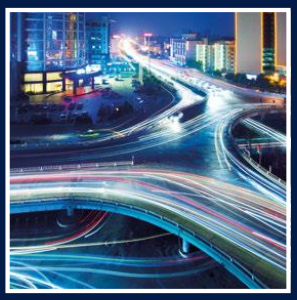
National Cyber Security Centre
a part of GCHQ

NCA
National Crime Agency

The cyber threat to UK business








2017-2018 Report

Foreword: Ciaran Martin (NCSC)

As the Chief Executive of the National Cyber Security Centre (NCSC), it is my mission to make sure the UK is less and less susceptible to cyber attacks. This ambitious goal is being achieved so far not least because of the combined efforts of the NCSC and the National Crime Agency (NCA).

The last year has seen no deceleration in the tempo and volume of cyber incidents, as attackers devise new ways to harm businesses and citizens around the globe. Despite these very real threats to the nation's security, I am confident in the UK's ability to combat the attacks that we face every day.

The NCSC's aim is to make the UK an unattractive target to cyber criminals and certain nation states by increasing their risk, and reducing their return on investment. We have adopted a proactive approach to dealing with the increasingly challenging cyber landscape and in tandem with the NCA are taking a proactive approach to combating cyber crime.

This report examines how cyber activities over the past 12 months have impacted businesses - from their reputation, through to their systems, to their bottom line. Much of the impact on businesses is caused by cyber crime, but all nefarious cyber activity can be as damaging, as we experienced in wide-scale campaigns like Wannacry and NotPetya, the costs of which ran into hundreds of thousands of pounds.

Together with our law enforcement colleagues from the NCA, the technical experts here at the NCSC have been instrumental in helping citizens and organisations of all sizes protect themselves with the aid of guidance and other bold initiatives like the Active Cyber Defence[1] programme.

I am delighted that as part of our assistance to businesses across the UK, we are able to publish this annual threat report in partnership with the NCA. My hope is that by sharing our experiences of exposure to cyber incidents, we raise awareness across the board and, as a result, improve the nation's cyber defences for good.

Ciaran Martin
Chief Executive Officer, NCSC

[1] www.ncsc.gov.uk/active-cyber-defence

Foreword: Donald Toon (NCA)

The Cyber Threat to UK Business Report 2016/17[2] outlined the growing cyber crime threat that our country faces. That trend has continued this year, highlighted by high-profile cyber attacks with far-reaching consequences and real harm caused to victims.

This year's report recognises the most significant incidents from last year, but it also presents case studies where action has led to successful mitigation. It's been produced with the input of many in government and industry, and I especially thank members of the NCA's Strategic Cyber Industry Group for their contribution.

Early reporting of cyber attacks remains essential to mitigating the impact of an attack. Action Fraud[3], the National Fraud and Cyber Crime reporting centre for the UK, has launched a 24/7 live cyber attack reporting service which works in tandem with the NCA and other parts of government to ensure that we are able to prioritise cases, protect victims and find those responsible.

In the 2016/17 report, I highlighted that successful law enforcement and industry collaboration does not just enhance the UK community's response to the cyber threat; it underpins it. This still holds true, now more than ever. As the rewards for perpetrating cyber crime become greater, the need for businesses to focus on cyber security has become acute.

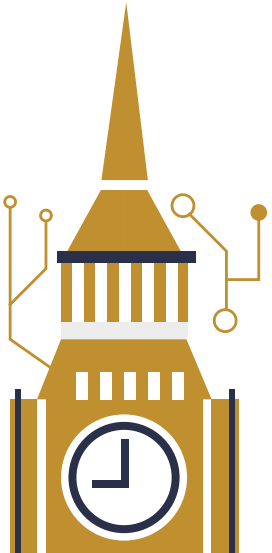
This year saw an increased number of law enforcement disruptions, with industry collaboration a key factor in their success. By working together at all levels, we can become even better at protecting ourselves against the cyber crime threat. We still have much work to do, but we can make the UK the safest place in the world to do business.

Donald Toon
Director – Prosperity, National Crime Agency

[2] www.ncsc.gov.uk/report/cyber-threat-uk-business

[3] www.actionfraud.police.uk/

Contents



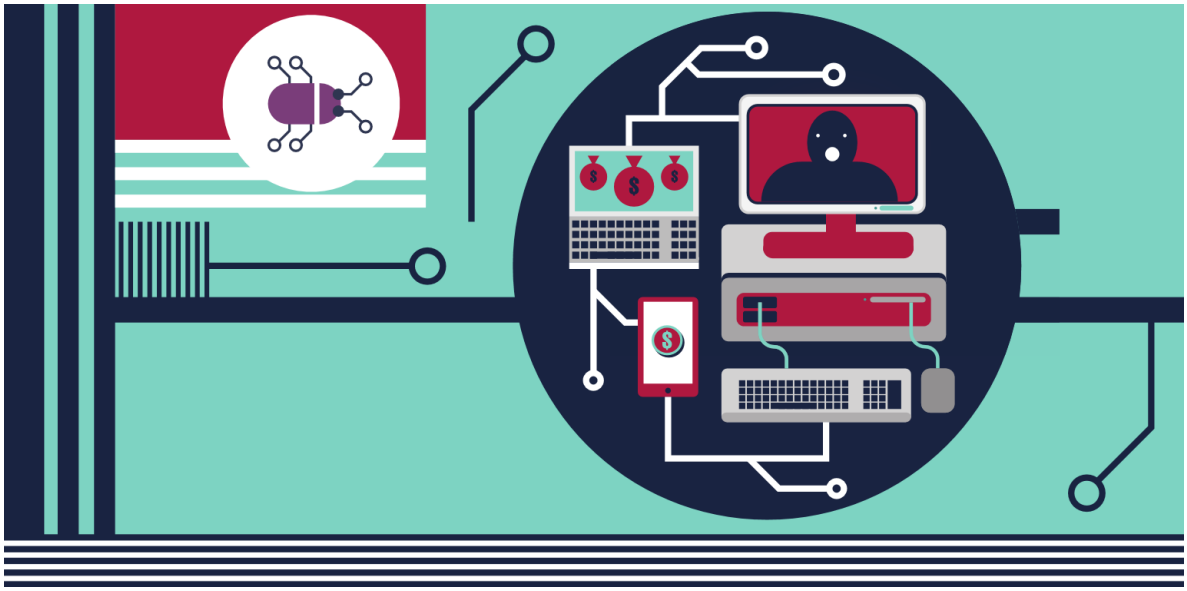
Executive summary

2017 will be remembered as the year of ransomware attacks and massive data breaches, supply chain threats and, of course, fake news stories. With attackers able to achieve many of their aims by using techniques that are not particularly advanced, the distinction between nation states and cyber criminals has blurred, making attribution all the more difficult.

The WannaCry ransomware attack in May spread rapidly and randomly due to its use of a self-replicating worm. 300,000 devices were infected, spanning 150 countries and affecting services worldwide, including the NHS. The attack demonstrated the real-world harm that can result from cyber attacks, particularly when they are designed to self-replicate and spread.

