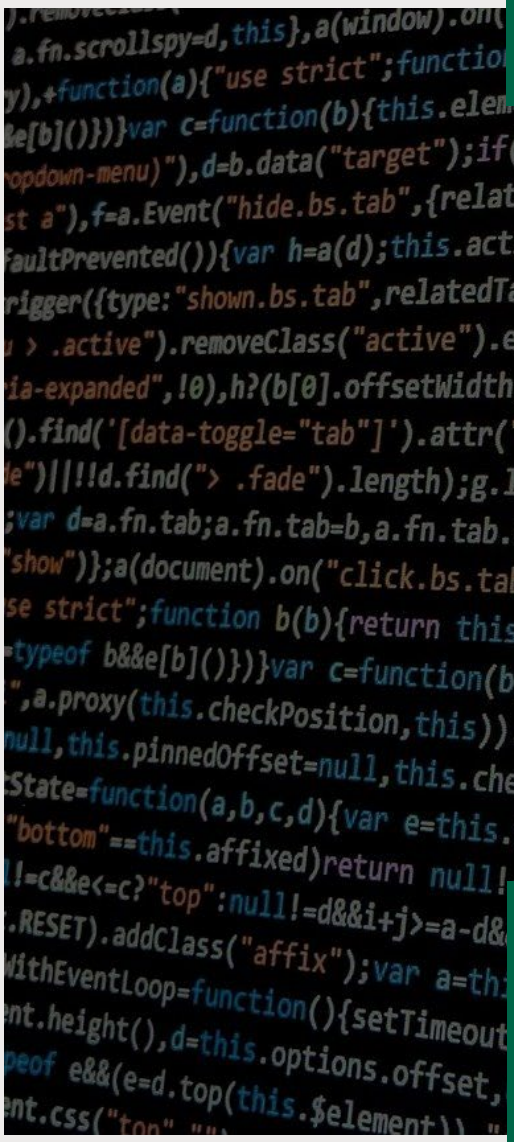
House of Commons Library

**Research Briefing**

22 June 2023

By Adam Clark

# Cybersecurity in the UK



Summary

## Image Credits

Image by madartzgraphics / image cropped. Licensed under Pixabay Content License - no copyright required.

## Disclaimer

The Commons Library does not intend the information in our research publications and briefings to address the specific circumstances of any particular individual. We have published it to support the work of MPs. You should not rely upon it as legal or professional advice, or as a substitute for it. We do not accept any liability whatsoever for any errors, omissions or misstatements contained herein. You should consult a suitably qualified professional if you require specific advice or information. Read our briefing 'Legal help: where to go and how to pay' for further information about sources of legal advice and help. This information is provided subject to the conditions of the Open Parliament Licence.

## Sources and subscriptions for MPs and staff

We try to use sources in our research that everyone can access, but sometimes only information that exists behind a paywall or via a subscription is available. We provide access to many online subscriptions to MPs and parliamentary staff, please contact hoclibraryonline@parliament.uk or visit commonslibrary.parliament.uk/resources for more information.

## Feedback

Every effort is made to ensure that the information contained in these publicly available briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

# Contents

# Summary

As IT systems become increasingly vital to the functioning of society and the economy, so too are they increasingly valuable targets for a variety of malicious activities. A cyber attack is an attempt by an unauthorised user to gain access to an electronic network or device. Cybersecurity is the practice of protecting IT systems devices and the data they hold from unauthorised access, interference, and use.

This briefing focuses on policy and legislative efforts to improve the UK's cybersecurity, broadly defined as resilience to cyber attacks. It does not discuss cyber in the context of military operations.

Cybersecurity policy is a reserved matter, as are many of the policy areas that it touches, including national security, product safety, and consumer protection. In devolved matters, such as education, the devolved administrations have their own strategies for implementing the UK Government's overarching cyber policy.

## Who carries out cyber attacks?

The cyber threat to the UK comes from a range of actors with differing motivations and levels of sophistication. They include state and state-sponsored groups, financially-motivated criminal organisations, and 'hacktivists' with political aims. The boundaries between these groups can be unclear. For examples, cyber criminal groups can operate with the implicit backing of states and (especially since the war in Ukraine) may choose targets, in part, for political reasons.

An additional complication is the rise in 'as-a-service' business models, where criminal groups or individual hackers sell their services to other actors.

## How are cyber attacks carried out?

Cyber attacks typically involve malicious software (known as 'malware') being executed on the target's system. Malware is an umbrella term for various types of software designed to damage, disable, and extract information from computer systems.

To carry out a cyber attack, threat actors typically need to:

- Develop or acquire malware;
- Identify a vulnerability in the target's IT systems – software applications, networks, devices – that allows them to install the malware;

- Deliver the malware to the target system and run it;
- Carry out the desired activities, such as stealing or encrypting data.

An estimated 95% of cyber attacks succeed due to human error on the part of users. This includes 'active' errors such as opening attachments in malicious emails and 'passive' errors such as using weak passwords.

## What is the impact of cyber attacks?

It is difficult to estimate the impact of cyber attacks because a significant amount of activity goes unreported. The available data is based on survey evidence, and it can be hard for organisations to quantify the impact of a cyber attack beyond direct effects, such as money paid to attackers.

The Cyber Breaches Survey, conducted annually by the Department for Science, Innovation and Technology (DSIT) reported in March 2023 that around a third of business and a quarter of charities had experienced a cyber attack in the previous 12 months. The larger the organisation the more likely they were to have experienced an incident: 69% of large firms and 76% of charities with annual incomes over £5 million reported breaches.

Larger organisations also face higher costs in responding to cyber attacks because they hold more data and attackers base ransom demands on the victim's ability to pay. In 2016, for example, a hair salon in Cheltenham was reported to have paid a £1,600 ransom after their computers were encrypted in an attack. At the other end of the scale, Capita, the UK's largest business process outsourcing firm, has estimated that responding to a ransomware attack in March 2023 will cost it £20 million.

## What is the Government's approach to improving cybersecurity?

Cybersecurity is a cross-cutting and technical issue. The key government departments are: the Cabinet Office, which has overall responsibility for cyber policy; DSIT, which is responsible for implementing large parts of domestic cybersecurity law and policy; and the Home Office, which is responsible for policy on cyber crime.

There are also various non-departmental public bodies involved in cybersecurity. The main one is the National Cyber Security Centre (NCSC), launched in 2016, which provides technical advice and guidance on cyber security.

Overarching policy on cybersecurity is contained in the National Cyber Strategy (NCS) 2022. The Strategy sets a series of objectives intended to achieve the Government's vision, which is that in 2030 the UK will

> continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals.

The NCS 2022 takes a 'whole-of-society' approach to cybersecurity, arguing that in order to improve the UK's resilience to cyber attacks the Government will need to work in partnership with private sector organisations and the cybersecurity profession.

One of the basic aims of the strategy is to shift the burden of cybersecurity from individual citizens to the organisations best placed to manage cyber risks. For this reason the Government is seeking to improve uptake of the NCSC's cybersecurity guidance, incentivise investment in cybersecurity measures, increase the number of skilled cyber professionals, and strengthen statutory cybersecurity responsibilities.

## How is cybersecurity regulated?

The UK's regulatory framework for cybersecurity consists of a patchwork of primary and secondary legislation. Different legislation covers the cybersecurity of IT systems, internet-connected products, and personal data.

Cybersecurity legislation is risk-based. Legal obligations are aimed at sectors and organisations where cybersecurity breaches would have a significant impact on society, the economy, or individual rights. This includes organisations designated under the Network and Information Systems (NIS) Regulations 2018 as operators of essential services (such as telecommunications and transport) or digital service providers (such as online search engines). The Product Security and Telecommunications Infrastructure Act 2022 will, once implemented, place cybersecurity requirements on manufacturers and distributors of internet-connected consumer products.

Organisations not covered by the above regulations will most likely encounter cybersecurity responsibilities through data protection legislation.

The obligations imposed by cybersecurity legislation are typically principles-based. They set general expectations regarding cybersecurity but do not prescribe specific measures that responsible organisations must take.

This approach provides organisations with a degree of flexibility in how they meet their cybersecurity requirements. The Government regards this flexibility as important given the rapidly changing nature of cyber threats. To support organisations, relevant government departments and regulators publish guidance tailored to specific sectors.

## Proposals for regulatory reform

The cyber threat landscape is constantly evolving as threat actors look for new methods and targets. Policy and legislation must therefore also adapt to keep up. Proposals for reform including the following:

- Reforms under debate among policymakers and industry stakeholders.

  - Whether there should be a defence in law for legitimate cybersecurity researchers who, in the course of their work, adopt methods used by malicious actors. This is known as 'ethical hacking'. Proponents of reform say that vulnerability to legal action has a 'chilling' effect on the cyber profession. Opponents say that permitting 'ethical hacking' could provide cover for malicious actors.

  - Whether ransom payments to cyber criminals should be banned. While paying ransoms to cyber criminals is strongly discouraged by the Government it is not illegal in most cases. Proponents of a ban point out that, while it is individually rational, paying ransoms is collectively irrational because it encourages criminals to engage in cyber attacks. Opponents argue that it is wrong to criminalise victims and that cyber criminals would likely adapt their methods in response.

- Reforms proposed by the UK Government through published consultations.

  - Strengthening the NIS Regulations by bringing more organisations into scope and broadening the range of incidents that need to be reported. The Government says that these reforms will be implemented once a "suitable legislative vehicle" is found.

  - Introducing a 'cyber duty to protect' which would place greater responsibilities on organisations who manage online personal accounts. The Government has not yet responded to this consultation.

  - Strengthening corporate responsibility by requiring large organisations to include a 'Resilience Statement' in their annual reports. The statement would set out the company's approach to managing threats to its resilience, including from cyber attacks. The Government has said that it will introduce the reforms but legislation has not yet been introduced.

- Reforms at the international level.

  - Negotiations are currently ongoing at the United Nations regarding a new international cybercrime treaty. Like the existing Budapest Convention, ratified by 68 countries including the UK, it would seek to harmonise cyber legislation and improve international collaboration on cyber issues. However, the treaty, which was proposed by Russia, has drawn criticism from human rights campaigners for its proposed criminalisation of 'content-based' activities in cyberspace such as disseminating 'seditious' material.

# 1 Understanding the cyber threat

As IT systems become increasingly vital to the functioning of society and the economy, so too are they increasingly valuable targets for a variety of malicious activites. A cyber attack is an attempt by an unauthorised user to gain access to an electronic network or device. Cybersecurity is the practice of protecting IT systems devices and the data they hold from unauthorised access, interference, and use.

This chapter discusses the cyber threat landscape. It looks at the groups who carry out cyber attacks, how they carry out attacks, and the impact they have on targets. The cyber threat landscape is constantly evolving as would-be attackers look for new vulnerabilities and new ways to exploit them. The final section of this chapter looks at some emerging cyber threats.

## 1.1 Who carries out cyber attacks?

The National Cyber Security Strategy 2016 identified the key actors that pose a threat to UK cybersecurity:

**Cyber criminals** – organised criminal groups, predominantly Russian-speaking and operating from Eastern Europe. Though financially motivated, cyber criminal groups are a significant threat. They typically operate by disrupting IT systems and demanding payments to stop the attack. Sophisticated groups can target high-value organisations, including governments and providers of essential services. Cyber criminals may also work as 'hackers-for-hire' and sell their services to others. This is discussed in section 1.4 below.

ENISA, the European cybersecurity agency, has observed a growing professionalisation among cyber criminal groups.[1] In February 2022, internal communications from Russian group Conti were leaked online, revealing an organisation with a similar set-up to a legitimate SME business, including an HR team, departmental budgets, and management structures.[2]

- **States and state-sponsored groups** – cyber operators acting directly or indirectly on behalf of nation states. Motives include espionage, financial gain, and retribution. Attacks generally target the government, critical

1 ENISA, Threat landscape 2022, 3 November 2022, p37. See for example, Times, How hackers are recruiting on the dark web, 7 May 2023

2 Krebs on Security, Conti ransomware group diaries, part 2: the office, 2 March 2022

national infrastructure (such as energy and telecommunications), and non-governmental organisations.[3] The National Cyber Security Centre (NCSC) regards Russia, China, Iran, and North Korea as the state actors that present the most acute cyber threat to UK interests.[4] The Parliamentary Office of Science and Technology briefing, States' use of cyber operations (October 2022), discusses this in more detail.

- **Hacktivists** – decentralised, issue-oriented groups with political motivations, such as Anonymous. While the majority of hacktivist activity is disruptive in nature, more capable actors have been able to inflict greater damage. ENISA reports that Russia's war in Ukraine has "defined a new era for hacktivism", with prominent hacking groups picking sides.[5] For example, one group, NB65, announced that it would only target Russian organisations and donate the proceeds to Ukraine.[6]

- **Less skilled individuals** using methods developed by others. They do not pose a substantive threat to the UK as a whole because they lack the skills to threaten well-defended targets such as critical national infrastructure. However, they can have a significant impact on the individuals and smaller organisations they target.

## 1.2 How are cyber attacks carried out?

To carry out a cyber attack, threat actors typically need to:

- Develop or acquire malicious software (malware);
- Identify a vulnerability in the target's IT systems – software applications, networks, devices – that allows them to install the malware;
- Deliver the malware to the target system and run it;
- Carry out the desired activities, such as stealing or encrypting data.[7]

### Malicious software

Cyber attacks typically involve malware being executed on the victim's system. Malware is an umbrella term for various types of software designed to damage, disable, and extract information from computer systems. The choice of malware depends on the actor's goals. Examples include:

3 See for example FCDO, Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion, 10 May 2022
4 NCSC, Annual Review 2022, 1 November 2022, p8
5 ENISA, Threat landscape 2022, 3 November 2022, p40-41
6 Secure World, NB65 hackers attacking Russian orgs in Ukraine retaliation, 11 April 2022
7 Adapted from Lockheed Martin, