National Cyber Security Centre
a part of GCHQ

NCA
National Crime Agency

The cyber threat to UK business

2016/2017 Report

Contents

Foreword (Ciaran Martin - NCSC) 2

Foreword (Donald Toon - NCA) 3

Executive summary 4

What is the threat? 5

The year in review: pivotal incidents of 2016 10

Horizon scanning: future threats 13

Fighting back: what can business do? 15

Case studies illustrating UK LEA and industry joint protect work 19

Debate: can we stop the Internet from being used for crime? 20

Foreword (Ciaran Martin - NCSC)

The new National Cyber Security Centre (NCSC) is at the heart of the Government's strategy for making the UK the safest place to live and do business online. We are working to reduce the harm caused by cyber attacks against the UK by spearheading an ambitious programme of initiatives that will make the UK the hardest target for potential adversaries. This work is underpinned by world-class research, staffed by some of the best people in technology anywhere in the world.

No single organisation can defend against the threat on its own and it is vital that we work together to understand the challenges we face. We can only properly protect UK cyberspace by working with others - with the rest of government, with law enforcement, the Armed Forces, our international allies and, crucially, with business and wider society.

In introducing this report, the first joint NCSC and National Crime Agency (NCA) Annual Threat Assessment, I want to acknowledge the outstanding contribution that law enforcement in general, and the NCA in particular, plays in detecting and deterring cyber attacks against the UK.

Cyber attacks will continue to evolve, which is why the public and private sectors must continue to work at pace to deliver real-world outcomes and ground-breaking innovation to reduce the threat to critical services and to deter would-be attackers.

> "Our agenda is unashamedly ambitious; we want to be a world leader in cyber security."
>
> **Ciaran Martin**
> **CEO NCSC**

As the national technical authority for cyber security in the UK, the NCSC shares knowledge, addresses systemic vulnerabilities and provides leadership on key national cyber security issues. Our agenda is unashamedly ambitious; we want to be a world leader in cyber security. We hope this report, alongside the other guidance and evidence we are making freely and openly available, will play its part in motivating our many essential partners to work with us to achieve our shared goals.

Ciaran Martin

Chief Executive Officer, NCSC

Foreword (Donald Toon - NCA)

The 2016 NCA cyber crime assessment outlined the real and immediate threat of cyber crime to the UK. In it we argued that collaboration between industry, law enforcement and government is the only way that the UK community will successfully outpace the cyber criminals and reduce the risk posed by cyber crime to the UK economy.

In this new report, written in collaboration with the NCSC, we build on that foundation and provide a more in-depth analysis of the evolving threat, together with an overview of the practical steps we can take together. I would especially like to acknowledge the contribution made by private sector members of the NCA's Strategic Cyber Industry Group, whose input to this assessment has been invaluable.

In law enforcement, we have long recognised the value industry can add to our investigative response, but to fight cyber crime in the 21st century, we need to work in active partnership from board level right through to the technical practitioners on the frontline.

"Successful law enforcement and industry collaboration doesn't just enhance the UK community's response to the cyber threat; it underpins it."

Donald Toon

DIRECTOR – PROSPERITY
NATIONAL CRIME AGENCY

To dynamically pursue the criminals, we need industry to report cyber attacks as soon as they know about them. To fully understand the threat landscape, we need access to industry's threat intelligence. And to take down organised crime groups, we need to work collaboratively with industry partners on attribution and infrastructure mapping.

Successful law enforcement and industry collaboration doesn't just enhance the UK community's response to the cyber threat; it underpins it. Together we can make UK cyberspace the safest place to do business globally.

Donald Toon

Director - Prosperity, National Crime Agency

Executive summary

- The cyber threat to UK business is significant and growing. In the three months since the NCSC was created, the UK has been hit by 188 high-level attacks which were serious enough to warrant NCSC involvement, and countless lower level ones.
- This threat is varied and adaptable. It ranges from high volume, opportunistic attacks where technical expertise is bought, not learned, to highly sophisticated and persistent threats involving bespoke malware designed to compromise specific targets. The lines between those committing attacks continue to blur, with criminal groups imitating states in order to attack financial institutions and more advanced actors successfully using 'off the shelf' malware to launch attacks.
- The rise of internet connected devices gives attackers more opportunity. Consumer goods and industrial systems combined with the ever increasing commercial footprint online provides threat actors with more attack vectors than ever before.
- The past year has been punctuated by cyber attacks on a scale and boldness not seen before. This included the largest recorded cyber heist, the largest DDoS attack and the biggest data breach ever being revealed. The attacks on the Bangladesh Bank, Democratic National Party and Ukrainian energy infrastructure also demonstrated the boldness with which threat actors can operate.
- The UK government is committed to making the UK a secure and resilient digital nation. A key aspect of this strategy is through robust engagement and an active partnership between government, industry and law enforcement to significantly enhance the levels of cyber security across UK networks.

What is the threat?

Current trends

The current cyber threat trends are underpinned by three key features:

- technical expertise is not necessary to carry out attacks
- a broadening attack surface leads to more opportunities for attackers
- threat actors are learning from, and using one another's skills and capabilities

The technical skill required to commit cyber attacks continues to decrease. Malware and services such as DDoS (distributed denial of service) are easily acquired on the dark web which means the number of individuals capable of launching basic cyber attacks is increasing.

As the number of internet connected devices grows, the attack surface and number of devices that can be leveraged to launch attacks expands. The Mirai botnet is the most notorious example of this, but the phenomenon also impacts mobile devices and wearables as well as Industrial Control Systems (ICS) and other automated systems.

Finally, the lines between different threat actors continues to blur as individuals and groups learn from, hire and work with one another. Criminal groups are imitating suspected nation state methodology in order to attack financial institutions, and more advanced actors are successfully using 'off the shelf' malware to launch attacks. Similarly some state actors are willing to conduct financial and intellectual property theft or to conduct denial of service attacks which are more often associated with criminals or hacktivists.

Cyber criminals

Cyber criminals seek to exploit UK organisations and infrastructure for profit.

Their technical sophistication varies from small scale cyber-enabled fraud to persistent, advanced and professional organisations. They may directly steal money or monetise their capabilities indirectly through intellectual property theft, through extortion (issuing ransom demands following denial of service or data theft), or through malware.

All these factors amount to a significant cyber threat to UK business. As reported in the Cyber Security Breaches Survey 2016, 65% of large UK firms detected a cyber security breach or attack in the past year. The report you are now reading aims to raise awareness and share knowledge of the threats and provide some guidance to business on how to mitigate against it.

