GET SAVVY ON CYBER CRIME

From preventing a hack to quickly bouncing back, here's how to help protect your business from cyber threats

Enterprise Nation

Direct Line®

Business owners need to wear many hats and become experts at everything from marketing to IT. That's why we, Enterprise Nation, have developed this guide to help you get to grips with cyber security and understand how to help protect your business.

By the end of it, we hope you feel empowered to take control and prevent the devastating impact of cyber crime. It might not feel easy right now, but you are taking the first step by educating yourself on the risk to your business.

STEP 1
UNDERSTANDING WHAT CYBER CRIME MEANS FOR YOU

STEP 2
PROTECTING YOUR BUSINESS

STEP 3
RECOVERING FROM A CYBER ATTACK

DIRECT LINE'S CONTACT DETAILS

Visit directlineforbusiness.co.uk/contact-us

STEP 1
UNDERSTANDING WHAT CYBER CRIME MEANS FOR YOU

What is cyber crime?

Cyber crime is criminal offences involving technology as the tool, means and target of a criminal act, or where the technology enables a 'traditional' crime such as identity theft.

According to the Crown Prosecution Service (CPS), the term cyber crime refers to any type of criminal activity conducted through, or using, an Information and Communications Technology (ICT) device.

Cyber-enabled crimes use technology to aid existing illegal activity. Lots of these attacks, such as fraud and intellectual property crime, have a serious impact on small businesses.

Some cyber crimes like Denial of Service (DDOS) attacks can completely shut down businesses' online operations. These are often motivated by profit but are sometimes simply malicious.

What impact can it have on my company?

Larger companies are more likely to experience cyber-attacks. However, the prevalence is increasing among small businesses. The UK government's 2019 Cyber Security Survey found that 28% of micro and 40% of small businesses had identified a breach or attack over the last 12 months. The same survey found that this had increased from 17% of micro-businesses and 33% of small firms just three years earlier.

Small businesses are collectively subject to almost 10,000 cyber-attacks a day, according to a report by the Federation of Small Businesses. The attacks are estimated to cost the UK economy £4.5bn.

Victims are most frequently subject to phishing attempts, with 530,000 small firms suffering from such an attack over the past two years. Hundreds of thousands of businesses also report incidences of malware, fraudulent payment requests and ransomware.

40%

of small businesses identified a cyber security breach or attack in the last 12 months.

1.3 DAYS

The time it takes micro and small businesses to deal with an attack.

£1,300

is the average loss to small firms caused by a single security breach.

Cyber attacks impact businesses in three ways:

1. Time
Waiting for IT systems to be secured, data recovered, and systems put back online wastes time – in almost one-fifth of cases reported to the 2018 Cyber Security Survey, it took businesses a day or more to recover from the breach.

Employees may be unable to do their jobs, and customers may lose access to services or are unable to buy products.

2. Cost
Cyber-attacks cause businesses to lose money through lost sales, stolen money and paying experts to fix problems. Around one-fifth of businesses impacted by cyber crime incurred repair or recovery costs. Research shows that the average cost per attack on micro-businesses is £1,300, but can go much higher than this.

3. Reputation
Cyber-attacks can lead to you losing customer confidence, as concerns about the security of information and access to services increase. Businesses have an obligation to report security breaches to customers, and within minutes you can lose the reputation you've spent years building. Local media may report the event, even if it concerns small businesses, and competitors may talk about the problem.

89%

of small businesses found their reputation was impacted by cyber crime, says government research

30%

lost clients and 29% found it difficult to win new business after a cyber attack, according to KPMG.

Common cyber threats explained

Small businesses are at risk of many forms of cyber crime. Having a broad overview of these techniques helps understand how security risks occur and what you can do to avoid them.

Fake log-in schemes: employees are directed towards fake login screens that look like common online tools. These websites capture passwords and redirect users towards the legitimate site, leaving them unaware the details have been stolen.

The primary method of defence: employee education.

Hacking: someone gains unauthorised access to a computer or network, to cause damage or steal information. A variety of tools have been developed to do this, which target security flaws in existing software.

The primary method of defence: updating your software with the latest patches and versions.

