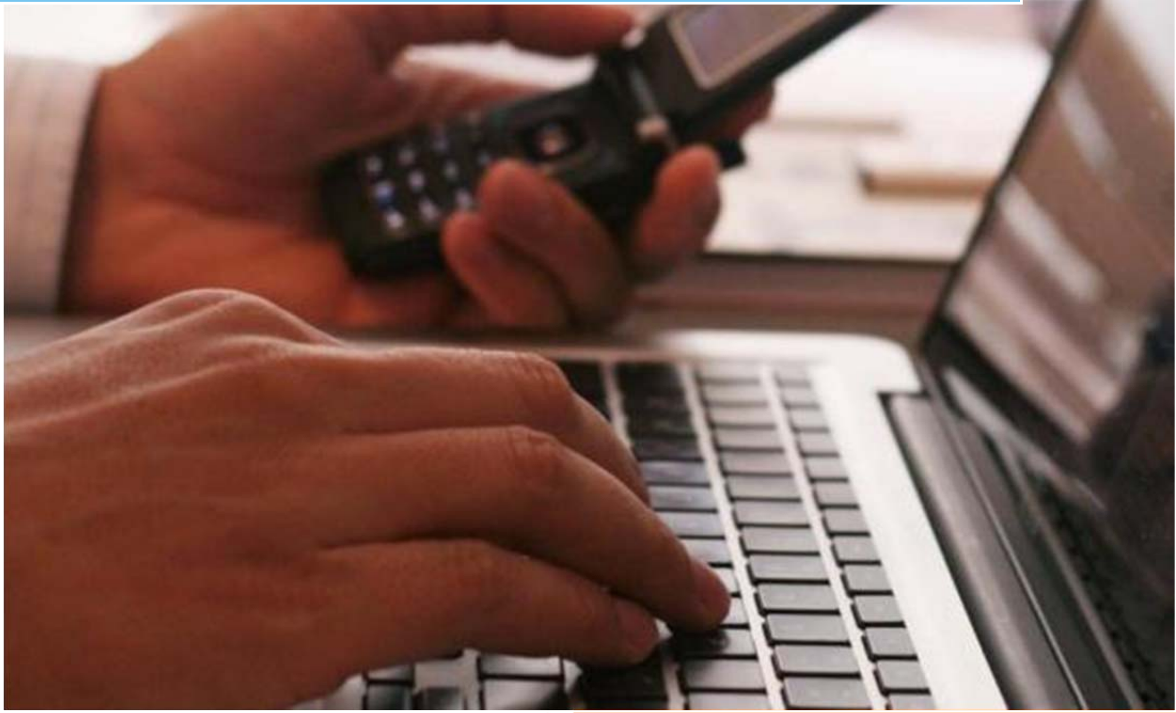
2011

Security Essentials for the Small – Medium Business



T Wake CISSP CISM CEH

Halkyn Consulting Ltd

www.halkynconsulting.co.uk

Contents

Guide to Security for the Small – Medium Business:

What this guide is:

No two companies face the same risks. However, every business needs to keep its physical and intangible assets safe. Indeed, your company might even face prosecution for failing to secure certain assets.

More positively, adopting simple and cost-effective security policies will bring you on-going financial benefits and can increase your customers' confidence.

This guide gives a quick overview of first steps you can take to improve your company's security. It will help you to consider what risks you may face and understand what you need to do to protect your organisation.

Who should read this guide:

This guide is written for owners and managers of small to medium firms. While the largest companies have access to full-time security experts, owners of small to medium size businesses must make their own decisions about what security they need.

What to do next:

This guide is your first step to identifying the risks to your business and planning strategies on how to counter them minimise or counter them.

Look at your business processes and consider any areas of potential vulnerability. Draw up risk management strategies, ensuring that any changes to your systems and procedures are based on realistic assessments of the relative likelihood and potential severity of threats. If necessary or appropriate, get expert advice.