Cyber extortion has increased

Cyber crime is becoming more aggressive and confrontational, with an increase in the use of extortion, whether it is through DDoS attacks, ransomware or data extortion. The Crime Survey for England & Wales demonstrates that computer misuse offences and cyber-related fraud are a more prominent threat than more traditional crime types.

Where the victim is suspected to have the means to pay, and/or when the data is likely to be particularly valuable to the victim, higher ransoms may be demanded.

Ransomware remains the most common cyber extortion method. Current trends to be aware of include:

- A move towards targeting specific businesses, where the rewards can be greater.
- To counter mitigation efforts, more ransomware is incorporating locker techniques that prevent the downloading of decryption tools. For example, new variants have been observed that copy and extract the files and then delete the originals. Once the ransom is paid by the victim the copied files are sent (as seen targeting MongoDB installations).
- As the ransomware market begins to mature, new strains increasingly employ unusual features to attract media attention in a saturated marketplace.

The threat of ransomware attack means that business should consider further mitigation and preventative solutions to combat it. These include maintaining appropriate backups and defensive systems that automatically sandbox email attachments.

The 'Internet of Things' botnets are growing…

Until recently, few could have imagined consumer devices would present a growing threat to the functioning of the Internet. Yet one of the most significant cyber security stories of 2016 was the rise of botnets exploiting security flaws in internet-connected webcams, CCTV, digital video recorders (DVRs), smart meters and routers.

The threat comes from internet-connected devices, part of the 'Internet of Things' (IoT), that are vulnerable to remote code execution or remote takeover. Many connected devices have been shipped with less secure software and default passwords. There is often no obvious way for consumers to update them, change passwords or otherwise fix security problems.

It is assessed that huge numbers of insecure devices can easily be found online. The Shodan search engine reveals, for example, over 41,000 units of one insecure model of DVR are connected to the Internet as of January 2017. All are vulnerable to being taken over by malware. The problem affects a wide range of manufacturers and products, and the risks of insecure devices were emphasised recently by NCSC Technical Director Dr Ian Levy, who demonstrated how an insecure device, in this case a doll, could be used to interfere with otherwise inaccessible products.

Hacktivists

Hacktivists aim to raise awareness for their cause. They focus on propaganda, defacement and DoS attacks. Few hacktivists can carry out a successful DoS attack against organisations with mitigations in place. This includes reputational hackers who seek to compromise a business simply to demonstrate their skill. Reputational hackers range from very low skilled individuals using tools purchased online, to highly skilled experts.

Insecure connected devices can easily be recruited into a botnet which can then be used to mount DDoS attacks on an overwhelmingly large scale. The attack on internet performance management company Dyn's DNS servers provides some illustration of the harm that IoT botnets can do. We should expect more such attacks, possibly on an even larger scale, in the future.

…but will they last?

The situation is likely to improve eventually. In the future, it may be possible to mitigate the impact of insecure devices. Meanwhile, there are likely to be more recalls of insecure devices, as has happened with one brand of CCTV cameras. Government also has a part to play in promoting smart device security and helping to develop standards such as the NCSC's and the Department for Business, Energy & Industrial Strategy's (BEIS) work to ensure the Smart Metering System has proportionate security measures in place, further details of which can be found online. This sits alongside work currently underway (and led by the Department for Culture, Media and Sport) to set government's overarching policy position on 'secure by default' products and services.

Despite this, millions of insecure smart devices will remain connected to the Internet before they fail or are replaced by their owners. Malware authors will continue to exploit them to mount attacks and will continue working to find fresh vulnerabilities. The 'botnet of things' will present a serious challenge to cyber security for a considerable time to come.

Anyone can be (or hire) a cyber criminal

Easy access to offensive cyber capabilities, such as ransomware or DDoS, has allowed individuals and groups to have an impact disproportionate to their technical skill. This year has seen attacks carried out against UK-based companies, that despite requiring little skill caused considerable disruption and were widely reported on by international media. For example, users of the Netspoof stresser targeted gaming providers, government departments, internet hosting companies, schools and colleges.

Operation Vulcanalia

The NCA Operation Vulcanalia targeted users of the Netspoof DDoS-for-hire tool. Based on intelligence gathered by the West Midlands Regional Cyber Crime Unit, a week of action in December 2016 saw more than 60 individuals targeted, resulting in 12 arrests, over 30 cease and desist notices served, two cautions issued and one protective visit made.

The developer is less exposed to the risk of deploying the malware itself but will still generate income, whilst the user gains access to tools and techniques that they would not normally be able to develop or use. As such the cyber-as-a-criminal-service model will continue to expand in terms of users and the range of services offered, especially with the source code of some malware variants freely available (e.g. Mirai).

Financial trojans have become more targeted and less visible

The distinction between typical criminal and state sponsored targets has been blurred by the Bangladesh Bank heist of February 2016. $81 million was stolen through fraudulent transactions sent via the SWIFT payment gateway following months-long activity. The number of crime groups engaged in similar activity for financial gain has increased in the wake of the Bangladesh heist.

One important example of this is the group behind the banking trojan Dridex. After a brief hiatus, spam runs for Dridex resumed in July 2016 with an updated payload. This new version of Dridex appears to target the back-office infrastructure of financial companies, with potential targets including a range of payment systems. The volumes of spam in this campaign were much lower than previous Dridex campaigns, suggesting a move towards a more targeted approach, possibly inspired by the high financial returns of the Bangladesh Bank heist.

Additionally, other financial trojans have started to come back into prominence. Ramnit returned in summer 2016, specifically targeting 6 major UK banks and Trickbot targeted banks in the UK, Australia and Germany, which may share links to the previously disrupted Dyreza trojan. In both cases, the trojans had previously been subject to substantial law enforcement disruption in 2015, further illustrating the resilient nature of top banking trojans.

The back-end systems and associated services of larger institutions will continue to be a target. If successful, an attack could have a major and substantive impact upon a UK bank. The specialist skills required to accomplish such a targeted attack may eventually be offered as-a-service and consequently become available for sale in the wider cyber criminal community, as the traditional banking trojan methodology remains resilient and extant.

Sophisticated actors don't need to be sophisticated

Some sophisticated actors are attracting attention for less sophisticated (but nonetheless effective) methodology that contrast the complexity of their usual cyber attacks. Businesses should be aware of the threat from nation states and in particular intellectual property theft, which is likely to impact organisations with a unique market offering.

Nation states

Nation states may seek to exploit UK businesses to further their own national agenda and prosperity.

Campaigns by nation states are often persistent, focusing on (but not limited to) espionage and intellectual property theft, taking place over many years and using significant technical capability.