Keylogging: programmes that record the keystrokes entered into a computer. If a keylogger is maliciously installed, users will unwittingly enter passwords and other confidential information.

The primary method of defence: up-to-date virus checking software.

Phishing: victims are contacted by email, telephone or text message by someone posing as a legitimate organisation. The perpetrator is aiming to get confidential details such as bank logins and passwords.

The primary method of defence: employee training.

USB stick: leaving USBs with trojan software on for staff to find is a common method of attack. Running files from the device can infect your computer.

The primary method of defence: employee education.

Malware: software that's designed to disrupt, damage or gain access to a computer system.

The primary method of defence: up-to-date virus checking software.

Ransomware: malicious software that takes control of a business' computer system and blocks the user's access. The system remains locked until payments have been made to the cybercriminal.

The primary method of defence: up-to-date virus checking software.

> "Phishing can take place over email. The target gets sent a seemingly authentic email with a link to a fraudulent site that's mocked up to look like a genuine site like a bank. In that email you're asked to reconfirm your details. You go online and you're unwittingly putting sensitive details into a fraudulent account."

LIONEL NAIDOO, MANAGING DIRECTOR
DRAGON INFORMATION SYSTEMS

Rootkit: software used to get access to a company's computer. Having "root" access to a computer generally means privileged control over the device that allows the hacker to do what they want.

The primary method of defence:
up-to-date virus checking software.

Social engineering: cyber criminals manipulate staff into divulging confidential information such as passwords and security processes. They may pretend to be an employee or supplier, and often collate information to sound convincing.

The primary method of defence:
employee education.

Trojans: malicious software that disguises its purpose, such as being part of a downloadable game, to encourage users to install the program. It allows cyber criminals to gain access to a computer.

The primary method of defence:
up to date virus checking software.

Worms: a malware computer program that replicates itself to spread to other computers. It relies on security failures and is often simply malicious rather than profit-seeking.

The primary method of defence:
up-to-date virus checking software.

STEP 2
PROTECTING YOUR BUSINESS

"Lots of things small businesses can do to reduce the risk of being impacted by a cyber-attack take just 30 minutes, but make a huge difference to their security levels."

ROBERT DUNCAN, CISO
DIRECT LINE GROUP

It's important to think about the steps you can take to help protect your small business. Robert Duncan, Chief Information Security Officer at Direct Line Group, urged business owners to take simple steps to make their business safer.

In this section, we've outlined the steps you can take to help avoid falling victim to cyber crime.

"The key thing is having strong passwords. It's important to have different passwords for different sites. Password management is a problem. Using something like a password manager can help."

LIONEL NAIDOO, MANAGING DIRECTOR
DRAGON INFORMATION SYSTEMS

Have strong passwords

Using a different password for each service, having passwords of sufficient length and encouraging staff not to write them down, helps to reduce risk.

Train staff in data privacy

It is crucial that staff understand how data is stored and why. Being careless and transferring data to systems that are less secure, creates risks. It also reduces the quality of the data as it becomes out of date or isn't accessible to your team.

Carry out an audit of where data is stored – both internally and in external cloud-based systems. Check that each system is secure and remove any unnecessary repositories. Give existing staff an update session on how data should be handled and ensure you cover the topic during onboarding.

Download security upgrades

Hackers find flaws in everyday software that can be used to attack businesses. This includes common software like internet browsers. Hackers automate the process of scanning multiple businesses' computers for particular flaws making it easy for small businesses to be caught out.

Software providers release security upgrades when these issues are discovered. Make sure you install upgrades when prompted. If possible, set software to update automatically.