Halkyn Consulting Ltd offer a range of security services, including risk assessments and policy development, which are suitable for small – medium businesses and individuals looking at identifying the real security risks they face. Our services can assist with peace of mind and help you win future contracts. For more information visit www.halkynconsulting.co.uk today.

Top Ten Tips for Good Security Practice

1 Know your assets
2 Identify your threats and risks
3 Select your staff
4 Guard your perimeter
5 Secure your IT
6 Educate your employees
7 Back up, Back up, Back up
8 Update when it makes sense
9 Investigate incidents
10 Find and fix problems immediately

Know your assets

At a most basic level, before you can improve your businesses security, you need know what it is that you want to protect.

You are already likely to have a strong control of your stock inventory but do you have the same with the rest of the important assets that keep your business running?

At this stage, it is essential that some time is spent cataloguing the things that make your business tick, so spend some time here. Make sure you don't just concentrate on what your business produces or handles on behalf of your customers (although these are important). You need to work out what you have that allows you to do business – you may be surprised at how much you have in the way of important assets.

Some examples to consider (in no particular order) are:

- **Stock** – If your business relies on stock, then without it you don't work. While you may already have an excellent stock inventory system, it is worth making sure that you still include the obvious things when you compile your asset register.
- **Business Tools** – these are the things you need to work, if you are a plumber you need spanners, if you are a hairdresser you need clippers. Without these assets, your business can not function.
- **Customer Confidences** – sometimes neglected, but always important. You need to consider what your customers entrust into your care. Apart from obvious things, this includes items which can have an unexpected value – home addresses, bank account details, even simply knowing when they are away on holiday. Losing this sort of information can not only destroy your customers trust but it can result in serious fines (up to £500,000) or criminal charges.
- **Supporting Infrastructure** – in addition to your main business tools, there will be things (physical objects and information) that you need to allow your business to run properly. Using the hairdresser example, clippers are an essential tool, but the chair and mirror provide supporting infrastructure. It is possible to work without them, but it won't be nice.

Anything that is important to you is important to someone else…

- **Business Information** – you need to properly identify all the bits of information that your business uses, not just your top secret plans for global domination, but (and this is especially important for the SME sector) your accounting information, your customer relationship information and so on.
- **Employees** – always an essential part of any business. You have spent time selecting and hiring good quality staff so it makes sense to look after them once they are working for you. ***Don't forget, if you have employees you will often be legally responsible for their safety and security in the workplace.***
- **Premises / location** – Some businesses can work perfectly well from anywhere, but if you have locations where you need to be (shop fronts, warehouses etc.) then these become assets you need to identify.
- **Reputation** – you have spent time building a brand or a name that people recognise and trust. Value this as an asset and protect it appropriately.

Remember the guiding principle here is anything that is important to you, is important to someone else. Until you find out what is important, you can't keep it safe.

If you can, put a value to your assets. This isn't just the cost of replacing something, but what you believe the costs to your business would be if the asset was lost, stolen or destroyed.

Identify threats and risks

Once you have determined what your assets are, it is time to take a realistic assessment of what threats are out there and what risks they create for your business.

This can be the hardest step, even if you know your market segment inside out. On a daily basis we are bombarded with information about crime, cyber attackers and natural disasters. It can be difficult to separate the wheat from the chaff where your business is concerned, but without this you run the risk of either being insecure or spending too much on security you don't actually need.

There are many methods to assess threats and risks and each has its strengths and weaknesses. It is important that you select the method that works best for you and your business. If you deal with clients worldwide, you face a different set of threats than someone who only interacts in their local community.

As a rule of thumb, the first step is to work out what threats you face. This can be complicated, but you can get advice from your local Police force crime reduction teams and Government (Home Office / Security Service / CPNI etc.) websites. Make sure you keep a realistic approach here – terrorism is not a significant threat to a rural dog grooming salon, for example – but remember to keep an open mind and it may be necessary to consider risks to businesses around you.

Don't forget to consider the threat from natural disasters, extreme weather events and similar. Although harder to quantify, these can be much more damaging to your business than the better publicised threats. For example, if you have identified your staff being in the office as essential to your business, a disruption to the transport network can be massively damaging.

