



IT West

# Cyber Security

---

the business  
owners guide

Phil Allatt

## Table Of Content

Introduction .....	2
It Does Not Have to Cost a Fortune .....	3
How Secure Are You Today ? .....	5
What Are the Threats.....	6
Marketing Malware .....	6
Ransom Attacks.....	6
Identify Theft.....	7
Infecting or Compromising Website Visitors .....	7
Data Theft .....	8
Malicious Intent .....	8
Why Are We Attacked.....	9
How Do We Get Attacked .....	11
Phishing.....	11
Infected or Fake Websites .....	12
Ransomware .....	12
USB Drives.....	13
Vulnerabilities in Software.....	13
Denial Of Service .....	14
Bot Nets – Spam Delivery.....	14
Lost, Stolen or Disposed.....	14
Data Harvesting & Key Logging .....	15
WiFi Networks.....	15
External Access .....	16
Brute Force Password Hacking .....	16
Cloud Services .....	17
What Should You Do .....	18
Free Resources.....	18
Where do you Start.....	18
Part of An Infrastructure Review .....	18
Not Part of An Infrastructure Review .....	19
It’s Not All About Technology .....	19
Our Process .....	20
Cyber Essentials .....	21

## Introduction

After 25 years in technology working with some of the largest corporations through to small businesses along the way, I have seen an extraordinary amount of change. This pales into insignificance compared to the exponential growth we are seeing today in cyber threats against UK business. We have put the following non-technical awareness document together to help business owners understand what you need to do to protect your business. We have gathered information from some of the leading technology and security companies in the world. These include for example Symantec, IBM & Cisco.

Reliance on technology has grown dramatically over recent years and is now the operational life blood of many organisations. Losing access to the technology you employ or the data you own may paralyse your organisation. Such situations threaten the survival of your businesses. Over this same period of time the sophistication and enormity of cyber-crime has grown exponentially.



There are now 1.2 million new pieces of malware created **every day**, that represents an 18,000% growth since 2009 <sup>1</sup>



You don't need to be a large corporation or government body to fall victim to cyber-crime. Simply accessing the internet is all it takes. An innocent click on a link in an email by one of your staff could threaten the survival of your entire business that you have worked hard to create.

As a small business you may feel you are unlikely to be the target of a hacker, but in reality the exact opposite is true. The criminal underworld has realised that smaller businesses have fewer defences in place making them an easy target. Compromising a large number of small organisations can be as valuable as a single attack on a large business. Hackers also see small companies who supply and partner with large organisations as an easier way into their primary corporate or public sector target.

A cyber threat may not always be trying to extort money or compromise your business, they may just want to recruit your technology and internet bandwidth to attack a larger prize. Organised cyber criminals control millions of zombie computers throughout the world. You may not even know your computer has been compromised, the infection just sits there waiting for the Global Command and Control Unit to instruct them to attack a single target. Even when your computer is attacking something else you may still be completely unaware it is going on.

It is important to not just consider your computers and servers in your office as the only target. The attack surface of your business is far broader than that. The complexity of technology is growing at a dramatic rate and not showing any signs of slowing down. Everything is gradually getting connected to your network and becomes a potential entry point into your business. Phones, mobiles, tablets, printers, CCTV, wireless access points, staff, websites and cloud apps are all examples of your attack surface.

1 - Symantec 2016 Internet Security Threat Report

In many cases a compromised website can be devastating for a business. If a large proportion of your income is produced by your website its protection is paramount. Even if your site is a simple online brochure for your business, it is still important. A compromised site may infect your customers when they visit or the site may be brought down for days, losing sales and credibility.



Google blacklists 10,000 websites every day <sup>2</sup>

75% of websites have un patched known vulnerabilities <sup>3</sup>



A Google Blacklisting can have a long term detrimental effect on the performance of your business. Once the infection is resolved you will need to spend time recovering your Google position.