'Dropping Elephant' (DE), is a group exposed by Kaspersky Lab in July 2016 and appears to have been active since at least November 2015. DE targets organisations, mainly in Asia, that are involved in economic and diplomatic activity related to China's foreign relations. It uses spear-phishing emails containing malicious payloads designed to exploit vulnerabilities in unpatched versions of Microsoft Office. DE also uses fake websites disguised as a news portals which deliver malicious payloads. Both are simple but effective social engineering techniques that use known exploits, some of which have patches available.

Similarly, Carbanak malware, which has been used by criminal groups to steal millions of dollars from Russian banks, has been known to exploit old MS Office vulnerabilities via attachments used in spear-phishing emails. These methods – spear-phishing, booby-trapping MS Office files and exploiting old vulnerabilities – are in contrast to previous sophisticated malicious actor behaviour, some of which have invested heavily in uncovering zero-day exploits and developing advanced, modular cyber espionage platforms customised to attack targets. These examples demonstrate however that it is not always necessary for sophisticated actors to invest in developing state-of-the-art technical exploits.

Nation states and other malicious actors will continue to develop sophisticated capabilities. However, continued success using old vulnerabilities and techniques means they are not required to reveal their hand. Instead they can use unsophisticated attacks on less well-protected victims, saving their best tools for the most rigorously defended targets. A plateau in the level of sophistication used to compromise organisations is concerning, as it could imply that defenders are not keeping pace with attackers.

The mobile threat is low, but is growing

Mobile malware continues to increase in both volume and sophistication, however the percentage of infected devices remains very low. There have been no reported cases of a mobile malware infection being used to pivot into a corporate enterprise network. It is more likely that mobile attacks will form part of the attack chain to target consumers and organisations, for example being used as a reconnaissance tool to gain access to various user login credentials. Trends worth watching include:

- Malicious apps which initially manifest as a nuisance, such as by delivering excessive adverts (adware), are increasingly also requesting elevated permissions. Malicious actors could use elevated permissions to install further malware such as key-loggers which could be used to steal login credentials.
- Fake apps mimic a brand or organisation to trick users into downloading them and entering credentials which are then stolen. Fake versions of various business enabling apps such as email and media sharing apps, all appeared in 2016. The vast majority don't make it on to legitimate app stores, but dozens of fake retail apps were discovered last year.
- SMS phishing, or SMishing, is often more effective than traditional PC phishing campaigns due to lack of awareness and implicit trust in the personal nature of SMS messages. Furthermore, a malicious SMS with a spoofed TPOA (the SMS header field that contains the message sender's number) will appear in the correct conversation thread, making it even harder to spot as a SMishing attempt. The Mobile Messaging Fraud Report 2016, polled 6,000 consumers and found that 58% received an unsolicited SMS message each week, with a third reporting that the message attempted to trick them into disclosing personal data.

Insider threats

Insider threats often have more knowledge of an organisation's vulnerabilities than any external threat. Insiders can be inadvertent - employees trying to bypass cumbersome security procedures or opening a malicious attachment. They can also be malicious - motivated by a sense of personal grievance, ideological or moral conviction, financial difficulties or pressures applied by external actors. Insiders can provide attackers with login credentials or can conduct activities such as data exfiltration.

Social media as an attack vector

Malicious actors have followed their victims onto social media, exploiting the environment of trust and familiarity that these sites facilitate. With abuse of trust being the primary mechanism for starting an attack, social engineering is thriving on social media. If employers allow their employees to use corporate machines for social media, it is possible that those employees could click on links from social media connections, which presents the same risks as opening links in phishing emails. This is especially the case on professional networking sites where the information shared allows malicious actors to select targets.

Terrorist organisations

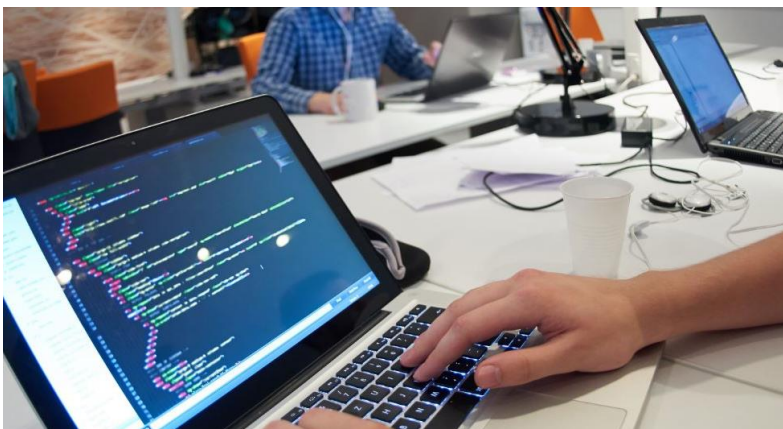
Terrorist organisations have limited cyber capability. Whilst they may aspire to use cyber to cause a destructive attack, this remains unlikely. It is more likely these groups will conduct cyber-enabled attacks, such as identifying potential victims through social media networks.

Social media accounts can also be used as command and control (C2) infrastructure. Security researchers have discovered malware campaigns which use Twitter and Instagram, highlighting that because many users interact with social media sites several times a day, it is easy for C2 channel traffic to appear normal.

The most commonly exploited vulnerabilities could have been patched

The most commonly exploited vulnerabilities in 2016 were well known and failing to patch legacy systems is leaving many organisations unnecessarily vulnerable. The vulnerability known as Heartbleed is one of the most published and discussed vulnerabilities in recent history, being disclosed in early 2014. Yet despite the wide coverage, even in mainstream media, a recent Shodan report suggests that there are still over 200,000 websites vulnerable.

The range of vulnerabilities being exploited is also increasing as a result of bad security practices in connected devices. Because of hardcoded or default admin credentials left on routers provided by ISPs, attackers were able to push fake firmware updates designed to recruit them into a botnet. Notably, the 'Annie' Mirai based botnet used an exploit that, instead of compromising the attacked devices, effectively created denial of service conditions which prevented users from accessing the Internet and other services. This is one example of where the Government's Cyber Essentials scheme, which lists 'patch management' among its five technical controls, can assist in improving an organisation's cyber security.



The year in review: pivotal incidents of 2016

Five pivotal cyber incidents of 2016 changed the security landscape. They included the largest recorded cyber heist, the largest DDoS attack and the largest data breach ever revealed. The attacks on the Bangladesh Bank, Democratic National Party and Ukrainian energy infrastructure also demonstrated the boldness with which threat actors can operate. Whilst some of the events may not have occurred in 2016, the aftermath or full impact was not felt until that year, and as such they have been included in the review.

