



your
workplace
technology
partner



Your simple guide to Cyber Security

#GetCyberSecure



Introduction

WHAT IS CYBER CRIME?

Although many SME's have been slow to implement adequate cyber security, believing their business would not be a target, recent high profile cyber-attacks are changing attitudes. It is not only larger organisations that need to dedicate resources to protect their networks against the increasing risk of online threats, all businesses are at risk.

As part of the governments Cyber Streetwise campaign, only 16% of respondents said that investment in cyber security was a top priority; an alarming figure considering the rapid pace of the cyber-crime which means in reality the threat has never been greater.

As with crime in the 'real-world' it is almost impossible to stop a determined criminal; however as with real world crime there are many things you can do to protect your business and make it less of a target. Cyber crime can operate in a number of ways from an individual deliberately targeting your business to viruses and malware which spread through unsecure networks.

The definition of Cyber crime, is the use of a computer as an instrument to further illegal ends. Cyber crime, especially through the Internet, has grown in importance as IT has become fundamental to the way companies operate. The breadth of cyber crime is wide and can include; breaches of personal or corporate privacy, transaction-based crimes such as fraud, money laundering, and counterfeiting or attempts to disrupt the actual workings of a company, ranging from spam, hacking, and denial of service attacks against specific sites or companies.

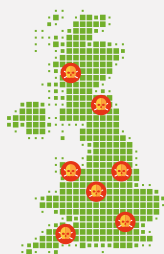
"Cyber security is massively important to a business like ours. We hold a lot of personal and confidential information about our clients; we also handle substantial sums of money through the business on a daily basis. Businesses like ours are seen as a soft target to cyber criminals. EBC Group have provided us with a series of firewalls and anti-virus protection meaning that our info and client data is much more secure and protected from cyber criminals."

*Rebecca Widdowson,
Managing Partner at Hallmark Hulme Solicitors*



Did you know?

DID YOU KNOW?

**2/3**

of large UK
businesses were
hit by cyber
breach or attack
in the past year



Almost
**six
million**
fraud and
cyber crimes
were committed
last year
in England and
Wales



The UK is
**1st most
targeted
nation in
the world**

for phishing
attacks and 2nd
for ransomware



36%
increase in
Ransomware
attacks such as
WannaCry,
which is the
fastest growing
threat



2015
saw a record
number of data
breaches of 191
million records



'Insider Threats'
committed by
current or
ex-employees are
responsible for
43%
of Data Breaches

Cyber Security

CYBER SECURITY

It is important to understand the dangers of cyber crime and that all businesses are vulnerable, but how can you prevent it?

As with a crime in the real-world it's difficult to stop a determined criminal but there are a range of security measures that you can implement which will make your business safer.

When it comes to cyber security 'prevention rather than cure' is the best method for staying cyber secure. There are methods of retrieving your data and getting a company's systems back online but it can be complicated and time consuming. Ensuring that your business is protected in the first instance is definitely the best way to stay safe.



Cyber Security Review

If you're not sure where to start, getting a cyber security audit of your IT network and the protection your business currently has in place is an excellent way to determine whether you are protected.

EBC Group offers a cyber audit of your business and can give advice on your network and systems.

To register: www.ebcgroup.co.uk/cyber-review

When thinking about becoming cyber secure there are a number of elements that your business should consider

Assess

Use penetration testing to identify known and newly emerging security vulnerabilities within your IT environment. Assess on a regular basis to keep abreast of the ever-changing security landscape.



Prevention

Having layers of protection and monitoring is essential. Using high-end technologies to track and monitor your network in real-time will keep you safer.



Processes & people

Evaluating all of your business processes to see if there is any vulnerability in the way you store and share data is vital. Your employees need to be engaged with your cyber security as people are often the weakest part of your security. From leaving passwords or devices unsecure to opening attachments and websites they shouldn't.



Continuity

Having a business continuity plan for what happens in the event of disaster is vital. Ensuring that you can get your data, applications and systems back working after an attack will mean your business can continue working.



Assess

ASSESS

We would recommend that a board level training and strategy meeting is conducted in order to set a cyber security strategy and prioritise your assets into critical, high, medium and low importance.

Penetration testing is the best way to fully ensure that your network is secure from external attacks and that you are able to demonstrate cyber security. The purpose of a penetration test is to simulate a cyber attack in order to assess your current security level, discover any vulnerabilities in your IT infrastructure and provide recommendations and guidelines in order to become more secure. After each penetration test a technical report will provide recommendations to the high, medium and low risk vulnerabilities detected. This will highlight the relevant issues and routes that might be exploited by attackers in order to compromise and gain unauthorised access to your network. Each issue highlighted includes an overview, analysis and security recommendations, which will, if implemented provide additional security and reliability of your systems and applications.

In order to ensure the integrity of the penetration testing that is carried out on our client's networks, EBC Group partner with a leading certified and professional penetration testing provider. They follow leading industry methodologies, such as OWASP and ISECOM's Open Source Security Testing Methodology Manual (OSSTMM). This means that you can be safe in the knowledge of the accuracy and veracity of the work carried out.

The penetration testing is available at 3 levels:



Vulnerability assessment: which provides a snapshot of the current status of your security and identifies any major issues. Vulnerability assessments can indicate whether you require a further evaluation of your security mechanisms.



Web Application Penetration Testing: will identify vulnerabilities within your website which could be accessed through online cyber attacks. An exploitation can result in the theft of information and irreparable damage to your systems.



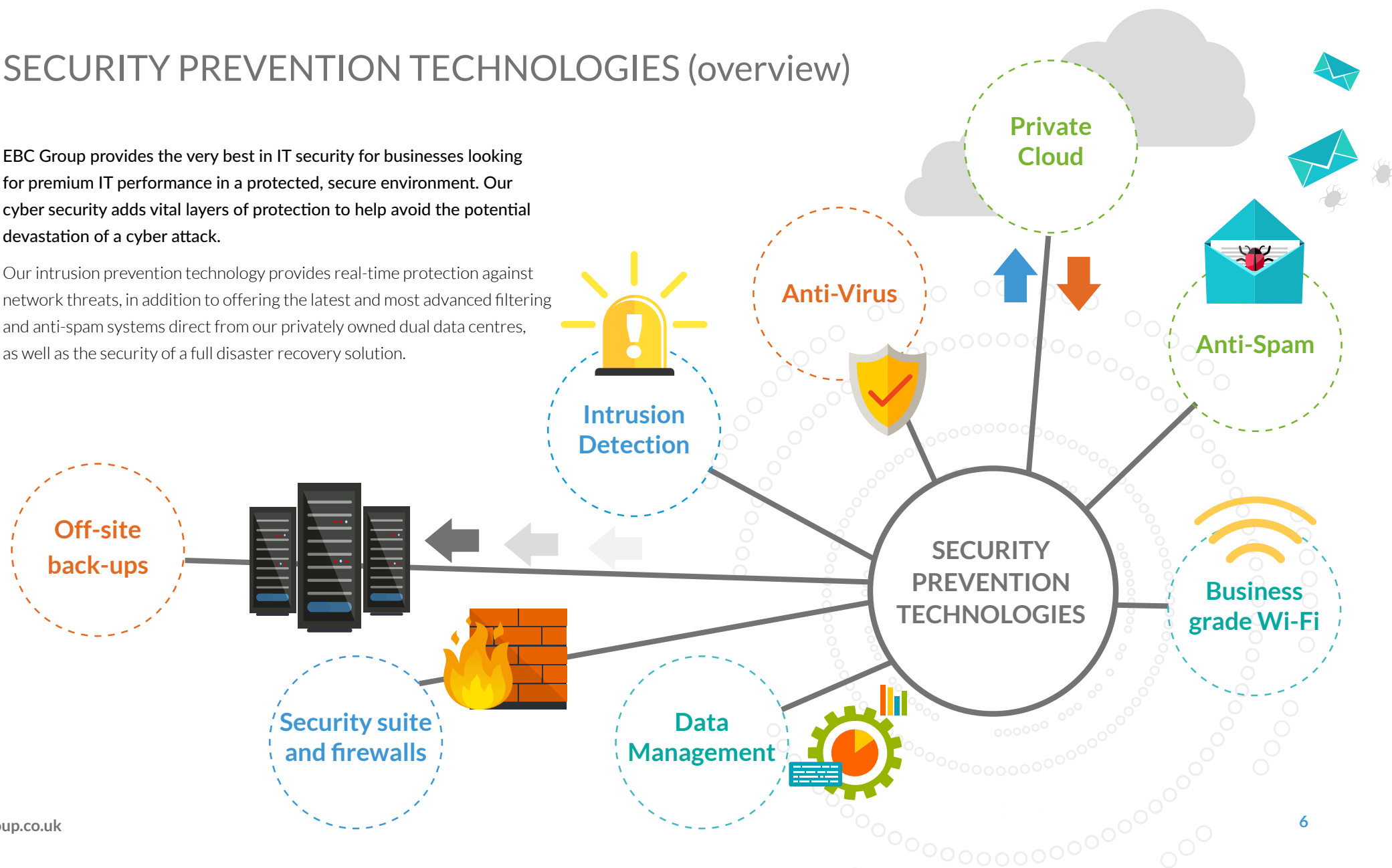
Network Penetration Testing: goes beyond vulnerability scanning and evaluates the security of a system, while attempting to expose and exploit vulnerabilities and weaknesses through a simulated attack. Bypassing known security weaknesses, the Certified Ethical Hacker (CEH) certified manual penetration testing will attempt to branch out and gain further access to other applications, databases and resources without causing any disruption or damage to your systems and processes.