Install and update antivirus software

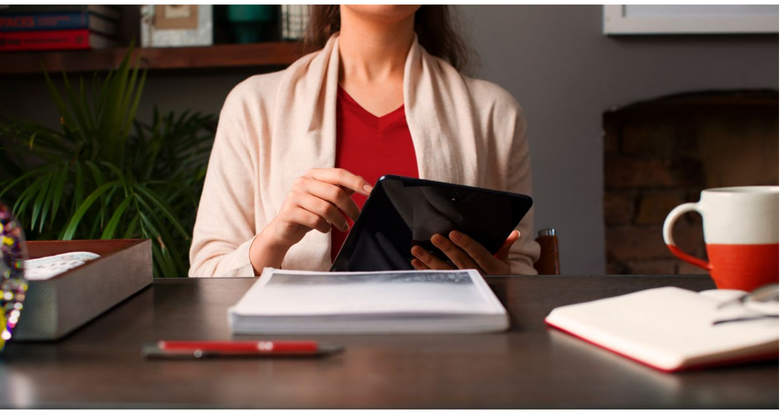
Antivirus companies are working to diagnose and prevent computer viruses as quickly as criminals create malicious programs to attack computers. This means it's really important to keep your virus software up-to-date.

Don't forget your smart devices

We're not just talking about your PC and laptop. Any device that is connected to the internet is at risk of cyber-attack. So that means regularly updating the security on your smartphones and tablets too.

Don't use public Wi-Fi hotspots when sending sensitive information, as these can be intercepted. Instead, use your 3G or 4G mobile connection or consider getting a virtual private network (VPN).

To prevent anyone physically accessing business data stored on your mobile device, set up PIN code or fingerprint recognition. You can also get software that allows you to track, remotely lock and wipe devices that are lost or stolen.



Set up two-factor authentication

Two-factor authentication relies on something a user has on their person to verify their security details. It's common for banks to provide a security device that requires a pin number to generate a code for a particular login or send a payment authentication code to someone's mobile phone.

The approach creates a significant barrier to cyber criminals. It's worth setting up two-factor authentication as standard for anything that's related to finance, such as cloud accounting software and banking.

Provide employees with devices

It's difficult to ensure laptops and mobile phones are secured properly when employees use their own technology. This includes having up-to-date antivirus software, handling data properly and not taking part in high-risk activities like visiting dangerous websites.

You need to decide whether you'll provide employees with the technology they need, such as a separate phone for work, or implement a security policy that covers their devices. Allowing staff to use their own devices may mean choosing different software to run the business. For example, you could let them work with a secure cloud system rather than storing information on their hard drive.

Backup company files

Having a backup of company files is essential to recovering from a malicious attack. Think about how regularly you want to make backups. If data is compromised and can't be recovered, you'll have to return to the last time it was backed up. Tools are available to automate this process.

Train staff to avoid social engineering

It's important that staff understand the risks posed by cyber criminals. Onboarding new employees should include a section on security, covering the topics outlined in this section, particularly the approach to passwords and devices.

STEP 3
RECOVERING FROM A CYBER-ATTACK

What to do if you're the victim of cyber crime

Taking action to respond to a cyber-attack as quickly as possible can significantly reduce its impact. Should the worst happen, insurance helps businesses deal with the impact and gets you back up and running as quickly as possible.

Identifying and containing a problem

Cyber-attacks can evolve as criminals gain access to more systems, so it's crucial to identify and contain the problem as quickly as possible. Start by changing passwords for third-party services such as online banking.

Get external support to help identify the extent of the problem – your insurance provider can be a good place to start. If your network has been compromised it normally requires a security expert to establish the extent of the problem through forensic analysis. Updated security software may identify and remove a virus but cyber criminals may have established other access points.

Reporting to relevant stakeholders

Action Fraud, the UK's national reporting centre for fraud and cyber crime, recommends that businesses, charities or other organisations call 0330 123 2040 as soon as they begin to suffer a cyber-attack. The service is available 24 hours a day, seven days a week.

Specialist advisers will ask questions to identify what type of attack you're experiencing, give you advice and pass it immediately to the National Fraud Intelligence Bureau (NFIB). After that, details will be sent to the relevant police agency which can be your local police force or the National Cyber Crime Unit (NCCU).

It's also important to share information with clients as soon as you understand the extent of the problem and immediately if they'll not be able to access services.

Customers understand that lots of companies suffer from cyber crime and they are more likely to judge you on the speed and quality of your response than the fact that you were the victim of an attack.

Keep them updated as new systems are brought back online. If possible, explain how the attack occurred to demonstrate trust and reassure them that you have taken the necessary steps to prevent it from happening in the future.