The enormous scale of the 2013 Yahoo breach[4], the 2016 Uber breach[5] and the 2017 Equifax breach[6] came to light this year, demonstrating that data is a valuable target for cyber adversaries.

Supply chain compromises of managed service providers and legitimate software (such as MeDoc and CCleaner) provided cyber adversaries with a potential stepping stone into the networks of thousands of clients, capitalising on the gateways provided by privileged accesses and client/supplier relationships. It is clear that even if an organisation has excellent cyber security, there can be no guarantee that the same standards are applied by contractors and third party suppliers in the supply chain. Attackers will target the most vulnerable part of a supply chain to reach their intended victim.



Cyber attacks have resulted in financial losses to businesses of all sizes.

Fake news amplified on malicious websites and via defamatory social media campaigns had an impact on UK businesses in 2017, showing the potential commercial impact of these practices.

Cyber attacks have resulted in financial losses to businesses of all sizes. The costs arise from the attack itself, the remediation and repairing reputational damage by regaining public trust. Attacks have also triggered declines in share prices and the sacking of senior and technical staff held to account for massive data breaches. The enforcement of the General Data Protection Regulation (GDPR) in May 2018 could, under certain circumstances, lead to severe fines for organisations which fail to prevent data breaches, which result in a risk to the rights and freedoms of individuals.

[4] www.bbc.co.uk/news/business-41493494

[5] www.bbc.co.uk/news/technology-42169813

[6] www.bbc.co.uk/news/technology-41286638

Between October 2016 and the end of 2017, the NCSC recorded 34 significant cyber attacks (that is, attacks that typically require a cross-government response), with WannaCry the most disruptive of these. 762 less serious incidents (typically confined to single organisations) were also recorded. 2018 will bring more of these attacks. The Internet of Things and its associated threats will continue to grow and the race between hackers' and defenders' capabilities will increase in pace and intensity.

With interest in cryptocurrency still strong, cryptojacking - where an individual's computer processing power is used to mine cryptocurrency without the user's consent - will likely become a regular source of revenue for website owners. Increased use of cloud technology to store sensitive information will continue to tempt cyber attackers, which could result in UK citizens' information being breached.

Many of these cyber threats can be prevented, or at least the impact reduced, by adopting basic cyber security measures as set out in the 10 Steps to Cyber Security[7], Cyber Essentials[8] or the NCSC's Small Business Guide[9]. Where relevant, references to other NCSC guidance is provided throughout this report.

The NCSC and NCA will continue their joint efforts to reduce the harm caused by cyber attacks against the UK and to make the country the safest place to live and do business online.

Trends in 2017-2018

The major incidents in 2017 included:

1. Ransomware and distributed denial of service attacks
2. Massive data breaches
3. Supply chain compromises
4. Fake news and information operations

[7] www.ncsc.gov.uk/guidance/10-steps-cyber-security

[8] www.cyberessentials.ncsc.gov.uk/

[9] www.ncsc.gov.uk/smallbusiness

1. Ransomware and distributed denial of service attacks

In addition to the WannaCry ransomware attack (the details of which can be read overleaf), ransom Distributed Denial of Service (DDoS) attacks - where hackers threaten to conduct DDoS attacks unless a ransom is paid - have increased since mid-2017 when a South Korean web hosting company paid a ransom fee in Bitcoin equivalent to US$ 1 million.

In late 2017, the hacking group Phantom Squad targeted organisations in Europe, Asia and the US. They threatened financial institutions, hosting providers, online gaming services and Software-as-a-Service (SaaS) organisations and demanded a 're-instatement of services' payment in Bitcoin. The anonymity provided by virtual currencies like Bitcoin allow cyber criminals to conduct bold attacks and potentially make a profit.

Screenshot from a device infected with the WannaCry ransomware.

The increase in availability of DDoS-for-hire services and the proliferation of unsecured Internet of Things (IoT) devices has led to an increase in DDoS attack attempts. According to a survey by Corero Network Security[10], the number of monthly DDoS attack attempts between July and September 2017 showed a 91% increase when compared to figures in the first quarter of 2017.

[10] www.infosecurity-magazine.com/news/ddos-attacks-nearly-double-since

Case Study: WannaCry ransomware

A global attack using ransomware known as 'WannaCry' was launched on 12 May 2017. WannaCry encrypted victim machines, rendering them unusable, and demanded a ransom of US$ 300 in Bitcoin to unlock each machine.

The ransomware was distributed by a self-replicating worm, which meant WannaCry's spread was rapid, random and untargeted. The worm relied upon two cyber tools that had been released publicly in April by the Shadow Brokers group. These tools exploited a vulnerability within Windows systems that Microsoft had patched in March 2017 (MS17-010[11]). Consequently, only unpatched systems were vulnerable to WannaCry. 300,000 computers in 150 countries were affected.

Prominent among the victims was the National Health Service (NHS); over a third of England's NHS trusts were disrupted, with over 6,900 NHS appointments cancelled and some patients needing to travel farther for accident and emergency care. Most of the NHS victims used systems for which patches were available but had not been applied, highlighting the importance of basic security practices.

Amongst the other unpatched systems were both older systems no longer supported by Microsoft and unofficial copies: a particularly high number of WannaCry infections in China were attributed, in part, to the prevalence of pirated software in the country.

The WannaCry attack was conducted for financial gain, but poor implementation prevented the attackers from profiting as they had intended. Successful ransomware campaigns rely upon their victims believing that their data will be decrypted if they pay the ransom. However, most WannaCry victims found that paying the ransom did not result in machines being decrypted. The NCA strongly recommends not paying the ransom as there is no guarantee that you will get the files back.

The ransomware's spread was halted when a security researcher registered WannaCry's 'kill switch domain'. When the ransomware successfully contacted this domain, it took no further action.

WannaCry attribution

In December 2017, the Foreign Office Minister for Cyber Security, Lord Ahmad said, "The UK's National Cyber Security Centre assesses it is highly likely that North Korean actors known as the Lazarus Group were behind the WannaCry ransomware campaign."

Our response to WannaCry

The NCSC and the NCA worked in collaboration with a number of organisations to understand and mitigate the Wannacry ransomware threat. The NCA's investigation is ongoing.

[11] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Mitigations against ransomware and distributed denial of service attacks

The NCSC recommend that you:

- deploy critical security patches as soon as possible
- deploy an always-on antivirus solution that scans new files
- conduct regular vulnerability scans and action critical results
- implement application whitelisting technologies to prevent malware running on hosts
- implement a policy of least privilege for all devices and services
- establish configuration control and management

For more information, please refer to the following guidance:

- www.ncsc.gov.uk/guidance/10-steps-secure-configuration
- www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware
- www.ncsc.gov.uk/guidance/denial-service-dos-guidance-collection
- www.ncsc.gov.uk/guidance/end-user-device-security

2. Data breaches

The reported number and scale of data breaches continued to increase in 2017, with Yahoo finally admitting in October that all of its 3 billion customers had been affected by the 2013 breach.