Sitting back and thinking “it will never happen to us” is a dangerous strategy. It is no longer **IF** we get attacked it’s **WHEN**. Securing your business against cyber-crime and having the processes in place to recover from an incident is more important than putting your money in the bank.

### It Does Not Have to Cost a Fortune

Although the number of threats are extensive there are a core set of systems and processes you can put in place to dramatically harden up your defences. These initial stages do not need to cost a fortune and will deliver considerable results for the level of investment made. Some of this work can be done in house, such as instigating training or setting up policies and procedures.

IT West has provided a comprehensive range of FREE resources on line to help you undertake this with minimum or no expenditure. We are also here if you need us to help. For more details go to:

## **itwest.co.uk/cyber**

You will find a range of valuable resources including:

- On Line Video Training for staff awareness
- An analysis tool to identify your current defence level
- Standard policies and procedures
- A Process to help improve your level of security

2 – Sucuri – Specialists in Website Monitoring – managing 400,000 websites worldwide

3 – IBM Security Intelligence

Don't just take our word for it, to truly appreciate the enormity of the security task we all face today visit the Norse real time cyber-attack map.

web address: [map.norsecorp.com](http://map.norsecorp.com)



This map only represents a small proportion of the cyber-attacks happening every day.



Bret Hartman, VP and CTO of Cisco's security group reported that they see about 20 billion cyber-attacks every day



Free cyber security resources and information



[itwest.co.uk/cyber](http://itwest.co.uk/cyber)

Further advice and assistance please contact



[phil.allatt@itwest.co.uk](mailto:phil.allatt@itwest.co.uk)



01736 758370

## How Secure Are You Today ?

This section helps you gain a basic indication of the security defence level you are currently achieving within your business. Today most businesses should be aiming to get within the green segment making you 80% to 85% secure.

Your security level requirements for your website and local office network may be different. This is part of the evaluation process you need to go through to identify the criticality of each element. The decisions on what level you invest in relates to the appropriate level of risk you believe to be acceptable.

A complete security defence level analysis tool is available on the IT West website for download.

This will help you register your current security defence level and identify the scope of work to raise the level to satisfy your business requirements.

IT West also has a proven security management process which will enable you to continually manage your security position.

The remainder of this document is designed to help a business owner or senior manager understand the security threats at an appropriate level to help you make an informed decision.

IT West are available to help at any stage in the process simply as an advisor or an implementer of the security systems and processes.

Free cyber security resources and information



[itwest.co.uk/cyber](http://itwest.co.uk/cyber)

Further advice and assistance please contact



[phil.allatt@itwest.co.uk](mailto:phil.allatt@itwest.co.uk)



01736 758370

Level	Local Network	Out of 100
Basic	Anti virus, off site backup and basic password access to data	30
Reasonable	Network monitoring, Backup monitoring, regression & restore tests, strong password policies, formal disposal, effective control on cloud services.	60
Fairly secure	Strict software usage control, locked down access from the outside world, staff security training, security policies and procedures e.g. (leavers, new starters, social media), segmentation of data network e.g. segmented wireless, restricted USB drive access,	80
Secure	2 factor authentication, encrypted data on laptops, encrypted external access, authorised device access, denial of service protection, threat response procedures.	85
Very secure	Internal detection of active threats e.g. system behaviour analysis, cloud system security policies, strict change control, formal removable media control, facilities to disable lost or stolen mobile devices.	89
Maximum security	Fully managed Security Information System, simulated cyber attacks, penetration testing, security audits on new staff.	95

Level	Website	Out of 100
Basic	Off site backup, basic password access	30
Reasonable	Strict admin access control, backup monitoring, restore tests, strong password policies, multiple versions of back up	60
Fairly secure	strong firewall policies, PCI security scans, patches applied every two weeks, strong database password encryption	80
Secure	2 factor authentication for administration access, vulnerability monitoring, threat response procedure, denial of service protection	85
Very secure	real time Intrusion detection monitoring and management	89
Maximum security	Fully managed Security Information System, simulated cyber attacks, penetration testing, security audits on new staff.	95



## What Are the Threats

Security incidents are inevitable and they will vary in their business impact. A security compromise may be low risk with minimal impact all the way through to an incident that paralyses your entire business and steals your money. These incidents can also degrade your brand, erode customer trust and result in significant legal penalties. Unrecoverable compromises of this scale have been known to force the closure of a business.



