as at cafes and public buildings. Once again staff behaviours may need to be regulated with an appropriate policy.

People

Implementing an effective ISMS is actually as much about people as it is about technical controls. One IT professional recently commented that the best control of all is to “*stop people doing stupid stuff*”! So it will require awareness training, and permanent behavioural change at all levels of the organisation, and it must therefore be championed and resourced from the top. Ideally it should be supported and enforced by a series of cyber security policies.

Further Action

In today’s internet-dominated and inter-connected society cyber security is vital for all businesses. As indicated in this guide, it is not expensive nor does it require an expert to improve your cyber security posture. Aside from protection, there are commercial advantages in doing so too, as more and more government departments are insisting that their suppliers are accredited to the Cyber Essentials scheme - https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

This Guide, intended for fencing business managers and owners, will hopefully act as a first step towards that goal and enables fencing businesses to get ahead of the game.

Glossary of malware and hacking terminology?

Malware is a generic term for malicious software which is designed to gain unauthorised access to and control over IT systems. Once infected an IT system can be compromised or exploited in any number of ways: sensitive personal or commercial data can be extracted; data can be deleted or corrupted; your systems may be used to launch another attack on another's system. Some common types of malware include:

Adware: a revenue generating tool for advertisers. Generally more annoying than dangerous, although often comes bundled with Spyware or other forms of malware.

Bot: a software program designed to automatically and remotely perform some task. Collections of Bots are called Botnets, and are used to perform activities such as mass mailing of spam/spy ware, DDoS attacks.

Bug: a bug is a common term used to refer to a flaw in a software program. Some bugs lie undetected for years. Bugs can give rise to vulnerabilities which, if exploited, enable unauthorised access to IT systems.

Cryptoware: identifies files on a victim's computer that are likely to be valuable, e.g photos, letters, videos, etc, and then encrypts them so that the victim cannot read them until a ransom is paid.

DoS: a denial of service attack overwhelms a system, e.g. a website, by sending it more network traffic than the system can cope with rendering it useless. Often this is followed by a ransom demand.

DDoS: a distributed denial of service attack is a DoS attack launched by thousands of sources simultaneously, such as a Bot net. Typically used against large corporate systems with large network capacity.

Keyloggers: a form of Spyware that can record your keystrokes and send them to a remote attacker, revealing everything that you type, including all your usernames and passwords.

Phishing: individually targeted malware, usually by an Email faked as if to appear to be from a known contact. The Email will contain a link to a malicious website and/or run malicious code clicked.

Ransomware: holds a client to ransom after performing some malicious act, e.g. defacing a website, or crashing a web server. The victim has to pay a ransom for the damage to be reversed.

Rootkit: a rootkit is a particularly dangerous piece of malware that 'buries' itself deep inside a computer's inner workings, and becomes effectively invisible to most anti-malware programs. From this privileged position it usually 'opens up a door' to allow other malware in.

Social Engineering: tricking or otherwise persuading people into revealing confidential information. This may be by phone or in person. Watching the keyboard as a user enters their password or listening in to a private conversation is a form of Social Engineering.

Spam: spam is the most common form of Email, although also seen on text messages, social media postings blogs and web forums. Spam is not malware per se, but is often used as a delivery mechanism.

Spyware: allows attackers to remotely gather data about your use of your IT systems, e.g. by watching the contents of your monitor screen. A typical use may be to track your internet usage, determine your interests, and send back targeted Adware.

Trojan: a Trojan (horse) disguises itself as legitimate program to trick users into downloading further malware.

Virus: one of the most common types of malware which attaches itself to legitimate programs and replicates itself and executes malicious code when the programs are run.

Worm: is a type of virus which self-replicates throughout IT systems automatically, typically either consuming bandwidth and over-loading networks, or 'eating' (deleting) data.

About this guide

This guide has been produced principally for the benefit of the members of the European Fencing Industry Association (EFIA). Copies can be downloaded free-of-charge in the Member Area of the EFIA website (www.efia.co.uk). The website also contains examples of cyber security policy templates, customisable for your own business.

Further information about this document can be found by contacting the author:
Bernard J KilBride
European Fencing Industry Association
The Granary
Ty Coch
Upper Llanover
Abergavenny
NP7 9LA
T: 01873 880784
E: info:efia.co.uk
W: www.efia.co.uk

Further reading and information

Books & Journals:

- Global Internet Report 2015. Mobile Evolution and Development of the Internet.
- Garnaeva M, van der Weil, J, Makrushin, D, Ivanov A, Namestnikov. Y. Kaperski Security Bulletin 2015. Kaperski Labs.
- Internet Security Threat Report. Mountain View, CA: Symantec Corporation (2015)
- Data Breach Investigations Report. Tampa, FL: Verizon Enterprises (2014)
- Hacking for Dummies. 4th edn. Hoboken: John Wiley & Sons, Inc. (2013)
- ISO/IEC 27000:2013 Information technology. London: BSI (2013)
- ISO/IEC 27001:2013 Information technology – Security techniques – Code of practice for information security management systems – requirements. London: BSI (2013)
- ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. London: BSI (2013)
- Web download: Cyber Security Consultancy Cheltenham: CESG (2015)
- Common Cyber Attacks: Reducing the Impact Cheltenham: CESG (2014)
- 10 Steps to Cyber Security. London: The Cabinet Office (2014)
- Cyber Essentials Scheme (Requirements for basic technical protection from cyber attacks). London: BiS (2014)
- The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. London: The Cabinet Office (2011)
- Cyberstreetwise (Small businesses: What you need to know about cyber security). London: BiS (2015)
- The Standard for Information Assurance for Small and Medium Sized Enterprises – Issue 3.0. Malvern: IASME Consortium (2013)
- The Standard of Good Practice for Information Security. London: Information Security Framework Ltd (2015)
- ICC Cyber Security Guide for Businesses ISBN 978-92-842-0336-9. Paris: ICC (2015)
- Data Breach Investigations Report. Tampa, FL: Verizon Enterprises. (2014)

Websites:

- The Cyber Essentials Scheme: - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf
- About the ISO27k Standards - http://www.iso27001security.com/html/iso27000.html
- Top 125 Network Security Tools - http://sectools.org/
- Top global hacks - http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- CVE security vulnerability database. Security vulnerabilities, exploits, references and more - https://www.cvedetails.com/google-search-results.php?q=Windows+7&sa=Search
- Types of malware - https://www.veracode.co.uk/blog/2012/10/common-malware-types-cybersecurity-101