BlaserMills
Law

blasermills.co.uk

Online Fraud and Cybercrime

Essential knowledge for SMEs

This guide was co-authored by:

Daniel Martin, partner, head of Crime and Regulatory at Blaser Mills Law

DC Dan Maund, Police Cyber Security Advisor, South East Regional Organised Crime Unit

"Cyber-crime, by definition, is the greatest threat to every profession, every industry, every company in the world"
Ginni Rometty,
IBM Corp.'s Chairman, President and CEO

Every year Fraud and Cybercrime costs the UK economy an estimated £190 billion.

Online fraud is the fastest growing type of crime and the proceeds are often used to fund terrorism, drug importation and people trafficking.

A threat to your business

The increase of crimes committed in cyberspace means your company can be targeted from anywhere in the world by anyone at any time. Cybercriminals often aim to steal confidential information to impersonate a business, customer or supplier. This information can then be used to steal money from you or your clients. They will also seek to steal bulk personal data (known as "fullz"), which can be sold directly to other criminals on the dark web.

Types of cyber threat

Denial-of-Service (DOS) attack

: attempts to disrupt the service to a company's network. Cybercriminals send high volumes of traffic to the company's network until it can no longer function. This can lead to your customers being unable to access your company's website or place orders.

Hacking

the unauthorised intrusion into a computer or network by modifying computer software to perform a function that differs from its original purpose, often to steal confidential information. "Hacking" can be less technical than modification of software, and can include obtaining credentials via social engineering in order to commit the intrusion.

Spear Phishing

where fraudsters target an individual by email pretending to be someone in a position of trust/responsibility. The fraudster will often ask for confidential information or even request payment of a fake invoice.

Keylogging

where cybercriminals install software on to your computer that tracks each key stroke on a computer keyboard. This is done with the aim of gaining access to passwords and confidential information. These types of attacks can also include hardware – one delivery method involves dropping infected USB sticks outside company premises or giving them away at trade shows.

Malware

is software intended to cripple a network. Malware is usually disguised as a legitimate download such as an email attachment. It damages a computer as soon as the attachment is opened, allowing for confidential information to be stolen or encrypted. The two most common malware threats are Ransomware and Trojans.

Fake Invoice/Mandate

fraud often goes hand in hand with Business E-Mail Compromise (BEC). The majority of victims have had their e-mail accounts compromised and e-mail has been sent effectively as them. Most people think that fake invoice/mandate fraud emanates from domains outside the organisation, but actually the majority relate to BEC, which itself comprises over 90% of our regional victims. BEC is very easy due to widespread password reuse, poor passwords, and lack of 2FA (two factor authentication)