Security prevention
technologies

SECURITY PREVENTION TECHNOLOGIES (overview)

EBC Group provides the very best in IT security for businesses looking for premium IT performance in a protected, secure environment. Our cyber security adds vital layers of protection to help avoid the potential devastation of a cyber attack.

Our intrusion prevention technology provides real-time protection against network threats, in addition to offering the latest and most advanced filtering and anti-spam systems direct from our privately owned dual data centres, as well as the security of a full disaster recovery solution.



SECURITY PREVENTION TECHNOLOGIES (In detail)

Security suite and firewalls

A firewall is a device that acts as a barrier to keep harmful or destructive elements out of a network. Firewalls are configured to block or prevent unauthorised access to a network. Firewall protection such as the 'Total Security Suite' from Watchguard has advanced malware protection, data loss protection, enhanced network visibility capabilities, and the ability to take action against threats.

Anti-Virus

Increasingly sophisticated viruses such as malware and ransomware are being created to breach vulnerabilities in a company's network. Anti-virus protection such as Kaspersky Endpoint is a sophisticated anti-virus tool which is designed to track these threats in real-time, ensuring it provides the most robust protection in the world.

Anti-Spam

Spam emails which are sometimes referred to as junk emails fill an employee's inbox with unwanted mail which often contains harmful links or attachments that direct the recipient to phishing or malicious websites. An anti-spam product will protect your employee's in-boxes from this harmful content.

Business grade Wi-Fi

Relying on a consumer level Wi-Fi risks leaving your network open to abuse by hackers. A business-grade Wi-Fi solution such as Xirrus means that you can keep separate logins for business and guests. Cloud managed portals means you can restrict access to undesirable website, apps and social media which may harm your network.

Intrusion Detection

Real-time monitoring of network traffic and host activity looking for traffic patterns commonly associated with an attempt to compromise the IT infrastructure.

Off-site back-ups

A backup is replication of your files and data meaning if you are hacked you can retrieve your files. However not all backups are good enough because as the ransomware encrypts your files, the backup program is often backing up the files in their newly encrypted, and therefore useless, state. A secure offsite backup in a cloud environment which is 'always' on provides an essential extra layer of protection.

Private Cloud

A private cloud environment means that your business doesn't need to connect via the internet to access your systems, applications and data which exposes your business to potential risks. With private cloud your business is not sharing your IT environment with anyone else, whereas with Public Cloud you share your resources with other businesses and your data and systems can be stored at a third party provider sometimes overseas where it is subject to different international laws.

Data Management

One of the most valuable things to a hacker is your data, whether that is to sell on to a criminal or to prevent you from getting access to it such as Ransomware. Having a Document Management system in place such as M-Files makes it harder for hackers to get to your data. Unlike mapped network folders, M-Files documents cannot be edited or changed unless they have been 'checked-out' which requires admin rights.

People & Process

PEOPLE & PROCESS

Unfortunately, staying secure is not as simple as purchasing security technology and then sitting back and doing nothing. As with security in the real world if you were to protect your business with sophisticated locks, high-tech alarms and CCTV, but, then a member of staff leaves the front door open you are still vulnerable. That's why alongside technology every business should implement simple processes and procedures to keep their networks safe.