### Marketing Malware

Even the low impact risks are unwelcome. This may be a simple Adware infection that just interrupts what your staff are doing with continual pop up adverts. Another example may be an intrusion that simply monitors what websites you visit allowing you to be targeted with specific adverts. These are more annoying than dangerous to your business. They can however impact productivity and make your computers unstable, potentially impacting your bottom line.

You will have noticed that a computer gradually gets slower as it is used over time. These relatively inert infections tend to be the culprit for these performance frustrations. This not only reduces the productivity of your team, it also impacts their job satisfaction, company loyalty and staff retention. If you don't take care of their productivity your staff may also lose interest in their productivity.

### Ransom Attacks

Compromising or attacking systems then holding a company to ransom is the most prevalent cyber-crime currently in operation today. Its significant success is fuelling a staggering rate of growth. The most common one that is heavily targeted at small businesses is data encryption malware. These are generally invoked by a member of staff simply clicking on an email attachment or link. Immediately the infection starts to automatically encrypt all the files it can see, this not only impacts the user's computer but the entire business network. Any file that the infected user can access could be encrypted. An entire network can be rendered unusable within minutes of the infection taking hold. This infection is followed by a ransom demand for a few thousand pounds to get the key to unlock all of your data.

 There has been a **200% growth** in new ransomware applications in the last 12 months,  the level of growth is continuing to rise <sup>4</sup>

4 - Symantec 2016 Internet Security Threat Report

Another example of a ransom attack is where a company is contacted with a threat that their website will be brought down if they don't pay the ransom. This is commonly through what's known as a Denial Of Service (DOS) attack. This involves sending an overwhelming amount of traffic to a single website which can bring it to its knees. These attacks can go on for days which will have a serious impact on a business where their web site is critical to its operation or income. Such an attack will also erode customer confidence in your brand, which may have much broader-reaching and longer-term consequences to your business.

## Identify Theft

Identify theft is another common attack on systems, generally focused on databases that hold User Name and Password combinations. Because people use the same passwords on numerous systems this data is very valuable for second phase attacks. The Linked In database was compromised and this data is still being sold for \$2000, 4 years after it was obtained. Your website is probably one of the most common targets for gathering this information.



500 Million user identities are breached every year <sup>5</sup>



You are ethically and will be legally required to inform all of your customers you have had a data breach. This allows them to change their passwords if they have been used elsewhere. This in itself can be very damaging to an organisation. The latest data protection regulations may also place a fine on companies that have had such a data breach. Fines are up to €20 Million or 4% of your annual turnover.

## Infecting or Compromising Website Visitors

A large proportion of websites have vulnerabilities, making them targets for cyber criminals. Your website may be compromised to spread malware to anyone who visits it. Hijacked websites may also have different content to promote an alternative product or service. Other infections could re-direct customers elsewhere so they put their credentials or payment details into a page that can be captured by the intruder.

A majority of your website visitors and especially those you care most about are your customers. Your website, if compromised, could quickly destroy the valuable relationships you have worked hard to nurture. In the age of social media this damaging news will not take long to spread.

5 - Symantec 2016 Internet Security Threat Report



## Data Theft

One of the most dangerous and damaging threats is where one of your user login credentials get compromised. If the attacker can gain external access to your network, armed with this information they have considerable power. If the compromised user happens to have administrative privileges the attacker may be able to gain total control over your network.

Valuable information held on your network may include for example your financial details, your customers' financial details, other sensitive customer information, deals you are making or considering, your pricing information, product designs or manufacturing processes. Additional login credentials may also be available on the network allowing the attacker to compromise other systems you may use.