Sniffing

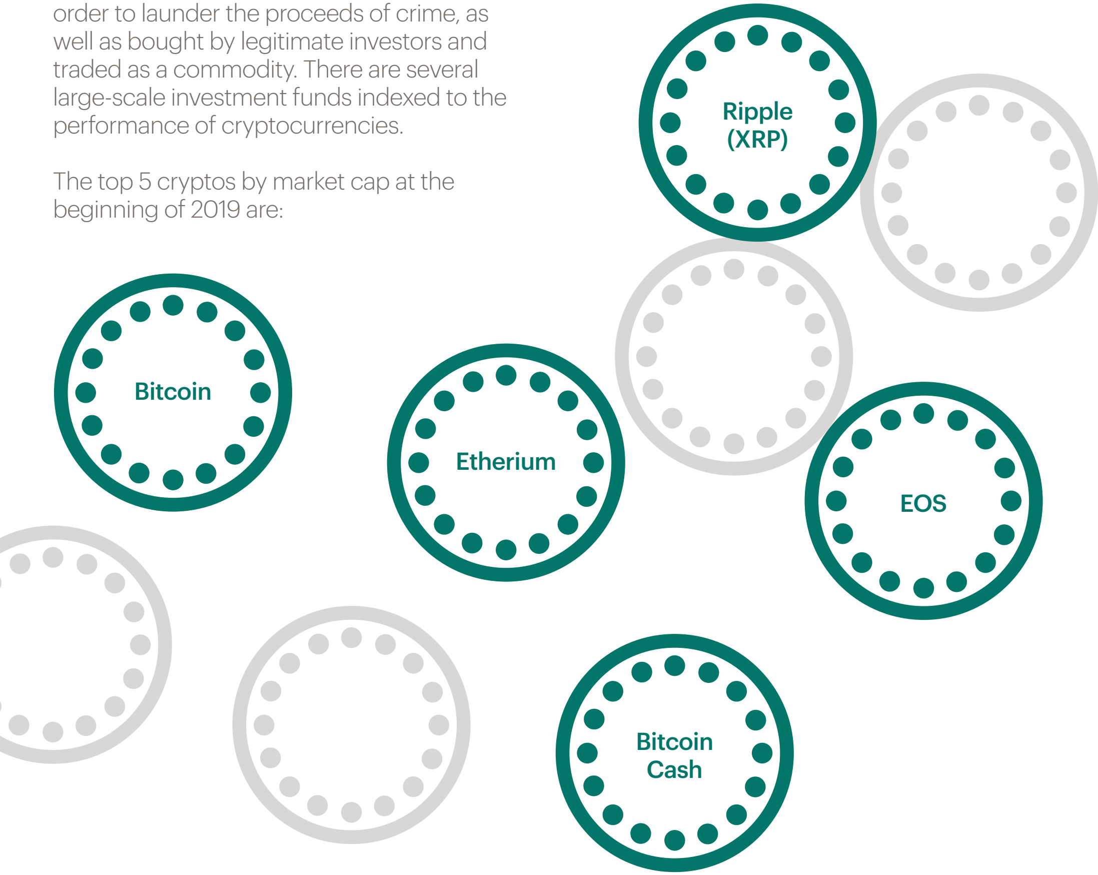
this occurs where employees use un-secured Wi-Fi networks, leaving their computers open to instrusion. When re-connected to the secure network, cybercriminals would then be given full access. The main problems that occur with unsecured Wi-Fi are MitM (man-in-the-middle attacks), Evil Twin and Rogue Access Point attacks.

Cryptocurrency

The use of cryptocurrency by cybercriminals to commit fraudulent crime is increasingly prevalent. Cryptocurrencies are a form of digital money, which are known for offering the user a higher level of anonymity than traditional currency. Transactions cannot be faked, can be actioned instantaneously and can convert and transfer value internationally that is then very difficult to trace.

The most commonly traded cryptocurrencies have several uses; they can be used by criminals to purchase illegal goods over the dark web, exchanged in order to launder the proceeds of crime, as well as bought by legitimate investors and traded as a commodity. There are several large-scale investment funds indexed to the performance of cryptocurrencies.

The top 5 cryptos by market cap at the beginning of 2019 are:



It is common for targeted hacks and malware attacks to involve demands for payment in cryptocurrency as it is more difficult for law enforcement to trace and recover.

The costs of cyberattacks in 2017-2018

The Department for Digital, Culture, Media and Sport (DCMS) recently commissioned a report entitled "Cyber Security Breaches Survey", which spoke to businesses that were materially affected as the result of a cyber-attack, for example due to loss of assets or data.

The report found that over the 2017-2018 financial year the average costs per business associated with cyberattacks were:

- £16,100 per company for medium businesses.
- £22,300 per company for large businesses.

Direct cost and recovery costs estimates tend to be higher for medium and large businesses. However, it noted that all companies affected by a cyber security breach can face the following consequences, which impact both a business' financial health and day-to-day running:

- Lost revenue where customers are unable to access online services.
- Additional staff time needed to deal with the breach or inform customers and/or stakeholders.
- Costs to repair equipment or infrastructure.
- Regulatory fines (GDPR).
- Reputational damage, which few businesses are prepared for.

Long-term costs of breaches can also include the loss of share value, the loss of investors or funding, the long-term loss of customers and staffing costs from handling customer complaints.