Destructive attack on Ukrainian power supply

SIGNIFICANCE: This is a watershed incident in cyberspace, primarily because it's the first confirmed case of cyber-enabled disruption to electricity supply on a regional scale. Often when discussing cyber attacks, it is difficult to extract the real-world impact, which tends to be a second or third order effect. However, in this case the physical impact on thousands of citizens brought home the very tangible effects that a cyber attack can have.

VICTIM: Ukrainian energy distribution companies

INCIDENT: Three Ukrainian energy distribution companies were victim to cyber attack in December 2015, resulting in electricity outages for approximately 225,000 customers across the Ivano-Frankivsk region of Western Ukraine. Attackers gained unauthorised entry into a regional electricity distribution company's corporate network and ICS. Subsequently seven 110 kV and twenty-three 35kV substations were disconnected for three hours.

METHODOLOGY: Spear-phishing emails with malicious Microsoft Word attachments containing BlackEnergy 3 (BE3) malware. BE3 did not directly cause the outage, but rather was used to gain access to the business networks of electricity supply companies.

Attackers reportedly gained access to networks more than six months prior to the December 2015 power outage. This was followed by the theft of credentials from corporate networks. The corporate VPNs and remote access tools were used to enter and manipulate ICS networks.

KillDisk malware was then deployed to erase the master boot record on targeted systems and log deletion to hide presence on networks. In one instance, attackers launched a telephone DoS attack to delay customers reporting outages to the affected company's call centre.

IMPACT: Attackers overwrote the firmware on critical devices used by the affected companies, forcing operators to control devices manually, leading to a significant drop in productivity. The length of the power outages was limited because technicians on site manually overrode circuit breakers and restored power after a few hours. However, more than two months after the attack, control centres were still not fully operational.

Historic Yahoo! data breaches

SIGNIFICANCE: Whilst this incident did not occur in 2016, it had significant impact this year for two reasons:

The scale. There are few incidents, in cyber or otherwise, that have the potential to impact such a large portion of the global population. This is likely to manifest itself through secondary attacks which use leaked details to target other organisations, such as credential stuffing, which exploits re-used passwords and usernames to compromise other accounts, and which is likely to have increased because of these breaches.

The cost. It is difficult to estimate the final cost to users whose accounts have been compromised, this will depend on many factors such as the success of follow-up phishing or fraud attempts. In business terms, after the revelation, the purchase price of Yahoo!'s core internet business by Verizon was reduced by $350 million to $4.48 billion. The decision could set a precedent for how cyber security can affect the valuation of an organisation.

VICTIM: Yahoo! and its customers

INCIDENT: In August 2013, data associated with one billion Yahoo! user accounts was accessed by an unauthorised party. Yahoo! believe the breach is distinct from another incident that occurred in 2014 which impacted 500 million user accounts. The stolen data reportedly included names, email addresses, telephone numbers, dates of birth, hashed passwords and in some cases, encrypted and unencrypted security questions and answers.

METHODOLOGY: Yahoo! stated that the 2013 breach occurred when an unauthorised third party stole data associated with accounts. Yahoo! has not been able to identify the intrusion associated with this theft. Outside forensic experts are conducting an ongoing investigation into the creation of forged cookies that could allow an intruder to access Yahoo! users' accounts without a password. Yahoo! have connected some of this activity to the 2014 data theft.

IMPACT: Breached data is often sold through the online criminal marketplace. Personal data can be used by criminals to access other accounts held by the victim, or even to create convincing phishing emails. It is likely that some victims of the Yahoo! breaches have been targeted for phishing campaigns or identity fraud.

Hacking the US Democratic Party

SIGNIFICANCE: This marks the first recorded attempt to use cyber to influence the democratic process in the US. The incident highlights the significant reputational damage that can occur if internal corporate documents or emails are leaked and has drawn attention to the potentially significant influence cyber attacks could have on democratic processes.

VICTIM: Elements of the Democratic Party, including the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC) and the email account of the Clinton campaign's chairman.

INCIDENT: In mid-June 2016, it was reported that the networks of the Democratic National Committee (DNC) had been compromised. A month later, thousands of stolen emails and attachments were published by WikiLeaks. The Democratic Congressional Campaign Committee (DCCC) was also attacked and documents on congressional races in a dozen states were leaked in August 2016. Two months later, WikiLeaks published a third wave of hacked emails, this time from the email account of the Clinton campaign's chairman. Further data was leaked by DCLeaks.com.

METHODOLOGY: The attack was carried out in the spring of 2016 using phishing emails sent to political figures. These enabled hackers to steal account credentials, implant malware and exfiltrate data. In the case of Clinton's campaign chairman, the phishing email took the form of a fraudulent account reset request apparently from Google.

IMPACT: It is reported that the DNC replaced its computer system, laptops and phones at short notice, while the DCCC shut down its system for a week. The DNC leaks prompted numerous critical press articles on the emails' contents. The subsequent DCCC leaks led to criticism from political opponents of Democratic congressional candidates. The Head of the DNC also subsequently resigned.

Theft of $81,000,000 from Bangladesh Bank

SIGNIFICANCE: The attack was a tailored attack which exploited the bank's access to the SWIFT payment system, used to securely transmit information and instructions among financial institutions. As such the attack targeted global financial services infrastructure through a specific bank and it is likely that the attacker will attempt to use this technique against other financial institutions. Perhaps unsurprisingly, the number of criminal groups targeting SWIFT has increased in the wake of the Bangladesh Bank heist. A new version of the Dridex financial trojan was launched in June 2016 with enhanced features, including functions to identify payment platforms, such as SWIFT.

VICTIM: Bangladesh Bank

INCIDENT: In February 2016, $81m was stolen from Bangladesh Bank by targeting the bank's SWIFT system. BAE reported that bespoke malware was used to attack the bank's infrastructure which also had the capability to manipulate the Bangladesh Bank's legitimate internal SWIFT payment orders system. BAE released further analysis on 13 May which indicates that at least one other financial institution, in Vietnam, has been targeted by the same threat actor.

METHODOLOGY: A police investigation into the theft has stated that the bank's IT technicians may have connected its SWIFT international payments system to the Internet while setting up a connection to the bank's domestic payments system. The technicians reportedly also left a hardware token inserted in the server for months at a time, though it should have been removed and stored securely after business hours each day.

Earlier findings from a Bangladesh government inquiry indicated failings such as technicians disabling anti-virus software and staff keeping a 'secret notebook' of login IDs and passwords on the system. The attackers injected six types of malware which captured keystrokes and screenshots. The investigators suspect that an insider at the bank provided the attackers with technical details about its computer network, as the malware was customised for the bank's system.

IMPACT: In December SWIFT, the global payment messaging system, warned users of an increased cyber threat to its systems, describing the threat as, "very persistent, adaptive and sophisticated – and here to stay." After the Bangladesh Bank attack, other cyber crime groups have ramped up their efforts to attack the SWIFT system, attacking mainly weakness in local security to compromise networks and send fraudulent messages requesting money transfers.

Public release of the Mirai malware source code

SIGNIFICANCE: DDoS attacks using botnets are not new. However, the rapid exploitation of the connected devices market to launch unprecedented, large and sustained attacks is a step change. The number of devices that could be recruited into a botnet has significantly increased and will continue to do so. Gartner estimate there will be 21 billion connected devices by 2020. It is highly likely that criminals will seek to monetise the Mirai botnet both in renting it out as a premium DDoS-for-hire service capable of launching notably large DDoS attacks in an otherwise crowded DDoS-for-hire marketplace. The threat from the Mirai botnet is here to stay.

VICTIM: Multiple victims, including the Brian Krebs security website, network provider OVH, and internet performance management company, Dyn. Indirect victims included organisations such as PayPal and Twitter. UK telecommunications provider TalkTalk and Post Office customers also reported internet connectivity outage following Mirai router scanning activity.

INCIDENT: Mirai is the name of the malware currently infecting vulnerable, connected devices. It is also the name of the botnet made up of compromised connected devices. The source code for the Mirai malware was released to the public in October 2016, and has led to a significant lowering of technical barriers to entry in the launching of large, sustained DDoS attacks. The attack against Krebs was the largest on record to date with a peak attack size of 665 Gbps. The network provider OVH reportedly suffered multiple attacks exceeding 100 Gbps individually, which collectively resulted in a 1 Tbps attack.

METHODOLOGY: Mirai scans for 68 user name and password combinations when seeking to brute force, infect and control a connected device. Attackers issue commands to infected devices worldwide, which then direct internet traffic to overwhelm victim sites and disrupt service provision. Newer variants of Mirai have been seen to scan for vulnerabilities within routers as an alternative means of infection.

IMPACT: The immediate impact is disruption to services, which varies according to the capability of a victim to deflect attacks. In some instances, attacks have caused disruption to services regardless of DDoS mitigation in place. There are financial costs associated with disruption recovery, as well as reputational costs for organisations whose customers are affected during attacks. Interestingly, the owners of infected connected devices suffer minimal disruption, making it difficult to encourage them to take measures to secure their devices.

Horizon scanning: future threats

The most impactful attack of 2017 will be against the Internet's 'building blocks'

In 2017 it will be tempting to focus on new technology and innovations such as the Internet of Things. However, we expect that the most impactful attacks will be directed at building blocks on which the Internet runs, rather than innovative technology.

The Mirai botnet attack on a DNS server provider is an example of this. The use of IoT devices to launch the attack was innovative, but arguably it was impactful as it targeted part of the Internet's critical infrastructure. Domain Name Servers providers translate human readable domain names into internet addresses, acting as the phonebook of the Internet; this helps users find the websites they are looking for. There are many critical internet services, other than DNS, including website hosting, email, database servers, authentication and authorisation. Whilst they are not all vulnerable to the same attack methodology as DNS, a successful attack on one could have an equally far reaching impact.

Rather than attacking a single website an attacker could target an upstream provider critical to the functioning of an organisation, such as DNS. An attack on upstream services would affect many organisations, serving to obfuscate the actual target or other simultaneous attacks.

Attacks on industrial connected devices will continue to increase

It is highly likely that connected devices in industry are already targeted and that incidents are more common than are currently reported or that have been detected. In the past, most industrial systems were securely locked down and not accessible to the outside world, but as more industrial systems become connected, the risk of an attack greatly increases. In some cases, sufficient safeguards are still not in place to protect these systems that were never designed to connect to the Internet.

Gartner predict that by 2020 there will be 21 billion connected devices used by both industry and consumers. Industry adoption of connected devices has often been overlooked compared to consumer adoption, however Gartner estimate it to be occurring at a faster pace, due to the demand for cost effective solutions in areas such as energy (e.g. smart meters), physical security (e.g. networked security cameras) and facilities automation (e.g. connected indoor LED lighting).

Connecting services and devices can have unexpected consequences, especially in industries that have not previously had to consider cyber security risks. A stark example of this was seen in Finland in 2016, when denial of service conditions disabled residential automated heating systems in apartment blocks for more than a week. Connected devices often provide tangible competitive and business advantage, but conversely the risk of connecting devices may be difficult to assess. As a result, it is likely that there will be an increase in high profile incidents which impact businesses because of lax security in connected devices.

Threat actors will not just encrypt or leak data – they will tamper with it

Attacks which tamper with, rather than steal or deny access to data, have always been a feature of cyber security. An attack on the integrity of data is particularly dangerous when the victim is not aware that changes have been made.

In December 2015 Juniper Networks announced that it had discovered "unauthorised" code embedded in an operating system running on some of its firewall products since August 2012. This would have allowed an attacker to gain control of affected firewalls and possibly even to decrypt VPN connections. Using an integrity attack against software to create VPN backdoors has considerable downstream effects, weakening security in their customers' networks, which may well have been the attacker's intentions.

In 2017, we may see the success of this technique encourage similar methods. This could impact numerous industries beyond IT. For example, at the end of 2016 cyber security researchers Security Research Labs (SR Labs) demonstrated how it was possible for relatively unsophisticated actors to change online flight bookings. Researchers suggested that access to booking data could enable an attacker to cancel or rebook a flight, or to steal passengers' reward miles.

Connected consumer devices will get ransomware

As the number of connected devices increases, so too does the potential cyber attack surface. Connected consumer devices will contain huge amounts of personal data, which could be targeted by criminals seeking to commit extortion or fraud using tailored malware.

In 2017 it is likely that ransomware will target connected devices containing personal data such as photos, emails, and even fitness progress information. This data may not be inherently valuable, and might not be sold on criminal forums but the device and data will be sufficiently valuable to the victim that they will be willing to pay for it. TrendMicro has released an analysis of Android mobile ransomware which locks the victims screen rather than encrypts data and can lock smart TVs as well as mobile phones. It is important to highlight that smart devices are still inherently more difficult to attack than computers. Incidents may initially be limited to users who download apps from third party app stores.

Ransomware on connected watches, fitness trackers and TVs will present a challenge to manufacturers, and it is not yet known whether customer support will extend to assisting with unlocking devices and providing advice on whether to pay a ransom.