Groups assessed to have links to state actors - sometimes described as APTs (Advanced Persistent Threat) - were likely responsible for some of the larger breaches. The techniques used in most cases were not particularly advanced (including exploiting unpatched vulnerabilities and spear-phishing), further demonstrating the blurring boundaries between nation states and cyber criminals, making attribution more difficult.

Examples of data breaches included:

- Equifax, where the personally identifiable information of 145 million US users and almost 700,000 UK users was compromised.
- Verizon's data on 14 million customers stored in the cloud, and controlled by a third party company, was exposed to anyone who could guess the web address.
- Uber was forced to reveal that it deliberately covered up a year-old breach by paying the hackers US$ 100,000 to destroy the data they had stolen. The data of 57 million accounts, which had not been encrypted, was exposed.
- An aggregated database of data, collated from multiple breaches, was discovered by security company 4iQ in December 2017. This contained 1.4 billion credentials in clear text, including unencrypted and valid passwords.

Analysis indicated a large number of incidents were caused by third party suppliers failing to secure data properly. Some of the examples above also demonstrate that it takes more than basic cyber security posture to prevent large-scale data breaches.

Case study: Yahoo

In March 2017, a grand jury in the northern district of California indicted four defendants for hacking, espionage and other criminal offences in connection with a conspiracy to access Yahoo's network and the contents of webmail accounts. The defendants included two Russian intelligence officers. According to the details of the indictment, the defendants used unauthorised access to Yahoo's systems to take information from at least 500 million accounts at Yahoo, Google and other providers. This included the accounts of Russian journalists, officials of the US and Russian governments, and employees of private sector companies in the finance and transport sectors. Some financial information was also stolen, including gift card and credit card numbers.

It is believed that a spear-phishing email was the most likely route into Yahoo, and through which employee credentials were obtained. In October 2017, Yahoo admitted that all 3 billion accounts had been compromised in the 2013 breach.

Case study: Equifax

Credit scoring agency Equifax was the victim of a data breach between May and July 2017, resulting in personally identifiable information of up to 143 million Americans being accessed. Data on approximately 400,000 UK nationals residing in the US was also potentially affected by the breach. The data reportedly included names, social security numbers, dates of birth and other personal information. Access to the data was gained via a website vulnerability, for which a patch was available.

Equifax later confirmed that a file containing 15.2 million UK records dating between 2011 and 2016, was involved in the incident. As some of the information was duplicated, the records related to nearly 700,000 people.

Our response to Equifax breach

The NCSC worked with international partners, the NCA and law enforcement bodies to provide full understanding of the extent of the breach. The NCSC provided situational updates across government as information became available.

Case study: Uber

In November 2017, Uber Technologies Inc. announced a security breach that took place in October 2016. The breach is reported to have affected 50 million customer accounts globally and 7 million driver accounts. Initial reports indicated that compromised information included names, phone numbers, email addresses and driving license details of some of their drivers. Uber reported to the media that there had been no evidence of credit card details or social security numbers being breached.

Media reporting suggests that the breach took place after credentials uploaded to GitHub (a software repository), by an Uber software developer, were used to access cloud-based storage, Amazon Web Services (AWS). It is also claimed that a ransom of US$100,000 was paid by Uber in response to the breach as an exchange for deletion of the breached data and that a non-disclosure agreement was signed by the attackers following this payment.

Our response to Uber breach

The NCSC and NCA worked closely with other agencies and the Information Commissioner's Office during this incident and investigated how this breach affected people in the UK. The NCSC provided advice on appropriate mitigation measures for victims of the breach and worked to ensure Uber provided clear guidance to all affected. The NCSC provided situational updates across government as information became available.

Case study: Telecoms data theft

A UK-based telecoms company reported a cyber attack to Action Fraud, when they discovered that data about individuals due for phone upgrades had been stolen. This case was triaged as a priority by Action Fraud and passed to the NCA, who liaised with NCSC to ascertain the most appropriate response and analyse the large datasets involved.

Our response to telecoms data theft

It is assessed that this attack cost the victim company approximately £500,000. The prompt reporting of the crime enabled the NCA's investigation to seize evidence and trace those responsible, and alert and provide mitigation to other potential victims.

Mitigations against data breaches

The NCSC recommend that you:

Protect endpoints:

- use up-to-date and supported operating systems and software
- deploy critical security patches as soon as possible
- implement application whitelisting technologies to prevent malware running on hosts

Protect the network:

- use firewalls and network segregation to protect services
- deploy an always-on antivirus solution that scans new files
- perform regular vulnerability assessments against both internal and external services to scan for any insecure configuration

Protect the information:

- implement a policy of 'least privilege' for all devices and services
- use multi-factor authentication to protect sensitive information
- ensure that all services are protected by strict authentication and authorisation controls
- use password managers to help prevent password reuse between systems
- implement a practical monitoring and alerting service

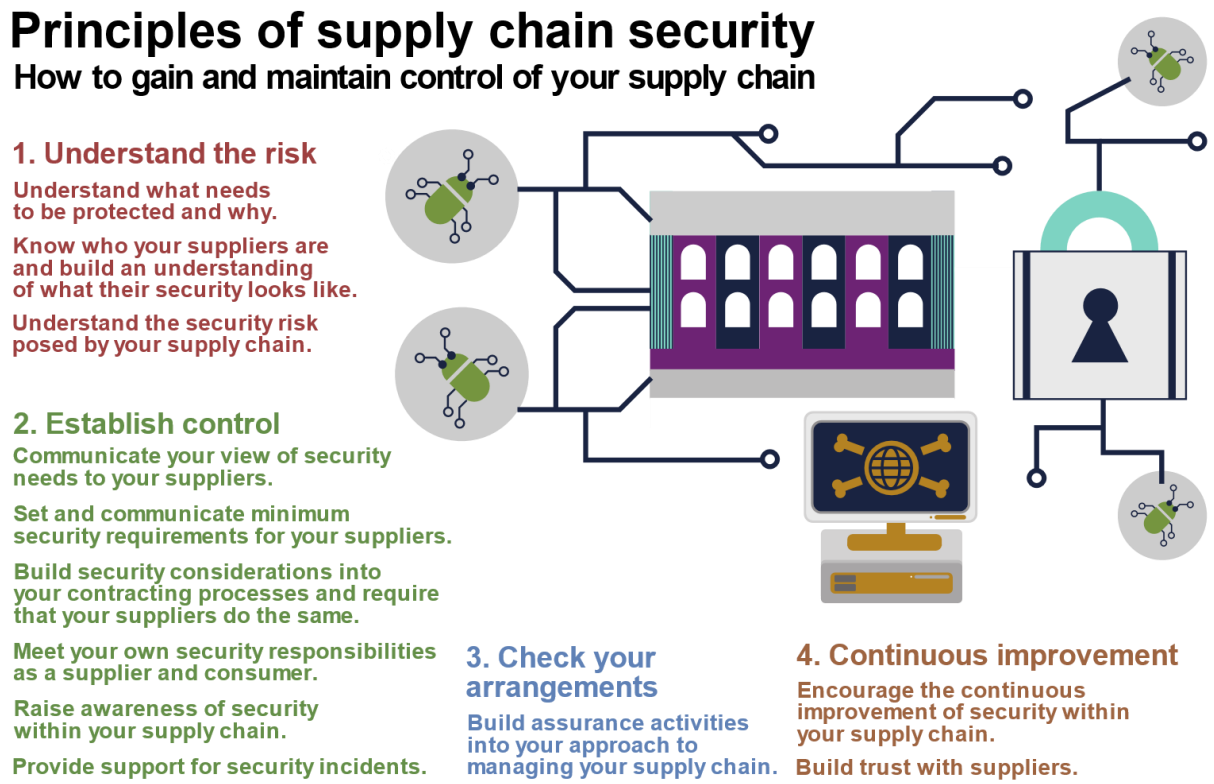
For more information, please refer to the following guidance:

- www.ncsc.gov.uk/smallbusiness
- www.ncsc.gov.uk/guidance/10-steps-network-security
- www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

3. Supply chain compromises

2017 saw some significant examples of supply chain attacks, including the compromise of a large number of managed service providers (MSPs), enabling access to commercially sensitive data from them and their clients. At least two software companies had their products (MeDoc and CCleaner) compromised at source, resulting in their customers being infected with malware when downloading the software/updates.

Supply chain compromises typically seek to introduce security flaws or other exploitable features into equipment, hardware, software, or services, prior to their supply to the target (or make use of a compromised supplier organisation's connections to the target). Operations or activities are usually designed to breach confidentiality and integrity, but they may also be designed to affect availability (such as supplying defective equipment). Ongoing servicing, support or updates to equipment, hardware or software may also provide opportunities for threat actors to interfere with the supply chain.



Find out how to secure your supply chain by reading the NCSC's supply-chain guidance[12]

When done well, supply chain compromises are extremely difficult (and sometimes impossible) to detect. Network monitoring can detect unusual or suspicious behaviour, but it is still difficult to ascertain whether a security flaw has been deliberately introduced (possibly as a backdoor) or results from a careless error on the part of developers or manufacturers – or indeed to prove that any potential access has been exploited. Services of almost any sort can be affected, particularly if they involve electronic connectivity or data import.

[12] www.ncsc.gov.uk/guidance/supply-chain-security

Case study: Compromise of MSP

A known cyber actor was found to have compromised several global managed service providers (MSPs) in 2017, although the compromise probably took place at least as early as May 2016. These MSPs deliver IT, HR and business services to clients who have outsourced various elements of their infrastructure.

The compromises are a high-profile example of a supply chain attack, in which a cyber attacker sought to compromise a third party to use it as a stepping stone to the intended end target. MSPs represent a particularly attractive target as they have links to thousands of customers worldwide, through private network connections and other relationships. Even if a client has a strong outward-facing security posture, it may find itself vulnerable if a trusted network link to an MSP is compromised.

The actor is believed to have intended to obtain commercially sensitive data from the MSPs and their clients. Information held by MSP clients potentially covers a vast range of areas of interest to malicious attackers, including foreign intelligence services. It is highly likely they will continue targeting MSPs for cyber espionage reasons, due to the potential access to companies and governments worldwide.

MSP compromises attribution

Industry partners assess these compromises are highly likely to have been carried out by a China-based threat actor.

"[The actor who compromised the MSPs]….is highly likely to be a China-based threat actor."

PwC UK & BAE Systems, Operation Cloud Hopper report[13], April 2017

Our response to MSP compromises

The NCSC worked closely with industry partners in the Cyber Incident Response Scheme (CIR) to understand the targeted attacks against MSPs. Guidance was provided on the NCSC website and a technical assessment was published on our Cyber Security Information Sharing Partnership (CISP) platform.

[13] https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html

Case study: compromise of legitimate software (NotPetya)

On 27 June 2017, the day before a Ukrainian public holiday - Constitution Day - companies and organisations in Ukraine, Russia and beyond were infected by malware variously known as Petya, PetrWrap, ExPetr, GoldenEye and NotPetya. The malware encrypted the hard disks of infected computers, causing widespread disruption.

International companies doing business with Ukraine which were also infected reportedly included Cadbury's, FedEx, Merck and Moller-Maersk. A small number of UK companies were affected. Moller-Maersk later reported an expected loss of revenue of more than €350 million from the attack.

Investigations conducted by the cyber crime unit of the Ukrainian police revealed the attackers had managed to interfere with a legitimate software package, MeDoc, an application widely used by businesses in Ukraine for handling tax returns. A MeDoc update, which had been maliciously modified at source, infected users of the application. The malware was then able to spread itself within networks.

While the attack vector was ostensibly ransomware demanding a US$300 payment, similar to the Wannacry incident the previous month, it is highly likely that the aim of the attack was disruption rather than financial gain.

NotPetya attribution

In February 2018, the UK, US, and Australian governments publicly attributed the NotPetya cyber attack to the Russian military. Other partners, including Canada and New Zealand, made supportive statements condemning malicious behaviour in cyberspace.

"The UK government judges that the Russian government, specifically the Russian military, was responsible for the destructive NotPetya cyber attack of June 2017."

Lord Ahmad, 15 February 2018

Our response to NotPetya

The NCSC worked closely with partners to identify UK victims as well as distribute the most up-to-date advice during the incident. The NCA criminal investigation is ongoing.

Case study: compromise of legitimate software (CCleaner)

Between 15 August and 12 September 2017, signed downloads of a specific version of CCleaner and CCleaner Cloud (widely used, free computer clean-up tools) were infected with multi-stage malware, possibly affecting well over 2 million downloads by both individuals and businesses.

Companies which received a secondary payload from the attackers (suggesting that they were the main targets of interest for the attackers) included large technology and telecommunications companies based in the UK, Taiwan, Japan, Germany and the US.

The software download was signed with a valid certificate issue to Piriform, the CCleaner developer. This suggests that some part of the CCleaner development or build process was compromised and, as with MeDoc, a legitimate software update from a trusted source was then used to infect customers.

The infection was identified by security researchers who quickly notified CCleaner's owner, Avast. Avast and Piriform issued a security alert and worked with US law enforcement to shut down the command and control server being used by the attackers.

CCleaner attack attribution

The incident has been widely attributed in public by companies and security researchers. According to security researchers, the code used in the malicious version of CCleaner was similar to that previously used by a Chinese cyber espionage group.