Ways of minimising risk

Your Employees
Discourage attacks through proper risk management training. Your workforce should be able to recognise the warning signs of malicious emails and other cyberattacks.

Employees are capable of targeting your company; it is wise to put in place policies and disciplinary procedures that are specifically aimed at discouraging internal cyber threats to your business.

PREPARE employees for a cyber attack, and make sure that they know how to react in given situations, and have immediate access to any relevant contact details. Remember, the phone systems and computers might not be working! Run simulations, just as you would for a fire drill.

Note: you can visit the ROCU page on NCSC website for free cyber awareness input from the police here.

Your Bank
Educate yourself and your employees on your bank's individual fraud and cybercrime policies. Most banks will never ask for confidential information over the telephone and will have a designated point of contact.

Your IT
The main principles are:

1. Update anti-virus software regularly and keep all operating systems and software patched.

2. Back up data – do this regularly to avoid loss of data, limit damage and allow your business to continue to trade. Verify and test backups often.

3. Strengthen passwords –NCSC advises that passwords should not be complex and use symbols and numbers as previously thought, but should be made up of 3-4 unconnected words put together in random order.

4. Switch on two factor authentication for all online platforms that support it. There is a range of popular software available that may suit your business.

5. Risk assess your IT security and act quickly to resolve any vulnerabilities.

6. Least Privilege – users should only have access to the functions and permissions that are essential for them to carry out their role.

7. Consider carrying out high risk operations (eg network admin or finance) on dedicated terminals which are "locked down" to exclude general browsing/e-mail. You can then also invest in greater endpoint security to protect these terminals more cost effectively (target hardening). Network admin accounts should never be used for general browsing/e-mail, only for the admin function.

8. Plan and Prepare for how you will respond in the event of a given attack, including media release. Test your plans

9. Once you think you're invulnerable, hire a pen tester. Then get ready to fix more holes. Repeat.

For more information and practical steps your business can take see our Cyber toolkit for SMEs further on. Also, go to www.ncsc.gov.uk which has a large volume of helpful information in relation to cyber attacks.

Insider threat
A third-party contractor was recently jailed for 18 months for carrying out a devastating cyber attack on Aviva, which involved hacking into 900 phones belonging to the insurance company. The offender pleaded guilty to carrying out the attack as revenge after falling out with colleagues at the company. He was previously a director at Esselar, a security firm who Aviva employed to run its network.

In the attack, a former director of the firm, Esselar, hacked into the system while they were delivering a security demonstration. He created a false employee identity, which he used to reject expenses claims by his former colleagues. He also hacked Esselar's social media accounts, changing the emblem to a bleeding heart, which signifies a security breach.

The attack was designed to embarrass Esselar, who estimated their direct losses to exceed £500,000, but described the full extent of the damage to be 'incalculable'. However, the case also demonstrates the insider threat posed to organisations by third-party companies contracted to provide services, and highlights the need for effective due diligence and monitoring in this area.

Online fraud in numbers

In 2018 the following cybercrime statistics were recorded:

only

27%

of businesses have formal cyber security policies in place.

Annual revenues of cybercrime:

£1.14trn

£655bn - illegal online markets
£2.29bn - crimeware and ransomware
£122bn - illicit data trading
£381bn - trade secret/IP theft

43%

of businesses experienced a cyber security breach of attack within the 2017/18 financial year.

HM Government

On 1 November 2018, the Government published its National Cyber Security Strategy 2016- 2021 in response to the growing threats to British businesses caused by cybercrime.

National Audit Office

According to the National Audit Office (NAO), cybercrime was the most common offence in 2016 with 1.9 million cyber-related incidents committed in that year. Individuals lost an estimated £10 billion, while the private sector lost a staggering £144 billion.

National Fraud Intelligence Bureau

The National Fraud Intelligence Bureau (NFIB) reported that there were 19,532 computer misuse offences recorded between April 2016 and March 2017, an increase of 48% from the previous year. More recent figures show that this upward trend continues.