For the purposes of this guide, we will talk about the "risks" as being some way in which you can quantify the danger that a given threat poses. The easiest and most flexible method for this is to assign the likelihood of something happening a value of 1 (very, very unlikely) to 5 (almost certain). Then do the same with the amount of damage (impact) this can cause – using 1as almost no harm to your business, and 5 as catastrophic. This allows you to multiply the two numbers to get a "risk score."

"risk score" =
likelihood x impact

Once you have a scoring system, you can quickly and easily identify what risks are actually important, and which you can ignore – at least for now.

At Halkyn Consulting we always recommend that you build a risk register, but how this looks and what it holds is really down to your needs. Whatever you decide upon, it is very useful to keep a record of your risks and what actions you have taken to mitigate them. Not only will this help ensure you stick to cost-effective measures but it can also help with meeting legal or regulatory requirements.

Select your staff

Staff can be, and probably are, one of the most essential assets your business has. Except for a sole trader, your business operations rely on your staff carrying out their duties. Getting good, productive, employees can make the difference between one company failing and one dominating the market.

Getting good, productive, employees can make the difference between one company failing and one dominating the market.

With this in mind, the only sensible option is to properly recruit and screen your prospective employees before offering them a job. Not only do you have to ensure you are getting someone trustworthy who has the right skills and potential, you have to ensure you are complying with legal obligations (such as the Immigration, Asylum and Nationality Act 2006). Remember failure to comply with the Act can result in Civil Penalties of up to £10,000 per worker.

Depending on the nature of your business, there may be additional checks that are required – such as Criminal Records Bureau (CRB) check or financial checks. Where a regulatory obligation such as this exists, it is essential that you maintain a properly accounted record of your hiring process.

In addition to meeting legal obligations, employee recruitment is a basic stage of your business' security. The "insider threat" is one of the main threats to UK businesses and this applies to all sizes of enterprises. While you may not be targeted by international criminal gangs or intelligence agencies, the low level threat is very real and very common. If you work in retail, then employee theft can be a significant source of revenue loss. If you handle sensitive data on behalf of your customers then there is a risk that this information is going to fall into the hands of criminals, which in turn will cause your business reputational damage and probable direct financial losses.

The "insider threat" is one of the main threats to UK businesses and this applies to all sizes of enterprises

There are many organisations and agencies which offer a background screening, but for most SMEs this is something that can be carried out in-house. Once your business has grown to the point at which you are recruiting many new staff, across geographically separated locations, it may be worth considering outsourcing this process.

The main points to consider when you offer a job are how you verify the following:

- Identity
- Work History
- Right to work
- Address

Depending on the nature of your business, there may be other issues to consider – such as a CRB check, credit history, driving licences, professional registration etc.

Guard your perimeter

After your employees, the next biggest vulnerability your business can face is how well you have defined and protected your perimeter. This is the case both in terms of "physical" security (doors, locks, walls, fences etc.) and the more technical IT security (where we talk in terms of Firewalls and IPS systems).

Physical

It doesn't matter if your place of work is in a shared office or an isolated workshop, it is essential that you establish some method of defining and demarcating your boundary. At the most basic level, by establishing an area that is clearly identified as belonging to your business you will provide a deterrent effect to the most casual of security risks.

While this won’t prevent a determined attacker, it forms a base level on which you can build.

Once you have defined your perimeter, you need to decide on the best way to defend this. Here, the risk register comes in handy – hopefully you will have properly identified where the risks are coming from and this will give you direction as to how you should secure the perimeter.

As with most aspects of security, this is something that is only limited by your imagination – there is a very broad selection of security measures you can chose, ranging from fences, specialist doors, alarm systems, CCTV, infrared sensors and so on. If you are in any doubt here, it is well worth seeking professional advice but make sure that any security measures are proportionate to the risks you face.

Technical

In a similar manner to the provision of physical measures to demarcate your boundaries and deter intruders, when it comes to your computer systems a perimeter must be in place and it makes sense to make sure you have some form of alarms.