Security researchers, 3 October 2017

Our response to CCleaner

NCSC worked to alert potential victims of the CCleaner compromise and the possible targeting of their organisations

Mitigations against supply chain operations

The NCSC recommend that you:

- work (where possible) with companies certified through the NCSC Cyber Essentials Scheme[14], or those that can demonstrate that they've followed the NCSC's 10 Steps to Cyber Security[15]
- follow the principle of 'least privilege', especially for external parties that may need remote access into your networks for specific administrative tasks

For information, please refer to the following guidance:

- www.ncsc.gov.uk/guidance/supply-chain-security
- www.ncsc.gov.uk/guidance/managing-risk-cloud-enabled-products

[14] www.cyberessentials.ncsc.gov.uk/

[15] www.ncsc.gov.uk/guidance/10-steps-cyber-security

4. Fake news and information operations

The UK benefits from a free, open and accessible media, but social media presents opportunities for those looking to cause reputational damage to a business. For example, disgruntled employees, competitors or 'pranksters' can easily create fake news stories which can cause embarrassment or damage.

Whilst most of the press coverage over the past 18 months has focussed on the effect of fake news stories on the electoral process in several countries, businesses are not immune. While fake news is not strictly speaking a cyber threat, our adversaries regard it as one of the many tools available to them as part of a hybrid campaign.

The unregulated nature of social media presents opportunities for those looking to cause reputational damage to a business. The spreading of fake news cannot only damage a company's reputation but can affect the share price or sales. In extreme cases, smaller businesses could be forced to close.

Case study: fake news

Websites have been set up which allow people to create fake news, ostensibly to fool friends, but they can also be used maliciously. A Trend Micro report[16] highlighted the tools and services that are available in various online communities worldwide, which manipulate and spread fake news across relevant social media networks.

In May 2017, at least six Indian restaurants in the UK were targeted by fake news stories. One restaurant had to cut staff hours (and saw its revenue fall by half) after the fake story was picked up and spread on social networking sites.

In another case, a UK businessman was the target of a defamation campaign where false and doctored stories were shared on social media. His lawyers served an injunction against "persons unknown", in a case believed to set a legal precedent. The injunction was emailed to the perpetrator who confirmed via a delivery receipt that they were aware of the injunction and the campaign ceased.

Our response to fake news

The NCSC has helped to combat cyber attacks on the UK electoral system by providing advice and guidance to local government and political parties, but does not have a role in policing content on the Internet. In January, the UK government announced plans to set up a National Security Communications Unit, under the Cabinet Office, to counter disinformation by state actors and others.

The NCSC will continue to provide technical expertise and collaborate with cross-government and wider initiatives.

[16] www.trendmicro.com/vinfo/ie/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media

Other significant incidents

The other significant incidents described in this section have been included to provide a wider view of the threat landscape from the past year. Once again, the examples we've included demonstrate that small businesses are just as much at risk as larger ones.

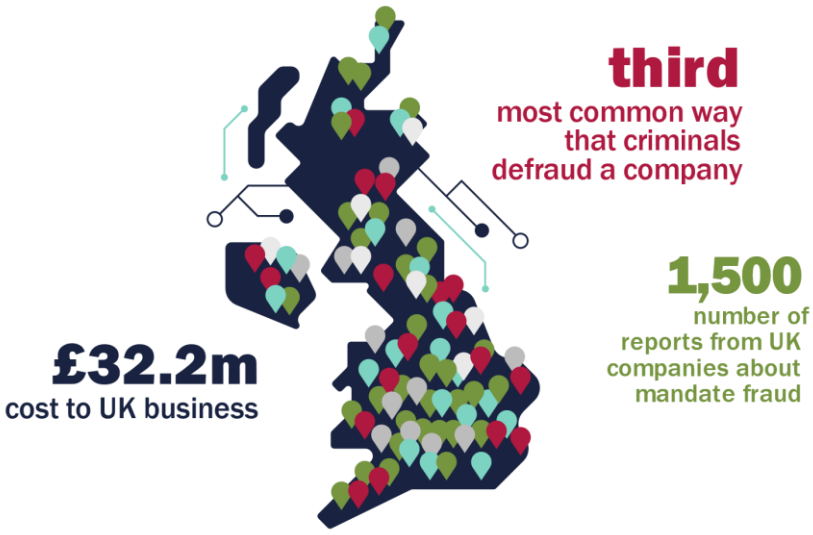
1. CEO/business email compromise fraud
2. Major security vulnerabilities
3. Financial sector compromise
4. Targeting of parliament
5. Cyber crime as a service

1. CEO/business email compromise fraud

Business email compromise (BEC) is a form of phishing attack where a cyber criminal impersonates a senior executive and attempts to coerce an employee, customer, or vendor to transfer funds or sensitive information to the phisher.

BEC scams are a serious threat to organisations of all sizes and across all sectors, including non-profit organisations and government. It represents one of the fastest growing, lowest cost, highest return cyber crime operations.

According to a mid-2017 report by Cisco[17], cyber criminals made US$ 5.3 billion from BEC fraud during the last 3 years, compared to US$ 1 billion from ransomware. Industry experts project that global losses from BEC scams will exceed US$ 9 billion in 2018.



The cost of BEC in the UK in 2016-2017 (source: Action Fraud)

In 2017, Dublin Zoo was hit by a BEC scam, with cyber criminals reportedly obtaining nearly US$ 600,000. They allegedly intercepted legitimate supplier invoices sent to the zoo and manipulated data on the documents to change payment details and account numbers, requesting that funds be sent into a fraudulent account.

Other examples highlight a string of BEC attacks on the art industry, when art galleries and dealers have been targeted by invoice scams after cyber attackers infiltrated their emails.

[17] https://cybersecurityawareness.co.uk/2017/07/24/ceo-fraud-attacks-lucrative-ransomware/

On a similar theme, mandate fraud is when someone convinces an organisation to change a direct debit, standing order or bank transfer mandate, by purporting to be a company that receives regular payments from them, for example a subscription or membership organisation or a business supplier.

According to Action Fraud data, there were over 1,500 reports from UK companies about mandate fraud in 2016-2017, which cost businesses approximately £32.2 million. Mandate fraud is the third most common method criminals use to defraud a company.

The growth of BEC is unlikely to result from significant technological developments; rather criminals are continually honing techniques to exploit victims. They use increasingly sophisticated techniques that often include a combination of social engineering, email phishing, email spoofing and malware. There has been a noticeable change in trends, moving from exploit kits to social engineering emails with malicious attachments. This is largely due to systems being upgraded and patched, so exploit kits no longer work as well as they used to.

In addition, the adoption of fluent business terminology, industry knowledge and personal references from social and professional networking sites have made the deception associated with BEC attacks difficult to uncover until it is too late.

BEC has been used to obtain sensitive commercial data and intellectual property which could be sold on black markets online. This represents an evolution in intent whilst also allowing criminals to target more victims in an organisation, rather than just the budget holders. This trend will continue and may represent a particular risk to intellectual property.

Mitigations against business email compromise

Action Fraud and the National Fraud Intelligence Bureau (FNIB) operate a 24/7 hotline on 0300 123 2040 for businesses to report live cyber attacks. If you think you've been a victim of cyber crime, we recommend you keep a timeline of events and save any information that is relevant to the attack.