Action Fraud

In the three months April-June 2018, Action Fraud received 130, 519 reports from businesses and members of the public who said they had been the victim of fraud or cybercrime.

72%

number of businesses with 250 employees or more who have been subject to a cyber breach or attack within the same 12 month period

Cyber Security Breaches Survey 2018
Bromium 2018

These attacks highlight the dangers businesses face day to day when using any digital platform.

WannaCry

Malware infected hundreds of companies including the NHS. Over 230,000 companies were attacked across 150 countries. The malware 'encrypted' computers' data and demanded a ransom of $300 to be paid using a cryptocurrency in order to release the files.

Equifax

One of the three largest US credit agencies suffered a massive security breach in May 2017, when 143 million customers found their personal information had been compromised.

Yahoo

The US internet giant was targeted in at least two separate 'state-sponsored' cyber-attacks in 2013 and 2014, which affected more than 1bn of its users' accounts.

Boomerang Video

A video game rental website was hacked and 26,331 customer details were stolen. As a result the business was issued with a £60,000 fine by the ICO.

British Airways

The airline was forced to apologise to customers and promise compensation after the details of 380,000 bank cards were stolen by hackers during a major two-week security breach of the company's website and mobile app between August and September 2018.

Facebook

Facebook's share price has dropped dramatically after 2018 saw the company blighted by data breaches and security flaws, which risked the privacy of users. The share price dropped 3% on a single day in September 2018 after Facebook announced almost 50 million of its users were left exposed after cyber attackers took advantage of a security flaw to gain control of people's accounts. The company was also fined £500,000 by the Information Commissioner's Office (ICO) for its role in the Cambridge Analytica data scandal, which saw Facebook allow access to users' pages without permission.

US newspapers

In December 2018, a cyber-attack prevented three major US newspapers from printing their papers. The LA Times, the Chicago Tribune and the Baltimore Sun, who all shared production platforms, were all hit after malware temporarily crippled the network, leading to distribution delays across the publications' readerships. While no data was believed to have been lost, several of the papers' subscribers were without a weekend newspaper due to the cyber-attack.

TJMaxx

The department store chain was an early adopter of WEP (Wi-Fi) protocol for point of sale terminals. However, when WEP was shown to be insecure and newer protocols were developed (WPA/WPA2) they were slow to respond and replace the technology. As a result, one of the largest breaches of customer credit card data took place (45.6 MILLION card numbers!)

Maersk (Global Shipping Giant) and NotPetya

NotPetya appeared to be ransomware but was in fact a wiper. It was delivered from within a legitimate software update that had been compromised at source (supply chain attack). Maersk, being a huge corporation suffered from network sprawl and had lost control and visibility of its network.

As a result, the installation of the infected file on a single computer ripped through the whole organization, causing global shutdown and led to shipping containers being held outside ports as documentation could not be raised (20 mile lorry queues outside port of NJ). Maersk had previously identified the need for an IT overhaul, but had apparently not prioritised/incentivised it to those responsible for delivering the scheme, and it had been put on the back burner. Acknowledged losses to Maersk were of the order of £400m, with the US administration dubbing it "the most costly cyberattack in history"

Cyber toolkit for SMEs

Be cyber-savvy and implement a risk management approach to protect your business.

When developing your approach you should consider and encompass the following:

People likely to target your business

Criminals: out to steal a company's valuable information, trade secrets, IP or to disrupt your business.

Script Kiddie (often for the challenge)
Hacktivist (in furtherance of some form of political/social agenda)
Organised Crime Group (for cash)
Nation State (for intelligence, competitive advantage, cash and political agenda)

Employees: a company's own employees could pose a risk to the company's cyber security. This could be through accidentally opening a fraudulent email or negligently (or even intentionally) downloading malicious software.

Regulation and Guidance

Check whether your industry regulator has published any guidelines you can follow to combat cybercrime. The Government advises SMEs to "get the basics right, and then take a risk management approach". The basics include using strong passwords, deleting suspicious emails and updating anti-virus software regularly.