Malware infections on a computer can scan the data on a network or register your keystrokes. These advanced applications are very effective at automatically finding important information on your systems. The malware transmits information back to a central command centre. With advanced intrusion technology it does not even need to be a person in your network, a program can do the job very effectively.

## Malicious Intent

Other attacks may have a malicious intent to create inconvenience or disruption to your business. Ex-employees, disgruntled customers or suppliers, even activists can get their hands on tools to cause significant disruption to your business. Unfortunately, there is an entire industry of criminals selling technology or services to compromise the technology a business employs.

Terrorists may also utilise technological solutions to compromise the prosperity of a nation. Attacking companies on a grand scale could have a significant impact on the financial stability of a nation.

Free cyber security resources and information



[itwest.co.uk/cyber](http://itwest.co.uk/cyber)

Further advice and assistance please contact



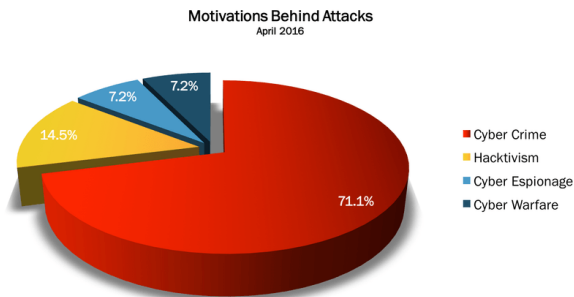
[phil.allatt@itwest.co.uk](mailto:phil.allatt@itwest.co.uk)



01736 758370

## Why Are We Attacked

There are numerous types of cyber attackers all with their own objectives. The criminal underworld with the objective of financial gain is one of the largest threats. The introduction of technology such as Bitcoin which enables anonymous payment has driven some of this recent growth. Criminals can now monetise their criminal activity in complete anonymity.



There are many other groups of individuals with alternative objectives that can be leveraged through compromising your business in one way or another.

Terrorists represent a potential threat as they become more technically advanced. The havoc they can create by compromising the commercial framework of a nation is a realistic risk.

Hackmageddon - Information Security Timelines and Statistics

Certain nation states actively employ technology to compromise business. Nation state sponsored cyber activity can have a devastating impact on the economy of a country. Some speculate that the 3<sup>rd</sup> World War may even be fought in cyber space.

Activists also known as hacktivists use cyber threats to express their point of view when they discover something they don't agree with.

Disgruntled employees or ex-employees could use their inside knowledge to impact the operation of your business. Over time our new recruits are becoming more technically savvy which makes this threat even greater.

Unethical marketing tactics employ malware to infiltrate our lives in an attempt to promote their products and learn our behaviours.

Above all else cybercrime is big business and very profitable. According to Kaspersky Lab, one of the world's fastest-growing cybersecurity companies, a cyber-criminal may get 2000% return on investment for an attack. As the cyber-criminal underworld evolves it continues to become more advanced, finding different ways to monetise its operation. We are now seeing recognisable cloud services and products including:

- Cybercrime-as-a-Service
- Cybercrime-Infrastructure-as-a-Service
- Malware-as-a-Service
- Ransomware-as-a-Service

This formalised structure is making the tools to stage an attack more accessible to a broader audience. It is now possible to rent a global Denial Of Service Botnet for £25 per hour. Ransomware is also packaged as a service and sold for as little as £50. Vulnerabilities in technology are also provided in Exploit Kits and sold to cyber criminals. New exploits get automatically distributed within a week of their release to all the users of these exploit kits.

Cyber-crime is becoming increasingly advanced technologically and very well-funded from numerous areas.

Free cyber security resources and information



[itwest.co.uk/cyber](http://itwest.co.uk/cyber)

Further advice and assistance please contact



[phil.allatt@itwest.co.uk](mailto:phil.allatt@itwest.co.uk)



01736 758370

## How Do We Get Attacked

Over the years cyber-attacks have become far more sophisticated, improving the attackers' success rates. Greater success coupled with increased capability through advanced threat automation, means cyber-crime is developing rapidly. There is a continual battle for supremacy between the security defence industry and the cyber criminals. It is important to continually review your defences to ensure an acceptable level of protection is in place.