Rather than a fence or wall, when considering your network, the perimeter becomes your firewalls and routers.

Even if your internet connection is provided by an ISP (such as BT or Virgin Media), you still need to have at least one firewall between your business and the internet. While the ISP filters will keep out a lot of the bad people, you really can’t rely on it as your only line of defence.

When considering your network, the perimeter becomes your firewalls and routers

To keep this firewall effective, you also need to have a process in place by which your firewalls are regularly updated with the latest patches. If you do have a business network that you want to connect to the internet, it makes sense to make sure you either employ skilled network managers or you outsource to an appropriate provider.

Remember, when it comes to technical attacks, unlike physical attacks, it is very cost effective for hostile parties to mount a persistent series of attempts. This means that any internet facing connections you have will be scrutinised by a variety of malicious individuals – here you need to keep your defences strong all the time.

Secure your IT

Following on from protecting your IT perimeter you also need to make sure all your business IT assets are protected from likely threats.

Again, this is where your asset register and risk registers come into play. You need to ensure that all your business IT assets are accounted for and protected, because in a networked environment, your security really is only as good as its weakest link.

In this section we will look at some of the common types of business IT you need to consider, and some ideas about how you can protect them. This is not an exhaustive list and every business will have different needs. Also please remember that any regulatory obligations will need to be factored in – such as complying with the Payment Card Industry security requirements (PCI-DSS) if you process card data.

PCI-DSS is a global standard designed to help reduce credit card fraud.

For a detailed assessment of your requirements, we suggest you contact a specialist security company for advice.

Standalone IT assets

Although it is rare now, there are going to be several reasons why you may need to have a computer (or similar device) that doesn't connect to anything else but performs a critical business function. Some examples can include bespoke DTP applications or CAD equipment.

While it may seem "more secure" to have a computer that is not connected to anything else, there are still risks you face which need to be protected against. To assess these you need to consider possible scenarios where your IT asset could be damaged or compromised and the impact on your business if this happens.

One of the most significant concerns about an isolated asset is what happens if it is broken (accidents happen, fire & flood damage etc.). When you are unable to take advantage of things like network back up, you need to ensure that you have a rigorous process in place.

It is a common misconception that standalone equipment doesn't need to be locked down to the degree that network devices do. In reality you still need to make sure your user accounts are properly managed, your software is patched properly and that there is a good anti-virus scanner in place.

Networked IT assets

If your computer is connected to others, either on a local network or over the internet, then it faces a different variety of threats. Here it is likely that malicious individuals and groups will be actively scanning your machine for vulnerabilities. When one is found, it is likely to be exploited quite quickly – sometimes without you finding out until it is too late.

Even if you believe that your business doesn't hold anything that someone would want to steal over the internet (and this is unlikely, remember if you value it, it has value to others as well), you face the risk of your network being used to mount an attack on someone else. For some businesses this can be even more serious than having your own data stolen, as you could end up being held accountable for the target system going down and you are likely to suffer serious reputational damage.

An additional concern with internet-connected computers is the activity of your staff on the internet. In most businesses there are significant benefits from allowing your staff to access websites but there are still risks that have to be considered. In addition to the possibility that your employees may inadvertently allow malicious software on to your network, there is the risk that something your employees say or do leaves your company open to adverse publicity or legal action. In general terms, anything that your employees say or do on the internet, in work time and using work equipment is likely to be deemed as if it is done with your business' approval.

Remember, you are likely to be held responsible for what your employees do online.

This is especially important if there is criminal behaviour taking place. To avoid the possibility of being caught up in any legal action, you need to ensure you have a well-documented policy on what your employees can and can't do online.

You can protect against this by taking a common sense approach – make sure there is a firewall in place; make sure as much of your operating system security is enabled as possible; educate your users about passwords; use web / email filtering software; enable logging on your systems; document your acceptable use policies and ensure all staff are aware of the rules.

Portable IT assets

When it comes to easily portable assets (such as laptops, netbooks, PDAs and even portable Chip and Pin readers) all of the above apply but you have the extra added concerns that come from these devices being easily portable and of high value to opportunist theives.