- 1 Educate and train all of your staff about the importance of being cyber secure**
- 2 Good password management – keep it strong, long and protected!**
- 3 Never perform business tasks on an unsecure network**
- 4 Don't leave your devices unattended or unlocked, especially in public**
- 5 Be cautious when clicking on unknown attachments or links in emails**
- 6 Manage user privileges to ensure employees, visitors or contractors can only access the data they need**
- 7 Have policies in-place to ensure ex-employees can't access your data**
- 8 Using virtual desktops ensures your data is kept on a secure offsite server**
- 9 Ensure your data is backed-up and can easily be restored**
- 10 Never put unknown devices into your computers or networks**

CONTINUITY

What if the worst happens?

As this document has highlighted prevention rather than cure is the best method to keep your business safe. However, as with the real world a determined hacker may still find a way through, therefore having a disaster recovery and business continuity plan in place is vital.

Do I need a disaster recovery plan?

Could your business be without access to key data and systems? If the answer is 'no', then a disaster recovery plan should be high on your agenda. Depending on the nature of your business you could need critical elements to be recovered in days, hours or even minutes

A question that is sometimes asked is what's the difference between Backup and Disaster Recovery, aren't they just the same? Whilst both are important, backup is just one part of the disaster recovery process. Backup takes care of your data by periodically saving it in a secure location (on-site or off-site), and bringing it back to you when you need it. Disaster recovery is a function that replicates your entire computing environment – data, systems, networks, and applications – and makes it available when your primary environment is unavailable.

How EBC Group can help with disaster recovery (DR)

Our specialist team will perform full risk assessments and business analysis to identify the IT services and technology that are vital to your businesses critical operations, whilst establishing recovery time objectives (RTO's). From here, we can help write a business continuity plan that implements a system of plans and procedures to ensure your businesses critical functions can be restored and run with minimal disruption.

Powered by the world's leading cloud solution, EBC Group's disaster recovery provides a scalable solution for your business servers and desktops which let your business feel confident that whatever happens, it will be in safe hands. Our solutions range from a simple cloud backup solution to disaster recovery as a service (DRaaS). Your DR and business continuity plan will include advanced features that are optimised to work within your business environment, without impacting on your day-to-day operations.

Whether you have a physical or virtual environment, EBC Group's disaster recovery plan will provide cutting edge techniques and can backup and restore work alongside your live environments with no disruption.

Who are
EBC Group?

WHO ARE EBC GROUP?



We are your workplace technology partner. EBC Group is an award winning provider of managed services including IT support and solutions, telephony and connectivity, print solutions and document management.

As a total solutions provider we enable you to run your business, whilst we plan, implement and support your IT and technology. We are an award winning IT and technology provider and have been the trusted partner of companies for over 25 years.

We take cyber security seriously, which is why we are certified to 'Cyber Essentials Plus', the highest level of the government certification. We partner with world's leading brands such as Kaspersky Lab and Watchguard and our team is highly qualified and experienced with access to the very latest in threat protection products.

We privately own our entire IT infrastructure which means we can provide businesses with their own private cloud environment, hosted within our primary data centre with a fail-over from our secondary data centre, providing a true disaster recovery solution.


“Cyber crime has become a threat to all businesses, not just large organisations. That’s why EBC Group aim to help companies of all sizes take a more proactive approach to protecting their networks and data. By implementing the latest cyber security technologies, we are able to monitor our client’s network and proactively respond to threats to reduce their risk of an attack.”

Faisal Iqbal, IT Director EBC Group



Next steps

WHAT SHOULD YOU DO NOW?



Assess

Get a cyber specialist to conduct an audit of your IT infrastructure to see where your vulnerabilities may be



Implement

- Implement your cyber security technologies
- Train your staff and implement policies and procedures



Evaluate

- Implement a disaster recovery and business continuity plan
- Consider Cyber insurance
- Apply for Cyber Essentials to assess your company's cyber security and gain certification to prove you're cyber secure

Your next steps with EBC Group...

- 1 Discover more about Cyber Security by visiting www.ebcgroup.co.uk/cyber-security
- 2 Learn more in-depth information by attending one of our free 'Cyber Security Essentials' workshops at ebcgroup.co.uk/events
- 3 Register for a free cyber review to get advice and an audit on your cyber security www.ebcgroup.co.uk/cyber-review

Get in touch:

0121 585 4412

hello@ebcgroup.co.ukwww.ebcgroup.co.uk/contact