In the early days there were single phase attacks where a simple virus had a single, self-contained attack objective. We are now seeing a coordinated series of attacks that collectively work towards an end goal. The ingenuity of these attacks is also continuing to evolve at a rapid pace. Not that long ago malware could be spotted by simply comparing them to a database of file names. Malware is now perfecting the art of disguise.

Heuristic technology has been employed for a number of years now to try and detect the behaviour of malware to thwart their advance. A single piece of malware will automatically and continually change shape allowing it to avoid detection.



A single virus may change its disguise by mutating thousands of times a day <sup>5</sup>



Infections are also now changing behaviour making them increasingly difficult to identify using the single layer anti-malware and anti-virus defence solutions. Although anti-virus or anti-malware provides a level of detection, you should not allow them to offer a false sense of security. Unfortunately, a large proportion of modern attacks continually manage to bypass current day anti-virus technology.

### Phishing

Phishing is a very common method used to attempt a system infection or extract sensitive information from users. A large proportion of phishing attacks are delivered via email trying to persuade unsuspecting users to click on an attachment or a link. Advanced techniques are being adopted to make the phishing email look increasingly authentic. The attacker will invest time learning about an organisation or the individual and personalise the communication based on what they have found. This is referred to as Spear Phishing which achieves a far greater hit rate.

Phishing is also executed via SMS or by phone, all with the intent to trick the recipient into doing something or divulging something sensitive. Social Media is a growing channel to deploy these same phishing exploits.

5 - BBC – Spencer Kelly - How malware disguises itself to avoid detection

## Infected or Fake Websites

75% of legitimate websites have known security vulnerabilities<sup>6</sup> making them a key target for attackers. Popular content management systems such as WordPress are a particular focus due to their market share. An organisation's legitimate website can be infected to distribute malware to website visitors. Importantly a majority of your website visitors are your most valuable asset; your customers.

The other technique is to trick a visitor into doing something they did not intend to do. A website visitor may be transparently redirected to a fake website. The fake website may be designed to look exactly like the site they came from so the visitor is oblivious to the fact that they have moved to another website. Alternatively, the attacker may have injected their own fake content directly into the legitimate website. A fake form may ask for information, the cyber-criminal sits behind that website simply collecting the entered data. This information allows them to undertake the next phase of their attack.

Unsuspecting users are also coerced towards a fake website via a link in a phishing email. A fake domain may be registered so for example: xyzcompany.com may be the legitimate site and the fake site may be xyz-company.com. The fake website can be easily set up to look exactly like the legitimate one. The user does not notice this slight variation in the domain name and innocently browses around filling in forms and logging in. All of this data is collected and employed in a second phase attack.

## Ransomware

Ransomware is a payload that may be delivered as part of a successful phishing attack. This infection encrypts the data on the computer and network rendering all your data useless. A ransom payment is requested to recover your data. Many ransomware attacks have been fixed without paying the money by restoring from a backup. The next evolution of this infection is to undertake a stealth attack on your backups first without you knowing. The software may sit on your network for a few weeks infecting the backups first then infecting your files a few weeks later. It is only when your files are encrypted that you realise you have an infection. Restoring from backups is no longer a viable option because they have also been compromised.

6 – IBM Security Intelligence

## USB Drives

Any external data devices that are plugged into the USB slot are used as a mechanism to transmit an infection. In some circumstances just the simple act of plugging in a USB stick may instantly infect a system. Viruses jump from machine to USB stick then from USB stick to machine. This is how it spreads by jumping from machine to machine via a USB stick.



One way an attacker will compromise a target organisation is to drop an infected USB stick in the car park. Someone will innocently pick it up and plug it into their machine at work. The payload is delivered and the attack starts.