The biggest advantage portable devices bring to your business is the ability for your employees to work in a variety of locations – such as at home or in coffee shops – which can bring a dramatic increase to your productivity. But this needs to be done in a manner in which the extra risks are properly considered.

At a basic level, every portable device should be given some form of whole disk encryption so that your data is protected if the device is stolen or lost. In addition all staff who are given portable devices should be educated about safe usage – this includes things like not carrying laptops in obvious laptop bags, not leaving them unattended in public places (even while going to the toilet) and depending on the sensitivity of your data, making sure that when working on them no one can look over their shoulders.

In addition, you should ensure that your staff are provided with a means to lock away their equipment – both in, and not in use. This is often in the form of a Kensington Lock to secure laptops to furniture, but you also need to make sure employees are properly trained in what objects to pick. There is little value in securing a laptop to another easily stolen object.

If you allow your portable assets to connect to your business network – often the case when you allow staff to work from home – then it is important that you consider how you will enable this access. As a minimum you need to be able to establish a VPN and have a better level of authentication (such as two-factor). These two measures will go a long way to reducing the risk from this opening to your network.

When it comes to portable chip and pin devices you have to ensure that the data they send back to your payment processing systems is encrypted – this is a requirement of PCI-DSS. While these are less likely to be taken off your premises, any vulnerability can lead to significant reputational damage and financial losses.

Make sure you know what regulatory requirements apply.

Tips for IT Security

So, in summary, some things to consider regarding your IT Security are:

- Make sure your IT assets are physically protected. Lock doors and windows when offices aren't in use and use devices such as Kensington Locks to secure laptops. Server rooms should be given extra physical protection.
- Employ a good password policy and ensure your employees understand what this entails.
- Make sure your machines have a password protected screensaver and that this kicks in after a set amount of time.
- Have a system by which you make sure your Operating System and important applications are kept up to date with patches.
- Always have an anti-virus / anti-malware application.
- If you need a wireless network, take the time to employ the best encryption the hardware will support.
- Make sure logging is turned on where ever possible. This will allow you to know who is doing what on your network.
- Take additional measures for portable devices / remote workers.
- Produce acceptable use policies for all your assets, making it clear what you allow your employees to do with company equipment.
- Most importantly, make sure all your employees are fully aware of their role in securing your business.

Educate your employees

Although this is an often neglected aspect of your security, it really is essential. You can have the best security systems in the world, but if your employees don't understand them, and know how to operate them, they are going to be ineffective.

As previously mentioned, your staff can pose a significant risk ("insider threat") and even without being malicious, they are well placed for accidents to damage your business.

The three main areas in which you should ensure staff are educated – both on appointment and during their time in your employ – are:

If you create policy documents, make sure your staff read and understand them,

1. Policies. You have gone to the effort of creating these, make sure all your employees have read them and understand them.
2. Physical Security. Make sure all your employees understand what is required of them to ensure that your physical security measures are maintained. This can include things like being able to set the alarm, making sure doors and windows are locked, and how they interact with customers.
3. Information Security. Possibly the area that will need the most effort. Educate your employees about how to use their passwords, what sort of information they should be storing (and how), what they can and can't talk about outside work and so on.

It is important for you, as the business owner, to remember that a significant amount of security breaches result from the mistakes of employees. The term "social engineering" is widespread and often proves to be a cost-effective measure for attackers.

By spending a bit of time to educate your staff, you invert this and make it a very cost effective way in which you can block attackers.

Back up, Back up, Back up

It can't be overstated. You must ensure that all your business data is backed up. You must ensure that your backups work and are properly protected. You must have a process in place which rotates your backups so that you know the set periods in which you can recreate your data if needed.

This is fairly straightforward and something most people are aware of. The hard part seems to be putting it into practice.

You must ensure that your business takes the time and effort, though.

Like all insurance policies, we hope you will never need them, but the reality is that if you don't back up you will at some point suffer a catastrophic data loss. Only you can know how well your business can recover from this but it is better to never find out for definite.