GDPR

Following the introduction of the GDPR in May 2018, the Information Commissioner's Office has also launched an advice service for small businesses to ensure companies do not fall foul of the regulatory provisions on the processing of data. The ICO can take enforcement action against companies found to be in breach with serious financial consequences.

Oversight

With employees being among the highest threat-risks to most businesses it is sensible to put in place policies and training to both discourage and limit cyber threats. You should ensure that you and your staff understand the risks to the business. You should implement and oversee a culture of protecting privacy and sensitive information, as well as knowing what to do in the event of a breach to ensure compliance with the GDPR.

Data Protection Officer (DPO)

Consider training or appointing an Information Security Officer and a Data Protection Officer. Your ISO should be able to advise you on the cyber threats your business faces and the IT solutions you need to protect your vulnerabilities. The officer should oversee impact testing of the computer software to ensure that it is sufficiently robust. Your DPO should oversee and advise on all areas of data processing. Your DPO is your first port of call in the event of a data breach.

Quick Response

Early action in response to any suspected cyber-attack is critical; disconnect from the internet to avoid any further or more penetrative attacks. You should have the appropriate contingency procedures in place for cyberattacks/security breaches. Consider whether is it appropriate to immediately inform any customers and/or other data subjects you believe may have been affected to minimise the potential risk of harm.

Report

Report any suspected fraud or data hacks early to law enforcement, your regulator, your indemnity insurers, your DPO (if applicable) and consider whether self-referral to the ICO is necessary.

Learn and Adapt

In the event of an attack you should thoroughly investigate to pinpoint where your cyber security, the computer network or your anti-virus software has failed. Ensure that any weakness identified are immediately repaired and your existing software is replaced or upgraded to ensure that a cyber-attack of a similar nature does not happen again. Consider implementing a more targeted approach to training employees if the breach occurred with employee involvement.

Cyber-safe toolkit for small to medium sized businesses

SMEs can follow our 9 point guide to improving your cyber security across your business to help ensure you are prepared for tomorrow's threats.

1.

Identify the risk

- Assess your business' data processing and identify your most valuable data.
- Recognise how your business may be exposed, be it in the way your organisation is structured or in an unsecure network.
- Identify your network's vulnerabilities and potential points of entry for hackers.
- Identify possible vulnerabilities in your supply chain as a whole – might an attack on a supplier/customer cause disruption to you?

2.

Put policies in place

- User security: monitor and control how your employees use your computer network.
- Anti-malware: direct your employees to avoid downloaded untrusted or unsanctioned software.
- Passwords: Enforcing regular password changes is contrary to current NCSC guidelines. Passwords should be changed only if they are thought or known to be compromised. Regular changes result in "patterns", eg. moving from password1 to password2 and so on.
- Disciplinary: include in your disciplinary policy sanctions for computer misuse BUT encourage and reward quick reporting for those employees who fear they have "made a mistake".
- ID verification: put in place steps for when employees interact with customers.
- Consider cybersecurity when making acquisitions or working with third parties. Seek assurance through accreditation eg. CyberEssentials, ISO, CREST.

3.

Invest and insure

- Invest in cybersecurity software.
- Consider cybercrime insurance and compare different providers to find the product most suited to your individual business needs.
- Insurers may replace any damaged computer equipment, help with data restoration and cover any loss of earnings.
- Insurers may protect you from any claim for damages if confidential information is stolen.

4.

General Data Protection Regulation (GDPR)

- Be aware of the requirements of the GDPR.
- Ensure information is:
  - Processed lawfully and fairly.
  - Not stored for longer than. necessary.
  - Not transferred outside the European Economic Area without adequate protection.

5.

Educate Workforce

- Inform staff about current cybercrime trends.
- Ensure employees observe cyber policies.
- Help employees understand the risks of releasing confidential information with interactive/on-site training.
- Ensure all employee training is tailored to your business sector.
- Measure the effectiveness of your cybercrime training by testing employees' awareness.

6.