There have also been cases where a bulk order of cheap branded USB drives are purchased from abroad. These devices were delivered with malware pre-installed. The USB sticks are distributed free to thousands of organisations who may become compromised once plugged in.

## Vulnerabilities in Software

A software vulnerability is a bug that exposes an interface for an attacker to exploit. This can be any piece of software we use from an operating system like Windows to a website, business application, browser or just a simple plugin like Flash. There are millions of software applications, platforms and utilities in use.

On average a vulnerability may be unknown by the software vendor for 200 days. During this time these vulnerabilities are attacked without anyone knowing. At some point, someone or something spots one of these vulnerabilities being exploited. Assuming this is one of the good guys this is reported to the software vendor and a patch is created. As soon as a patch is published this vulnerability is advertised to the wider criminal world. There are automated mechanisms to distribute these vulnerabilities to the subscribing criminals. There is a race where attacks take place before companies apply these patches to their systems.

 Facebook have paid out \$4.3 Million just for highlighting 2,400 vulnerabilities in their own software as part of their bug bounty programme  <sup>7</sup>

Flash and Java are recognised to have some of the highest levels of vulnerabilities. Most users have Flash installed on their machines and a large proportion have Java. Old unsupported software still in use such as Windows XP no longer has vulnerability patches developed so there is an increasing volume of vulnerabilities being identified and exploited.

<sup>7</sup> – The Register – Leading global online technology publication



PHP is one of the most common website programming languages. This platform is insecure by default. Anyone writing software in PHP requires extensive skills to ensure their code is written in a secure way. It is relatively easy to quickly put together an application in PHP that seems to do the job. It requires much more skill and time to develop it in a secure way. The same goes for any software development, if the considerable development skills in Facebook can make 2,400 security mistakes, imagine what someone with a “little bit of knowledge” can do. As they say “a little bit of knowledge is dangerous”. In software development terms a little bit of knowledge can be disastrous.

## Denial Of Service

A Denial Of Service attack is where an overwhelming amount of traffic is targeted onto one internet address. This is most commonly targeted towards websites to bring them down. It is also possible that the same Denial Of Service attack could be targeted at your business. This will degrade or disable your business internet access. Because it is easy and cheap to rent Denial Of Service capabilities, this is becoming more common. In some cases, it may be invoked as a malicious act. In most cases it is threatened if a ransom is not paid.

There is a lot of criminal activity to recruit computing resource with internet bandwidth to perform these actions. Malware is distributed to computers and servers so they become part of a network of zombie machines. This malicious bit of software sits there awaiting instruction from Central Command and Control facilities. These zombie machines could be PC's, servers or web servers. A single Botnet can have in excess of 10 million computers worldwide under its control. A single control centre could direct those machines to attack a single chosen target.

## Bot Nets – Spam Delivery

The same Botnet malware approach is adopted to recruit a global network of machines to send spam email. One of the largest Botnets got to a stage where it was sending 60 billion spam emails every day from a global network of machines.

## Lost, Stolen or Disposed

Gaining physical access to computers, hard drives, USB drives even paper documents is a target for a cyber-criminal. These valuable data assets can fall into the wrong hands through theft, negligence or incorrect disposal. As soon as a criminal has physical access to these assets they can access everything they want. Even if you have deleted all the information on a computer or USB drive a criminal can easily retrieve that deleted data.

Do not consider just your passwords and bank account details to be the only sensitive information you need to protect. Sophisticated approaches make use of something as simple as where you buy

things from or what courier you use. This information can be collated into the first phase of a targeted spear phishing attack.

Consider everything to be sensitive and keep it safe.

## Data Harvesting & Key Logging

Malware that finds its way undetected into your machine can hide away collecting data and recording activity. This type of malware will report findings to a Central Command and Control feeding back what it has found. The malicious software is able to search your machine and network looking for signs of useful information. This may be documents with user names and passwords in it, financial records or legal documents. These same applications can log keystrokes allowing them to recognise and record username and password combinations. As the software finds this data it transmits it back to its master.