How you back up – what devices, how often etc. – will depend entirely on what your IT systems are like. As a general rule of thumb, at Halkyn Consulting we recommend that, as a minimum, you back up your application data (for example, word processor documents) daily and have a weekly / monthly archive system whereby your data is stored offsite. Backing up applications themselves may be less important, but this will be governed by your particular needs.

When it comes to the backup media, there are some things you need to bear in mind:

- Protect your backups in the same manner as you protect the original data. This can include encrypting the media or locking it in secure storage.
- Make sure that you can read it if your main system goes down. There is no point having encrypted backups if the key to decrypt them can only be found on the main system.
- Keep your backups away from the parent data. Ideally back up media should be stored far enough away that a single incident can't destroy both the working system and the disks. If you don't have off-site storage, then you can consider the use of fireproof safes and the like.
- Test the backups. Have a regular schedule by which you verify that the backup media is intact and working, that your processes don't corrupt the data and that you are fully able to restore it if required. The last thing you want to do is discover a problem when you have nothing else but backup disks.

Protect your backups in the same way you protect the original data!

One additional point – don't forget to "backup" paper documents you have. Although often overlooked, the loss of paper hardcopy documents can be just as damaging as losing your IT assets.

Make sure any business related paper data is copied (and certified if required) or scanned onto your IT, and then stored off site in the same manner as back up media.

Update when it makes sense

Whatever operating system or applications you use, make sure you have some way of testing and installing patches when they get released by the developers. Not only should you do this for the obvious software (such as your PC Operating System or word processor) but for as much of your technical equipment as possible. Depending on the nature of your alarms, CCTV, AACS Card Readers (and so on), you may need to establish some method of making sure these are kept up to date.

Patching is generally a good idea. When vulnerabilities (such as ones that allow virus / worm attacks) are identified, most software producers will create a way to prevent this and issue the new code as a patch. Normally this follows a predictable pattern (such as "Patch Tuesday," where Microsoft issue patches on the second Tuesday of each month) but critical updates - normally ones which address serious vulnerabilities – can be released at any time.

The downside of regular patch cycles is that it can give malicious hackers an opportunity to exploit the vulnerabilities before users have got round to installing the patches. For a day or two after patches are released, there is often a flurry of activity in which "script kiddies" make use of automatic attacks to find unpatched systems.

For the home user, the advice is often to simply install every patch as it is released. However this isn't always ideal for business users as occasionally patches on one product may impact others, or may impact how you use the application.

If you have specific applications, which are essential to your business then your patching process must take into account an assessment of what the risks are before deciding what to update. If your organisation relies heavily on IT, with business critical applications running, then it makes sense to develop a formal "patching board" process in which your IT personnel are given the chance to decide what should be updated.

Boundary firewalls and similar devices should always be patched

When it comes to security devices / applications, such as firewalls, then it nearly always makes sense to apply patches as they are released. Here the likelihood of something new breaking something you do is very low, and there is a genuine security risk that comes from running an unpatched boundary device.

Investigate incidents

If you suspect a crime has taken place, call the Police immediately.

It is a simple fact of life that no matter how good your security is, eventually something will fail. Security incidents are always going to happen, so you should develop a practical incident management policy well in advance. Every incident, no matter how minor it may seem, should be investigated and any lessons learned applied to your security plan.

The first thing to remember is that not all incidents are created equal – you need to be able to assess the nature of the incident and have a proportionate response. Very minor incidents (such as "near misses") will obviously need to be treated differently from major ones (such as a break-in where all your stock is stolen).

The next thing to keep in mind is that investigating a security incident should never be done with "blame" in mind. You may need to interview your employees and if they feel that the outcome will be disciplinary action they are less likely to be honest and forthcoming.

If at any stage of a security incident (either during the incident response or post incident investigation) you suspect a crime has taken place you need to inform the police immediately. Your incident response instructions should include relevant contact details for law enforcement agencies.