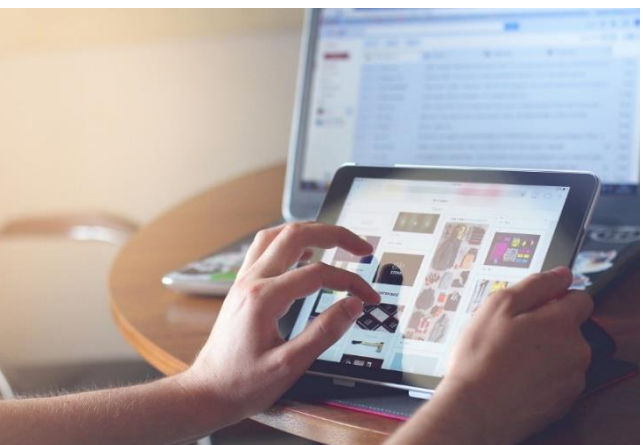
Attribution will become harder

Attribution is vital in understanding an actor's intent. Public attribution of actors forms an important part of deterrence. However, it is likely that attribution will become more difficult as malware is increasingly tailored for each victim and attackers use non-persistent implants which leave little trace of their presence for traditional forensic techniques to analyse.

There are four factors which will contribute the increased difficulty of attribution:

1. The rise of file-less malware. This allows attackers to directly inject payloads into the memory of running processes and execute without copying files to a hard drive. This makes the attack hard to detect and, because it does not write to a disk, it is difficult to forensically analyse and reconstruct. Memory resident malware and rootkits are types of malware that have file-less capabilities. These techniques allow an attacker to perform whatever action they need and to leave no trace that the victim has been compromised.
2. Bespoke malware for each victim. Tailored attacks and malware which may never have been observed before are difficult to attribute to a threat actor. If a different methodology and different tools are used for each attack, then there are no consistent features to connect the attacks to each other or to attribute to a threat actor.
3. 'Off the shelf' malware. Malware which is available for purchase on criminal forums or freely available online, such as the Mirai source code, can be acquired by any attacker with the available funds.
4. False flags. Often easier to create in the cyber domain than in the physical world, false flags are used as a misdirection tactic to deceive or misguide attribution attempts. Outsourcing, purchasing or mimicking exploits or otherwise designing an attack to look like another threat actor's *modus operandi* can confuse investigations.

These factors make it difficult to identify and reconstruct attacks. Even if they can be reconstructed, the attacks themselves are either unique or ubiquitous, making it difficult to attribute. Attribution is important in helping law enforcement and government conduct take-down operations of organised cyber crime groups. As such it is crucial that industry continues to report incidents which may help build the wider threat picture and support efforts to end criminal activity.



Fighting back: what can business do?

Challenges for business

There are both opportunities and obstacles within UK businesses for risk mitigation. In the current environment, no organisation is immune to the cyber threat. Cyber defence is characterised by complexity, requiring the involvement of all parts of any business to succeed. The landscape is therefore skewed in favour of the attacker, whose job is considerably simpler. There are three areas for businesses to consider:

Technology. It is possible to defend against all but the most determined and technically capable attackers, by investing appropriately in cyber resilience. However, many companies continue to fall victim to attacks enabled by the exploitation of basic and well known vulnerabilities (such as SQL injections or Local File Inclusions).

People. Cyber security is a complex sociotechnical system, in which people are a crucial component and can be the strongest link. Consideration given to good security design, usability, workflow and balancing information loads (giving the right training and awareness interventions at the right times) can help prevent compromises. An organisation's staff can be one of its most effective defences, yet for many businesses a lack of user-centred security design is leaving them vulnerable.

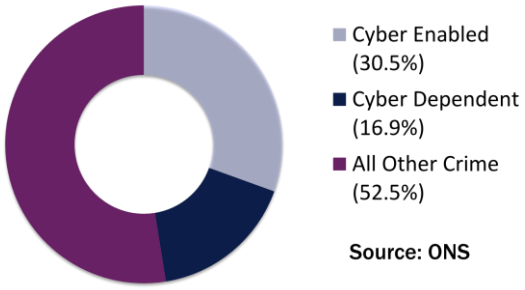
Processes. The digitalisation of processes and business is happening at an unprecedented pace, which can create vulnerabilities which could be exploited. Indeed, digitising a bad manual process often makes attacks scale more effectively. Many businesses, especially smaller ones, may have difficulty in balancing cyber defence with their available resources, especially if it impacts upon accessibility (both for staff and customers) or profitability. These issues are exacerbated by the size and/or complexity of some businesses themselves. For example:

- Teams within the same organisation not communicating with each other. This can lead to a simple failure to report important security information or an assumption that someone else is responsible for the risk.
- Security services contracted out to third party providers. This can lead to a mindset that risk has been 'out-sourced'. However, reputation cannot be outsourced and businesses will always bear ultimate responsibility for their security.
- Resource and awareness. Small to medium enterprises (SMEs) often do not have the resource to implement cyber security measures or are not aware of the risks.

What can we do to fight back?

No organisation can fully mitigate against the cyber threat. However, there are many opportunities that can dramatically reduce the potential impact of an attack by adopting the guidance and advice offered within existing initiatives.

Cyber crime as a proportion of total UK crime



1. Reporting means we can fight back

The threat of cyber attacks on UK businesses is serious and increasing. However, there is no clear understanding of the true scale and cost of cyber attacks to the UK, as it is widely under-reported both by industry and individuals.

Action Fraud only received 1,073 cyber dependent crime reports from businesses year ending October 2016. However, a successful attack can have a significant impact to a company's reputation, finances and systems. In fact, businesses are more at risk from a cyber-enabled or dependent crime than more traditional crime types.

If cyber attacks are reported, law enforcement agencies can investigate, arrests can be made and preventative actions can be taken.

Crucially, an organisation which has been the victim of a cyber attack - even one which they have successfully mitigated - may be subject to further attacks. This may be because the attacker is persistent, or more simply, because the organisation is perceived as an easy target.

Having an accurate understanding of the impact of cyber attacks helps us understand how to resource and fund the fight back.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Action Fraud is the UK's national fraud and cyber crime reporting centre. If you believe you have been the victim of online fraud, scams or extortion, you should report this through the Action Fraud website, where they can offer live support 24/7. If appropriate, Action Fraud will report it to the relevant police force or other law enforcement bodies (including the NCA).

www.actionfraud.police.uk

2. Successful risk mitigation

Risk mitigation efforts are successful when key decision makers are engaged. The more devices that your organisation connects to the Internet, the more exposed you are to potential attack, and there is a market for the many types of business and personal data that business leaders need to protect. Investment in cyber security is therefore critical if you wish to protect the operating capability, finances and reputation of your business. It is a case of when, not if, you will be targeted, and even basic cyber defences can protect against most attacks.