We all have a massive range of secure log in details for all the systems and websites we access. We may even need to share that information amongst selected team members. If this information is in a plain text document like MS Word or Excel it is very easy to detect. Don't think a document password will help, it will just take an attacker a few moments longer to crack. Many people also use the same password for many systems, so once one password is compromised a second phase attack may use it to try other common systems people use. Malware can actually learn about the websites you have visited so it can create its own list to try the user name and password combination it has found.

Webcams are now employed against us in an attack. Malware has the ability to switch on your webcam allowing it to record your keyboard activity. Once again this is looking for and analysing user name and password information.

## WiFi Networks

Wireless networks need to be employed with caution because they can be used to access information. Although there are passwords or access codes on your WiFi network many are reasonably easy to break into. There are free tools that can be downloaded from the internet together with simple instructions. It is important to note that access to your WiFi network can be outside the physical boundary of your building. It may be possible for someone to access your WiFi network while sitting in your car park. If your WiFi network is on the same segment as your business network, the hacker may be able to gain access to your systems. Once in, there are numerous opportunities that allow the hacker to move on to compromise your systems.

Innocent additions to your network by a member of staff could happen without your knowledge. Someone may decide they want wireless access for their mobile phone while in the office. They may buy a £12 access point, plug it into your business network and off they go. They may not realise they have opened up a security hole in your network that someone can jump into.

Public WiFi is also an area where caution should be exercised while using. Some public WiFi may be open and insecure. This means other people on that same WiFi network may be able to see what you are doing. A person with malicious intent could insert an access point pretending to be the official WiFi point. You still get access to the WiFi however this “evil twin” is sitting in the middle, intercepting and reading the data you transmit.

## External Access

As the connected world evolves, external access and integration into third parties such as suppliers, customers and partners continue to grow. It is important to recognise that the security of your own environment is only as good as its weakest link. If you provide access to a third party and their security has a vulnerability it may compromise you. If you have people who access your network for support purposes, you need to be confident in their security and confidentiality procedures.

Although Target is a large organisation, it demonstrates the point well. Target, the large retailer in the United States had a compromise on their Point Of Sale system. It is believed this ended up costing Target somewhere in the region \$420 million. The actual compromise happened by a leak in login credentials from an air conditioning company they used in some of their stores. This demonstrates how an attack can start in one place bounce over to the business network then bounce over to the Point Of Sale retail systems.

Home users are another attack point especially if the home user is using their own technology to access your business. A shared computer used at home is exposed to numerous vulnerabilities. It may not be protected in any way and could easily transmit or expose data.

Remote and mobile users are also exposed to an increased level of security risk. The fact that systems are used outside the physical security of your premises means that their network access is also via a broad range of technologies such as public or hotel WiFi.

## Brute Force Password Hacking

If passwords are not found through some form of data compromise or spyware there are other ways hackers break into systems. Studies have shown that 60% of people use the top 1000 most common passwords or password combinations. This makes a brute force attack very simple. There is extensive analyses of common passwords from the half a million credentials stolen every year.

A brute force attack is a method used where a machine continually tries the username and password combination until one works. The power of machines today also allows an 8-character password just containing letters and numbers to be cracked relatively quickly.

## Cloud Services

Whilst tier 1 cloud services have well designed security frameworks the risk relates more towards their use and adoption. Cloud storage is an area that can be set up quickly by any member of staff and quickly spiral out of control. Staff may be able to create their own free cloud storage accounts, start saving company data, then sharing it outside of the organisation. Before you know it, a complex web of uncontrolled data is distributed outside the operational control of your business. That member of staff leaves and the data is left on their home machine and many other computers. Whilst other cloud services have the capability to be secure, the responsibility for security still resides with the business using it.

Free cyber security resources and information



[itwest.co.uk/cyber](http://itwest.co.uk/cyber)

Further advice and assistance please contact



[phil.allatt@itwest.co.uk](mailto:phil.allatt@itwest.co.uk)



01736 758370

## What Should You Do

### Free Resources

To help small and medium businesses cost effectively manage and strengthen their approach to cyber security IT West has prepared and collated a range of free resources on our website.