Security

- Establish malware defences, antivirus applications, firewalls and content filters.
- Adopt "vendor diversity" – use solutions from different providers at different levels to benefit from expanded threat research.
- Use a "layered" defence – for example install a perimeter firewall, put vulnerable internet connected servers/services eg. web servers/guest WiFi behind it in a "DMZ" and then have a second firewall below which your sensitive network exists.
- Encrypt sensitive data at rest AND in transit.
- Use a website reputation service to generate a blacklist of websites.
- Use a VPN (virtual private network) to ensure data cannot be intercepted.
- Create user privileges and only give certain employees administrative network access.
- Privileged Access Management (PAM): only allow trusted employees to become 'privileged users' i.e. users with administrative access to critical systems. Make privileged user status subject to period review.
- Consider installing PAM software to monitor all privileged accounts across your systems.
- Close user accounts BEFORE employees leave.
- Prohibit employees from using their personal computer devices at work FULL STOP!
- USB sticks are a particular nuisance, and people charging personal phones from networked USB ports.
- TWO FACTOR AUTHENTICATION. A huge amount of business related cyber crime could be wholly avoided by using this feature where available.

7.

Back-up data

- Back-up on a minimum of three devices:
  - A local machine.
  - A secure cloud service.
  - An offline external drive.
- Make backing up data a daily process for employees.
- If using the Cloud, ensure that the provider can delete copies of personal data within a timescale.
- Verify and test backups.

8.

Put in place a Security Incident Response Plan

- Disconnect from the local network and the internet.
- Train your staff to take immediate action - just like fire response.
- Scan your PCs and computer network.
- Investigate how the threat materialised.
- Document the date and time of the attack and who reported it.
- Interrogate the computer hardware and incoming files.
- Learn from incidents.
- Test your plan.

9.

Report it

- Report the cyber-attack or data breach to:
  - The Police and/or Action Fraud.
  - Your bank to cancel any suspicious payments.
  - Your Indemnity Insurer, who may be able to offer you advice and assistance.
  - The relevant regulatory bodies, who may be able to investigate the matter further, including the Information Commissioners Office (ICO).

How can we help you?

BMLaw services

Corporate crime

- Advising on internal and fraud and misconduct investigations.
- Private prosecutions.
- Coordinating accurate reporting to and liaising with law enforcement agencies.
- Advising on external investigation, interviews and defending possible enforcement.
- Dawn raids.

Civil

Asset recovery steps

- Freezing orders.
- Proprietary injunctions.
- Search orders.
- Third party disclosure orders.

Litigation

- Breach of contract.
- Breach of trust/fiduciary duty.
- Fraudulent misrepresentation.
- Dishonest assistance.
- Unjust enrichment.
- Knowing receipt .

Breach management & mitigation

- Dealing with complaints and claims by data subjects.
- Enforcing processing and other data protection agreements.

Data Protection

GDPR & DPA18 compliance

- EPrivacy & PECR compliance.
- Data flow & gap analysis.
- Security analysis (software based).
- Data Protection Impact Assessments.
- Data Protection notices, policies and procedures.
- Legitimate interest assessments.

Processing agreements

- Data sharing/transfer agreements.
- Cross border data transfer agreements.

Managing subject access requests

- Breach assessment and reporting.
- Liaison with ICO/ Supervisory authorities.
- Notifying data subjects of breaches.

Staff training

Deal with due diligence in corporate transactions

- Outsourcing agreements.

Non-legal services

BM Data Services

- EURep service.
- UKRep service.
- DPO Service.

Blaser Mills Law is a leading law firm based in the South East.

We are a full-service firm, offering a comprehensive range of legal services to businesses and private individuals.

Our modern and innovative approach means that we deliver practical and cost-effective solutions.

Offices in
High Wycombe
Amersham
Rickmansworth
Silverstone
London

020 3814 2020
blasermills.co.uk

BlaserMills
Law

High Wycombe | Amersham | Rickmansworth | Silverstone | London
020 3814 2020 | blasermills.co.uk

@BlaserMillsLaw blaser-mills BlaserMillsLaw