Responding to short and long-term consequences

Think about the steps you need to take to get your business back up and running. What key systems are essential? Understanding the steps to recovery will increase the speed with which you can get up and running again. Remember you're not alone – sense check your priorities with a security expert.

You'll need to implement new security processes to make sure the same issue doesn't occur in the future. Take the time to learn more about the way your business was targeted and the steps that you can put in place.

While any kind of cyber-attack is worrying and can cause damage, it's an opportunity to improve the processes in your business and replace aging IT systems.

Cyber cover helps protect your business

If you're a victim of cyber crime, Cyber Insurance will help you deal with the fallout.

If your website or network is hacked, it takes time and money to fix. Without cyber cover to help you get back on your feet, the escalating costs of fixing the problem, protecting your systems and data and implementing new cyber security could cripple a small business.

You may have also breached data protection laws or contractual obligations (such as confidentiality agreements), which means you could be faced with fines and ordered to pay compensation.

Cyber cover will safeguard your business from being overwhelmed by expenses and provide you with expert assistance as you deal with this complex problem.

The key elements of Direct Line cyber security cover

COMPUTER SYSTEM DAMAGE

If your system is attacked, Direct Line will cover the costs of:

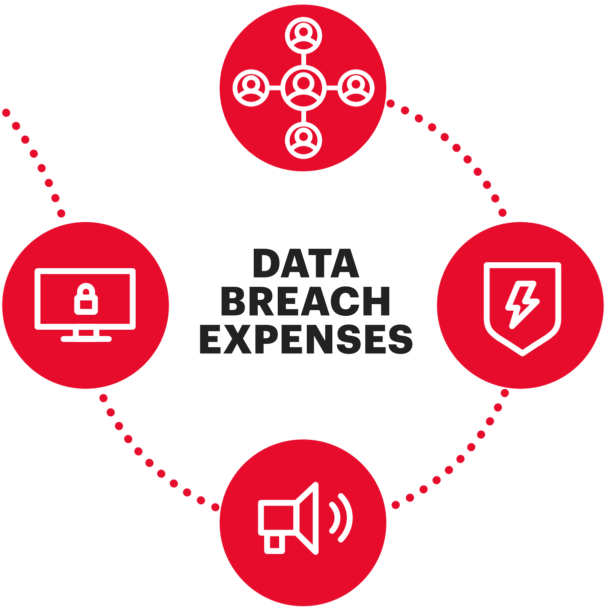
- Fixing any damage to computer systems belonging to you or a service provider.
- Locating and removing a virus from your computer system.
- Hiring professional consultants to provide advice on preventing future incidents.
- Loss of business income and the additional expense needed to minimise the impact.
- Direct Line will also cover data restoration or re-creation.

CYBER CRIME

Direct Line will cover your financial loss following:

- Social engineering, resulting in money being taken from your account or assets being transferred without your permission.
- Attempts to infiltrate your service provider's system, which results in a loss to you.
- Your computer system being hacked.
- Payments to your telephone service provider if affected by the criminal activity, should you be liable.
- If anyone threatens to perform a cyber-attack or release, publish or manipulate data, Direct Line will cover the cost of a response.
- Threats carried out by cyber criminals including payment of a ransom demand, if approved by Direct Line.

Direct Line Cyber Cover is
underwritten by U K Insurance Limited



DATA BREACH EXPENSES

DATA BREACH EXPENSES

In the event of a data security breach, Direct Line will cover the following expenses:

- Hiring professional IT services to help respond if you have failed to keep your data privacy obligations.
- Informing the data privacy regulator and other affected third parties.
- Providing support services to third parties affected by a security breach.
- Public relations and crisis-management experts to help you minimise damage to your brand, business operation and reputation.

CYBER LIABILITY

In the event that you or your service provider fail to prevent a data breach, Direct Line will cover you if:

- You unintentionally transmit or fail to prevent a virus, hacking attack or denial of service attack from your computer system.
- Someone claims against you for defamation or IP infringement (this cover may be removed if you have taken out a professional indemnity policy that already covers this risk).

CYBER LIABILITY

To see how cyber cover can help you deal with the fallout, visit Direct Line's cyber insurance page.

Enterprise Nation

Direct Line®