These can be found at: [itwest.co.uk/cyber](http://itwest.co.uk/cyber)

### Where do you Start

The first steps you take towards strengthening the cyber security of your business depends on where you are with your current network infrastructure. Although an infrastructure review strategy is another subject in its own right, it should be an integral part of your approach to security.

Our recommended strategic approach to infrastructure outlines a five-year primary review cycle. If you exercise such a strategy, you should start with where you are within this cycle. Are you planning an infrastructure review in the near future or not is the first question.

### Part of An Infrastructure Review

If you design your network correctly from the ground up a reasonable level of cyber security does not need to cost that much extra.

By starting with a Security First foundation your defences will be put in place during your network design and implementation programme.

If you are considering a review of your computing infrastructure it is important to factor in your security requirements.

The online resources on our website provides an [infrastructure scoping document](#). You can use this to help define your infrastructure review requirements.

IT West can help in a range of ways from simply providing audit and advisory services through to complete design, supply installation and support.

## Not Part of An Infrastructure Review

If you are not reviewing your infrastructure, then an audit would be a good starting point. We have created a free [Cyber Security Defence Level audit tool](#) you can download from our website.

This allows you to initially identify what security you currently have in place. The same tool also allows you to profile what you believe is necessary for your type of business. We have structured the profiling tool in order of importance and cost benefit. At the top of the list are the elements you should be doing first. As you progress down the list, cost may increase and the returns may be less.

There are a number of low cost quick wins that will have a significant impact on the level of security you have in place.

From a management perspective, the audit tool provides a cyber security grade from between 1 to 100. Having a base line is a good way to understand and monitor your progress.

## It's Not All About Technology

It is important to recognise your security level is not just a technology initiative. All areas of the business need to understand and contribute to the approach taken. Heavily locked down secure IT services may impact the efficiency of your organisation. A balance needs to be struck between operational efficiency and security. The freedom your staff have on IT equipment may need to change which needs to be handled carefully. Your staff need to understand why they can't use a free music download site on their works computer any longer.

The Cyber Security awareness of your staff is one of those high return minimum cost initiatives you can instigate immediately. This also brings them on board with the on-going programme of work you put in place.

We have produced a [staff cyber security awareness training video](#) on our website which is available for free.

Business processes, procedures and policies are another area that will heighten the level of security. Although some of these will integrate into your IT Services they need to be owned by the business and driven from the top down. Due to its importance, none compliance of your security policies should be built into your approach to disciplinary.

A standard set of policies and procedures have been prepared and made available for download at the IT West web site. The work in line with the staff cyber training videos.



## Our Process

Fixing your cyber security is not a one-time event. There is an on-going process of monitoring and review to ensure you keep on top of the ever changing landscape.

IT West has a proven process and a set of monitoring tools to help implement and maintain your cyber defence posture. More details about our [Pentagon Cyber Security Process](#) can be found at our website.



## Cyber Essentials

The information security arm of GCHQ has prepared a series of basic standards that small and medium businesses should adopt. These provide a completely independent definition of requirements with no ulterior motive other than to help protect the operational integrity of the UK.

IT West has achieved the GCHQ Cyber Essentials accreditation and we are also an Accredited Cyber Essentials Practitioners. As an ACE Practitioner we are qualified to help organisation gain their own accreditation and strengthen their security systems and processes.

Please feel free to head on over to [itwest.co.uk/cyber](http://itwest.co.uk/cyber) and use the valuable resource we have put together for you.

You are also more than welcome to get in touch by email or phone, we are always happy to help in any way we can.

Free cyber security resources and information



[itwest.co.uk/cyber](http://itwest.co.uk/cyber)

Further advice and assistance please contact



[phil.allatt@itwest.co.uk](mailto:phil.allatt@itwest.co.uk)



01736 758370