3. Managing cyber security

Cyber security is most effective when integrated well with risk management. Businesses can refer to a wide range of good cyber security guidance and adopt one or more of the available schemes to achieve a recognised level; ultimately the aim is to make it hard for attacks to be successful and be ready to respond to cyber security incidents. Depending upon the size and current security stance of an organisation, once basic cyber security is achieved, then build upon that as appropriate, e.g. SMEs may achieve cyber security fundamentals, whereas larger organisations should aim for greater depth.

General Data Protection Regulation

The General Data Protection Regulation makes breach notification mandatory in some situations. GDPR is designed to harmonise data privacy laws across Europe. Under this legislation, breach notification becomes mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals." Failure to do so can lead to sanctions being imposed, with a maximum penalty of up to €20 million, or 4% of annual worldwide turnover (whichever is greater).

The Cyber Essentials scheme was developed to show organisations how to protect themselves against low-level 'commodity threat'. It lists five technical controls (access control, boundary firewalls and internet gateways, malware protection, patch management and secure configuration) that organisations should have in place. In addition, the government will work with law enforcement agencies to significantly enhance the levels of resilience against cyber attack across UK networks.

Fundamentals:

- understand the impact of cyber attack
- implement basic cyber security to protect your business, such as Cyber Essentials and training your people, who can be part of your best defences

Greater depth:

- take cyber security further with 10 Steps to Cyber Security or an international standard and an enterprise cyber security mindset
- apply cyber security to all areas of your business, such as cloud services, business and personal devices or specific technologies used in the organisation
- maintain and share awareness of current threats

4. Promoting awareness

Business has a unique opportunity to promote awareness of stronger basic 'cyber hygiene' across British society, including for their customers and employees. Examples include:

- The promotion of existing cyber security advice, such as the use of strong and varied passwords by using the NCSC password guidance, available online.
- Where personal details are collected online, businesses are responsible for securely storing and processing it, using best practice encryption and other security technologies to minimize the impact of a successful attack.
- The signposting of Action Fraud on relevant company websites, to ensure customers know where to report cyber crime.

5. Reporting cyber incidents: what to report and who to report it to

Reporting is vital to the combatting the threat. It allows law enforcement to investigate crime and improves understanding that can inform future response. A more complete understanding of the scale of cyber crime can also help law enforcement respond, resource and fund prevention and protection efforts more effectively. Successful arrests and prosecutions act as deterrent and help change the misconception that cyber crime is risk-free crime, demotivating and discouraging other cyber criminals from conducting attacks.

Action Fraud is the UK's national fraud and cyber crime reporting centre. If you believe you have been the victim of online fraud, scams or extortion, you should report this through the Action Fraud website. If appropriate, Action Fraud will report it to the relevant police force or other law enforcement bodies (including the NCA).

A significant cyber security incident can also be reported to the NCSC by following the steps outlined on the website. In these cases, the NCSC provides direct technical support and cross-government co-ordination of response activities. The NCSC defines a significant cyber security incident as one which may impact on UK's national security, economic wellbeing or can to cause major impact to a large portion of the UK population or to the continued operation of an organisation.

6. Sharing knowledge and expertise

All businesses can benefit from sharing knowledge and expertise in a secure, confidential and timely manner through services such as the Cyber-security Information Sharing Partnership (CiSP). By sharing knowledge, we gain:

- early warning of cyber threats, allowing businesses to respond and adapt, potentially limiting the number of potential targets
- shared capabilities to better investigate, analyse and mitigate the threat
- shared experience, where lessons can be learnt and processes improved

Furthermore, industry and law enforcement collaboration is vital for tackling some of the more serious cyber threats. Industry expertise has greatly enhanced law enforcement operations, leading to significant disruption and judicial outcomes.

CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business. Over 2800 organisations and 8000 individuals have signed up to this free service.

www.ncsc.gov.uk/cisp

7. Developing cyber skills and awareness

Partnership work between law enforcement and industry has led to the improvement of cyber knowledge for the wider public and industry. This has encompassed a wide range of activity, tailored for businesses large and small. This ranges from Regional Organised Crime Units facilitating industry breakfast meetings, and attendances at local events and conferences, to the creation of academic courses in partnership with universities. Some further details on selected initiatives are outlined below.

NEW TALENT: As part of CyberFirst, we support the development of the UK's next generation of cyber professionals. Our student residential courses and undergraduate bursary scheme are helping the UK nurture talent for a future in national security.

CERTIFICATION AND SPONSORSHIP FOR HIGHER EDUCTION: Working with partners in government, industry and academia, we identify and support excellence in cyber security education and research and encourage industry investment in academic research. This includes supporting virtual academic research institutes, certifying degrees, recognising Academic Centres of Excellence in Cyber Security Research and sponsoring doctoral studentships at these academic centres.

INDUSTRY: The UK is a world leader in innovation and research. The NCSC aims to support, encourage and facilitate cyber security research and innovation within the UK. This includes initiatives such as the Cheltenham Innovation Centre (designed to help cyber security start-ups navigate those difficult early months of business) and the Industry 100 scheme which invites organisations to embed staff within the NCSC.

Case studies illustrating UK LEA and industry joint protect work

NCA
National Crime Agency

Following the operation to dismantle the Avalanche cloud-hosting service, which was led by Europol, the FBI and German police and supported by partners from 30 countries including the NCA, the NCA teamed up with a range of industry partners, including Trend Micro, F-Secure, McAfee, Microsoft, Norton and ESET, to offer advice and solutions to both remove the related malware and to protect against future incidents of it.