For more information, please refer to the following guidance:

- www.ncsc.gov.uk/guidance/avoiding-phishing-attacks
- www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing

2. Major security vulnerabilities

January 2018 saw the disclosure of two major security vulnerabilities, Meltdown and Spectre. The vulnerabilities make it possible for an attacker to steal almost all data that has been processed by a machine, including passwords and sensitive documents. Meltdown affects the majority of Central Processing Units (CPUs) made by Intel in the last two decades, whilst Spectre affects CPUs made by almost every manufacturer.

Patches have now been released by hardware and software vendors to mitigate this. However, the patch causes CPU performance to slow down. The exact figures are not known, but estimates range from a 5% slowdown to a 30% slowdown. This will not greatly affect individual consumers, but it will be noticeable for servers. Companies will need to take this deterioration in performance into account when applying the patches.

NCSC proactively advised all organisations and home users by publishing guidance on the NCSC website.

Mitigations against Meltdown and Spectre

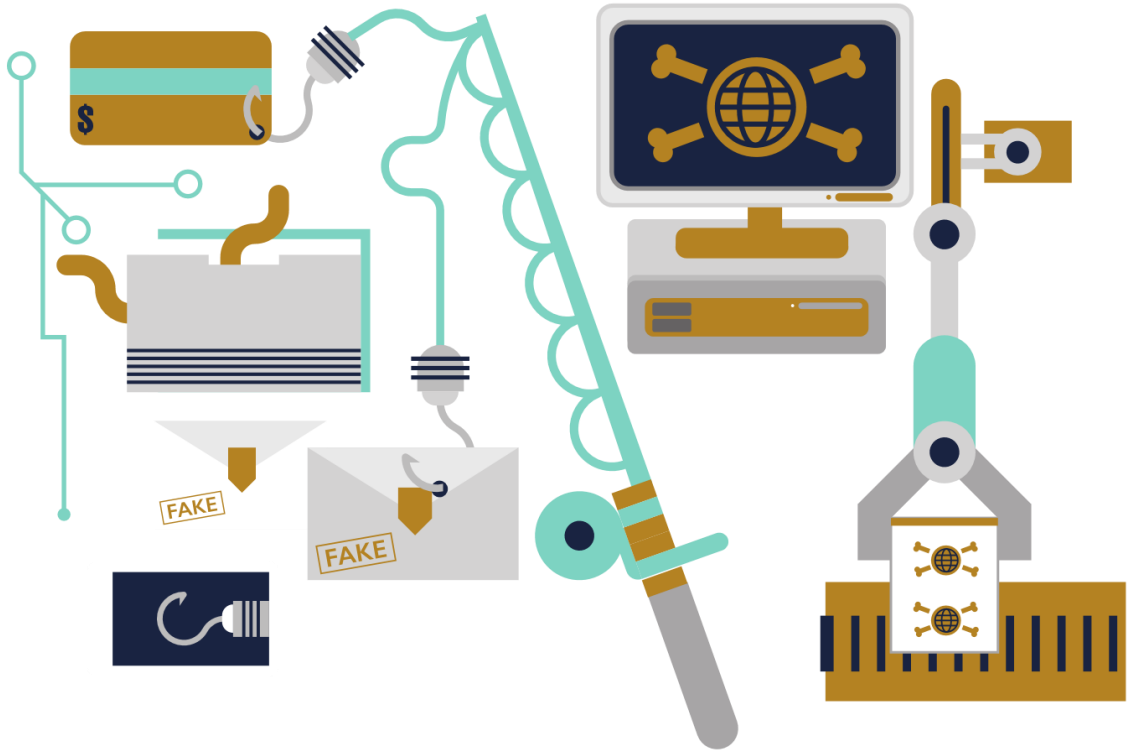
The NCSC recommend that you:

- use up-to-date and supported operating systems, hardware and software
- deploy critical security patches as soon as possible
- check the manufacturer of the hardware to see if they have published security updates, as not all security patches will be distributed by the operating system vendor

3. Financial sector compromise

On 5 October 2017, Far Eastern International Bank (FEIB) reported a cyber-enabled fraud that had been committed using the SWIFT system. Malware, believed to have been delivered by a spear-phishing email, infected the company's IT systems used for the SWIFT payment network. Attackers reportedly obtained valid credentials that allowed them to initiate a number of SWIFT messages totalling US$ 60 million. However, a large proportion of these messages were misconfigured, meaning only a small number of transaction requests were actually successful.

Total losses were estimated at less than US$ 500,000. Attackers successfully transferred funds from FEIB accounts to accounts in Sri Lanka, Cambodia and the US. Two individuals have since been arrested in Sri Lanka, while attempting to withdraw stolen funds.



Cyber criminals use phishing emails to deliver malware and steal credentials

This incident (and numerous similar ones) happened due to weaknesses in local security of the targeted banks, which allow the attackers to compromise the local network, probably obtain valid credentials and initiate fraudulent SWIFT messages. This also continues the trend witnessed over the last few years; instead of hacking the bank's customers (banking Trojans), more elite groups are putting the time and investment in to profiling and targeting the bank for a single large payout.

SWIFT is critical to conducting significant financial transfers and to the UK's finance sector and economy. Despite multiple attempts to exploit SWIFT, there is currently no credible evidence to suggest that the fundamental integrity of this international payment system has been compromised by a hostile state or criminal actor. However, sophisticated state and criminal organisations pose a significant and persistent threat to payment systems. A small subset of hostile state attackers almost certainly has the intent and capability to steal SWIFT credentials for financial gain, as demonstrated last year.

Our response to financial sector compromise

The NCA received intelligence that funds, fraudulently obtained as a result of administering Dyreza malware against UK and US victims, were being laundered through the UK. Over a three-year period, this UK-based group set up and controlled 400 bank accounts in a conspiracy which involved receiving stolen funds into one account, then dispensing it in smaller amounts to a number of other accounts. The process would be repeated several times to disguise the source of the money before it was transferred back to cyber criminals in eastern Europe. A bank manager was instrumental in the opening of a large number of these 'mule' accounts, using false ID and address documents.

The UK-based group were under surveillance by the NCA and were seen meeting with the bank manager in public places. On the day of the arrests, NCA officers recovered multiple mobile phones, financial ledgers, and 70 'mule packs' from the flat of one of the perpetrators. These packs contained ID and banking documents, bank cards and security information that enabled the group to access the accounts.

With the support of the banking industry and law enforcement partners in the UK, USA, Romania and Moldova, the NCA successfully shut down the networks, causing major disruption to these organised cyber criminals who no longer have access to their stolen profits.

In November 2017, the group were jailed for a total of 28 years for their roles in laundering at least £6.9 million stolen by international cyber criminals.