There will be stages during a security investigation where you may want to consider disciplinary action against employees. Before you do this, it is worth considering the effect this action will have on your other employees – for example will it discourage them from reporting incidents? – and ensure that you have engaged your HR department at the earliest possible stage.

There is no set method for security investigations, it really does depend on the nature of the incident, but at Halkyn Consulting we recommend you use a methodological approach working back from "now" to the point at which the incident occurred and then continue as far as possible.

Once you have carried out an investigation, it is important that you document the "lessons learned" from the incident. This will help you allocate security resources in the future and help ensure that your risk management strategy is based on genuine threats.

Find and fix problems immediately

In addition to incidents, you will frequently have to deal with more mundane problems on a frequent basis. Your risk management strategy should be set up in a manner that allows you to assess these and fix them. Remember, the longer you leave a problem, the greater the risk.

Security problems come in many forms – from a broken lock, to loose wiring on an alarm system, to a corrupted firewall rulebase. None of these would normally be treated as an incident, but all of them can serve to undermine your security.

Part of your routine work processes should involve some mechanism by which you can check your security equipment – looking for signs of wear and tear, possible failed intrusion attempts etc. The frequency with which this takes place will be driven by your business needs and the level of wear and tear the equipment faces. For example, door locks should be checked at least weekly, but the wires for an alarm system could be checked on a six monthly basis, or after severe weather. The more critical the assets being protected, the more frequent the checks should be.

If the routine checks identify wear and tear, then you should consider immediately repairing the damage or removing it from use. This will depend heavily on your risk management strategy, but in general if you have had a reason to install a security device, then it is probably worth repairing it. Remember, until you repair the damage, you should treat the security device as non-functioning and record this in your risk register.

Also, if your routine checks identify damage which is not wear and tear, then this should be treated as an incident and responded to appropriately.

Glossary

AACS Automatic Access Control System – usually some form of ID card reader that controls entry doors / turnstiles.

CAD Computer Aided Design

CCTV Closed Circuit Television, although nowadays this term also includes camera systems that broadcast over networks.

CPNI Centre for the Protection of National Infrastructure.

DTP Desk Top Publishing

ICO Information Commissioners Office

IDS Intrusion Detection System – this can be software that detects hackers trying to infiltrate your network or, in the physical security area it includes things like burglar alarms, movement sensors and the like.

IPS Intrusion Prevention System – similar to IDS, the IPS software will try to identify malicious activity, log it and prevent it from taking place.

ISP Internet Service Provider – this is the company that provides your connection to the internet.

IT Information Technology

Malware Malicious software. This includes computer viruses and other forms of technical attack.

OS Operating System – the software that runs your computer. Common examples are Windows 7 or Mac OS X.

PCI-DSS Payment Card Industry – Data Security Standard. This is a set of security obligations you must meet in order to process payment card (Credit Cards) information.

PIDS Perimeter Intrusion Detection System – normally refers to devices you set up on your perimeter to give you early warning of intruders.

Rootkit A type of Malware that allows an attacker to compromise the administration account on the target IT asset.

Script Kiddie A technically inexperienced hacker who makes use of automated attacks that have been created by others.

Social Engineering A method by which an attacker tries to convince your employees that they have a legitimate reason to either be somewhere or have some access that they normally wouldn't be allowed.

Who We Are

Halkyn Consulting is an independent security consultancy. We don't supply security equipment or services and we don't have links to other businesses. Our advice is unbiased and objective. We are committed only to providing our clients with the most cost-effective and complete security solutions for their needs.

Based in North Wales, we have experience across the full spectrum from security concerned individuals, to small-medium enterprises and world-leading multinational corporations.

Our breadth of experience covers physical & IT security, counter terrorist work, business continuity, threat & vulnerability reduction and regulatory compliance.

To find out more about what we can do for you, get in touch with one of our security experts today.

Email:	info@halkynconsulting.co.uk
WWW:	www.halkynconsulting.co.uk

Halkyn Consulting is a company registered in England and Wales with company number 7293628.

Registered office is 15 Llys y Nant, Pentre Halkyn, Holywell, CH8 8LN.