POLICE SCOTLAND
Keeping people safe

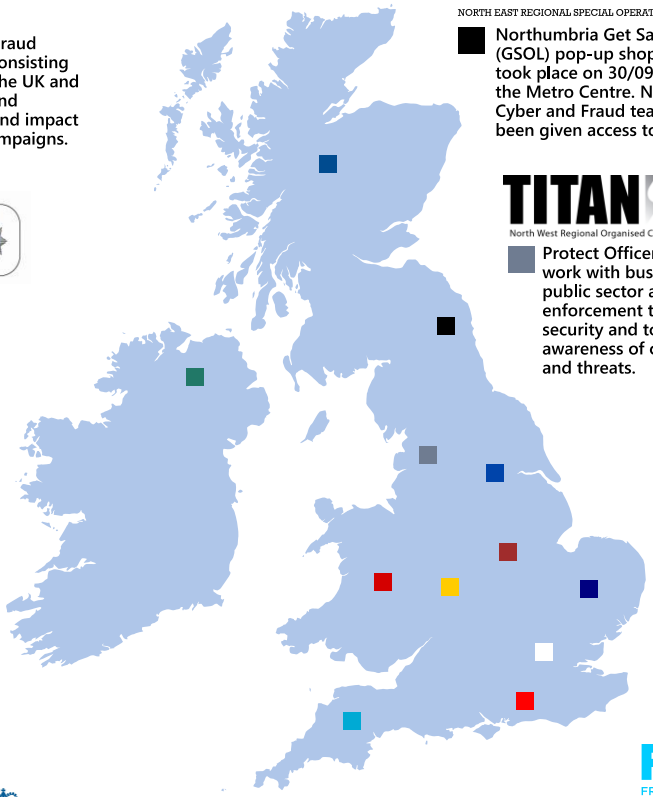
Police Scotland and Scottish Universities have collaborated to create the Cyber Badge, a 12 week cyber security course focusing on password security, online bullying, grooming, computer crime and social networking as well as an introduction to computer science.

POLICE SERVICE OF NORTHERN IRELAND

PSNI have engaged with the Fraud Liaison Group (FLG) a group consisting of major banking retailers in the UK and Ireland. PSNI have attended and presented on the mechanics and impact of industrial scale phishing campaigns.

NERSOU
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT

Northumbria Get Safe Online (GSOL) pop-up shop two day event took place on 30/09/16 & 01/10/16 at the Metro Centre. Northumbria Cyber and Fraud teams have also been given access to the CiSP.



East Midlands Special Operations Unit

EMSOU have engaged with locally based global brands. This has included a stress test event with a number of cyber scenarios where the companies response was tested at IT and senior level.

TITAN
North West Regional Organised Crime Unit

Protect Officers to continue work with businesses, public sector and law enforcement to drive cyber security and to raise awareness of current trends and threats.

POLICING
YORKSHIRE & THE HUMBER

Literature has been developed aimed at businesses, young people, carers, schools and vulnerable members of the community, with cyber crime advice and guidance distributed at events and presentations across the forces.

TARIAN

Protect presentations have been conducted focused on SME audiences. It is estimated that an audience of 700+ SMEs/organisations was reached in the last year.

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Essex Police, supported by ERSOU, hosted a 'Cyber Threat Awareness Conference' for businesses in and around the Eastern Region.

ROCU

The WMRCCU produced a video on cyber crime reaching an audience of thousands of local SMEs. They have also worked with BBC Midlands on material that was televised regionally and online.

Zephyr RCCU
South West Regional Cyber Crime Unit

Presentations, workshops and table top exercises have been undertaken by SMEs, NHS, Business forums and Universities. These have been throughout all five SW forces.

south east
Regional Organised Crime Unit

SEROCU support a banking customer security initiative and have given joint presentations to business partners. They have also conducted presentations, Q&A sessions and webinars for regional cyber security clusters.

FALCON
FRAUD AND LINKED CRIME ONLINE

The MPS Op FALCON team attended the ICE Totally Gaming Event where they offered fraud prevention advice to operators, regulators and customers, and also provided copies of their 'Little Book of Cyber Scams'.

Debate: can we stop the Internet from being used for crime?

The Internet has been compared to the Wild West, a place of lawlessness and no rules. Is this inherent in the Internet? Or is there a future in which it is possible for it to be a safe place for all? We asked two industry experts, both well respected in the cyber field, if they thought we could ever stop the Internet from being used in crime. Their answers are given below.

Matt Bottomley

Senior Manager - Cyber Risk
Lloyds Banking Group

"Yes"

Water, electric, gas and the internet. All modern-day essentials, but the Internet is not simply on or off like other utilities. It's multi-faceted in an online world with the most basic surfer demanding to understand more. What are the download speeds? Upload speeds? Ping rates? How strong is the Wi-Fi connectivity? Will I be able to watch movies on the go, do my online shopping and gaming, and have face-to-face chats with family members on the other side of the world?

To therefore suggest that even the most basic of user is powerless to understand how the Internet might be used to perpetrate crime against them is nonsense. With the majority of cyber attacks caused by some form of human negligence, the answer lies in equipping internet users who lack core digital skills.

As 'cyber security experts', we all have a role to play, including the UK government who have launched a plan to keep the UK at the forefront of the digital revolution by offering free digital skills to millions of individuals, charities and businesses by 2020.

But we shouldn't stop there. Identifying and pursuing cyber criminals poses a unique challenge to law enforcement as criminals operate across international borders - the direct reach of UK law enforcement is restricted with enforcement ending at national boundaries.

The threat is not restricted to international boundaries - Governments and law enforcement across the globe must work together to share intelligence and do more to ensure cyber criminals are pursued, disrupted and prosecuted to ensure the risk and cost to cyber criminals is increased. After all, even the Wild West was ultimately tamed.

James Lyne

Global Head of Security Research at Sophos

"No"

The Internet has grown far beyond the expectations of the original inventors. Its borderless nature and interconnectedness has allowed the Internet to develop vast resources. It has become a fundamental supporting pillar to education, finance and in many ways the whole of society.

However, the very interconnectedness that drives innovation also allows criminals to scale their attacks with lower risk, great anonymity and permits access to a huge number of potential victims. I personally do not believe the Internet can be secured to the point it cannot be used for crime, as that would require removal of much of the innovation and interconnectedness that makes it the valuable resource it is today.

As long as developers write code they will make mistakes and cyber criminals will capitalise. As long as people are online they will be tempted by 'unbelievable' deals and cyber criminals will find creative ways to trick people, as criminals always have in the real world.

That being said, just because crime cannot be eliminated does not mean we can't do more to prevent it. In many cases criminals take advantage of basic information security failures, such as terrible passwords, really out-of-date software or overt scams. The question is perhaps not 'can we make the Internet 100% secure?' but rather 'can we do better than we are today?'

The answer is absolutely yes. Policy makers and technologists have a part to play in enhancing the robustness of the technology, but more importantly we all can help by increasing awareness of security best practice. We can raise the cost for criminals and reduce the scale of their profits.

National Cyber Security Centre
a part of GCHQ

NCA
National Crime Agency

The cyber threat to UK business

2016/2017 Report

For further information, or to contact us, please visit:

www.ncsc.gov.uk @ncsc
www.nationalcrimeagency.gov.uk @NCA_UK