Mitigations against financial sector compromise

The NCSC recommend that you:

- use up-to-date and supported operating systems and software
- deploy critical security patches as soon as possible
- deploy an always-on antivirus solution that scans new files
- conduct regular vulnerability scans and action critical results
- implement application whitelisting technologies to prevent malware running on hosts
- implement a policy of least privilege for all devices and services
- establish configuration control and management

4. Targeting of parliament

In June 2017, sustained and determined attempts to gain unauthorised access to UK parliament email accounts was reported. Temporary access was gained to less than one per cent of the 9,000 accounts on the parliamentary network. The incident began on a Friday afternoon when most people had finished work for the week. A number of cyber attacks have begun at weekends or on the eve of public holidays (such as the NotPetya attack mentioned earlier). This is likely intended to delay or avoid detection of the activity.

These unauthorised access attempts sought to identify and break weak passwords. Many of the compromised accounts reportedly used passwords that did not conform to guidance issued by the Parliamentary Digital Service. Another vulnerability of the parliamentary system was that there were also no limits on the number of attempts allowed to log into the system.

Our response

The NCSC worked quickly with the Parliamentary Digital Security team to understand what had happened and to advise on mitigation. The NCA's criminal investigation is ongoing.

Mitigations against phishing attacks

The NCSC recommend that you implement a practical monitoring and alerting service which can provide actionable information to the necessary people.

For more information, please refer to the following guidance:

- www.ncsc.gov.uk/guidance/avoiding-phishing-attacks
- www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing

5. Cyber crime as a service

Goncalo Esteves ran the Counter Antivirus (CAV) service known as reFUD.me. The service allowed offenders to test, for a fee, whether their malicious cyber tools could beat antivirus scanners. Under the pseudonym KillaMuvz, he also sold custom-made, malware-disguising products and offered technical support to users. Esteves called these products Cryptex Reborn and Cryptex Lite. Part of a family of cyber tools known as crypters, they could be used by hackers to improve their chances of evading antivirus. He sold them for use in packages that varied in price according to the length of the licence.

A month of Cryptex Lite cost US$ 7.99 (about £5) while a lifetime licence for Cryptex Reborn cost US$ 90 (about £60). Esteves provided customer support via a dedicated Skype account and accepted payment either in conventional currency, Bitcoin or in Amazon vouchers.

Our response

The NCA worked collaboratively with Trend Micro to form a virtual team designed to find new and innovative ways to tackle cyber crime threats. This team assisted in the investigation into Esteves which resulted in his arrest and the takedown of both reFUD.me and both versions of Cryptex. Esteves was sentenced to two years in prison in January 2018 after pleading guilty on two charges under the Computer Misuse Act 1990, and one charge against the Proceeds of Crime Act 2002.

Future threats

1. Data breaches and legislation
2. Cryptojacking
3. Supply chain compromises
4. Increased use of worms
5. Internet of Things
6. Cloud security

Criminals are highly likely to continue to exploit long-standing and well-known vulnerabilities in victim infrastructure. We expect to see a continuation of cryptojacking and supply chain attacks, and an increasingly diverse range of ransomware variants.

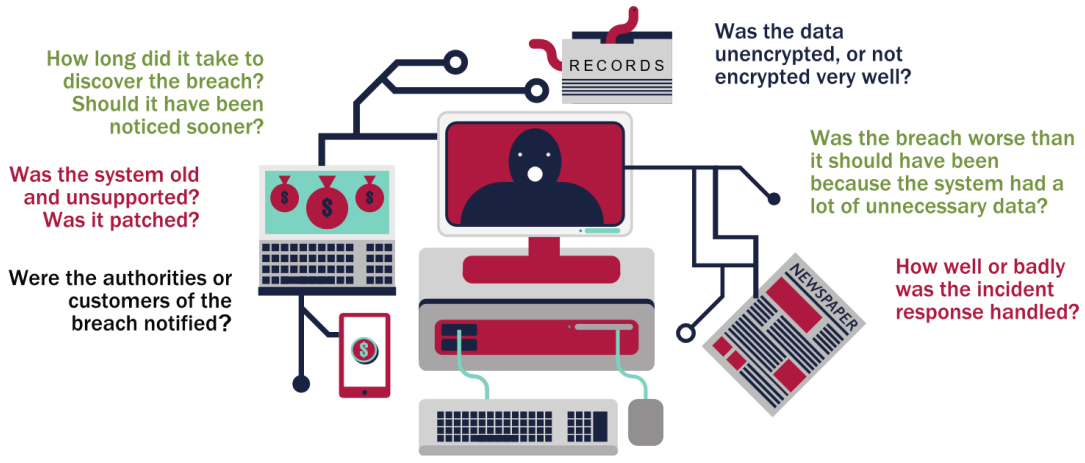
Data breaches and legislation

When it comes to data breaches, size matters - and makes media headlines. But it is not the only important factor. As coverage of the many large breaches reported in 2017 shows, commentators are quick to pick up on anything which may indicate poor security management, and this will only increase in the coming year with the implementation of new regulations.

Under the General Data Protection Regulation (GDPR), which will come into force from May 2018, organisations will have a duty to report to the relevant supervisory authority data breaches which are likely to result in a risk to the rights and freedoms of individuals. In cases where the risk to affected individuals is high, individuals will also have to be notified. A notifiable breach must be reported to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of the organisation becoming aware of the breach. Notification may take place in phases where investigations are still ongoing. NCSC expect to see an increase in the number of reported cyber incidents as a result.

Under GDPR, data controllers will have a responsibility for ensuring processors carrying out work on their behalf also comply with GDPR principles. Relevant guidance is available from the Information Commissioners website[18].

Organisations need to have completed risk assessments and put appropriate security measures in place. They also need to detect incidents quickly and to have planned and practised how to respond in the event of an incident occurring. Business continuity plans must be tested, and a media relations person should be ready to react to any fallout of a cyber incident.



[18] www.ico.org.uk

Likely media challenges after disclosure of a data breach

The directive on security of Networks and Information Systems (NIS Directive) is the first piece of EU-wide legislation on cyber security and provides legal measures to improve the overall cyber security of the EU. It came into force in August 2016 and EU member states have until May 2018 to incorporate the Directive into their national legislature. The directive contains a range of requirements around incident response, technical security measures and a risk-based security culture, which apply to operators of essential services (such as CNI) and digital service providers. There is information on the NIS Directive on the NCSC website[19].

Cryptojacking

The technique of delivering cryptocurrency miners through malware has been used for several years, but it is likely in 2018-19 that one of the main threats will be a newer technique of mining cryptocurrency which exploits visitors to a website. Throughout 2017, there has been an increase in cryptojacking (that is, using an individual's computer processing power to mine cryptocurrency without their consent). In December 2017, Check Point reported[20] that 55% of businesses globally were impacted by cryptominers.

Popular websites are likely to continue to be targets for compromise, serving cryptomining malware to visitors, and software is available that, when run in a webpage, uses the visiting computer's spare computer processing power to mine the digital currency Monero. In February 2018, over 4,000 websites worldwide (including approximately 600 in the UK) secretly mined cryptocurrency through a compromised screen-reading plugin for blind and partially sighted people. The only way users may notice their devices are being cryptojacked is a slight slowdown in performance. Using an ad blocker or antivirus programme (which have features that block browser mining) is the best way to prevent this.

We assume the majority of cryptojacking is carried out by cyber criminals, but website owners have also targeted visitors to their website and used the processing power of visitors' CPUs, without their knowledge or consent, to mine cryptocurrency for their own financial gain. In February 2018, a US online publication conducted a trial where its readers were advised that if they chose to block its advertising, the publication would use the reader's CPU to mine Monero. It claimed this was to recoup lost advertising revenue when readers use ad blockers.

Supply chain compromises

Criminals target commercial software, compromising end users and harming the reputation of the software providers. It is likely to continue, as it is extremely difficult to mitigate these threats, as users download software or updates issued by the legitimate supplier and have no way of knowing that software has been compromised. NCSC guidance on supply chain[21] has been published.

Increased use of worms

Having seen the success of using worms to propagate ransomware in the WannaCry attack, it's possible that hackers may be encouraged to use this automated and faster method of spreading malware through a network and beyond. Prior to WannaCry, the last significant worm was Conficker in 2008, which infected over 9 million systems and is still being detected in 2018, affecting systems which have still not been patched.

[19] www.ncsc.gov.uk/guidance/nis-guidance-collection

[20] https://globenewswire.com/news-release/2018/01/15/1289323/0/en/December-s-Most-Wanted-Malware-Crypto-Miners-Affect-55-of-Businesses-Worldwide.html

[21] www.ncsc.gov.uk/guidance/supply-chain-security

Internet of Things

With the number of devices connected to the Internet continually increasing, it is highly likely that we will see more attackers using the Internet of Things (IoT) to commit crimes. The research company Gartner predicts there will be 11.2 billion things connected worldwide by 2018. Many internet-connected devices sold to consumers lack basic cyber security provisions. With so many devices unsecured, vulnerabilities will continue to be exploited and used for activities (such as DDoS attacks) without the user's knowledge.

Current attacker business models are still in their infancy and mostly focused on DDoS. Many of the machines that have been compromised to date are not well suited for cryptomining (due to low processing power), or man-in-the-middle attacks (due to the need to break SSL).

The NCSC contributed to a report[22], published in March 2018, setting out how government will work with industry to address the challenge of insecure consumer IoT. The report advocates a fundamental shift in approach, moving the burden away from end-users having to secure their devices, and instead ensuring strong cyber security is built into IoT products by design. Central to the report is a code of practice for industry, which sets out thirteen practical steps for securing IoT products and associated services. The first three steps are:

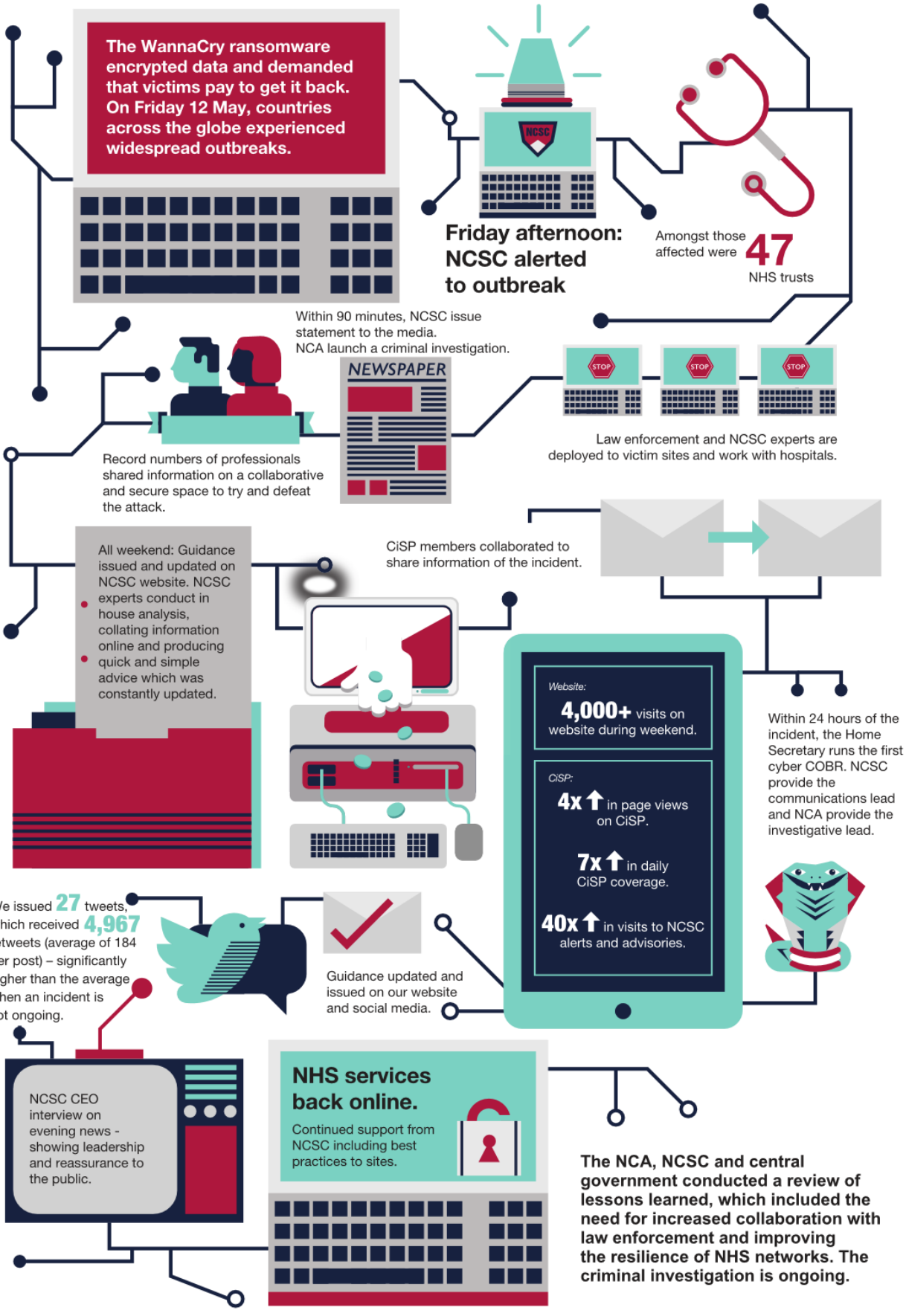
- avoiding default passwords
- implementing a vulnerability disclosure policy
- ensuring device software can be patched

Cloud security

Only 40% of all data stored in the cloud is access secured, although the majority of companies report they are concerned about encryption and security of data in the cloud. As more organisations decide to move data to the cloud (including confidential or sensitive information) it will become a tempting target for a range of cyber criminals. They will take advantage of the fact that many businesses put too much faith in the cloud providers and don't stipulate how and where their data is stored. This could lead to high profile breaches involving UK citizen information.

[22] www.gov.uk/government/publications/secure-by-design

Summary of response to WannaCry



National Cyber Security Centre
a part of GCHQ

NCA
National Crime Agency

The cyber threat to UK business

2017-2018 Report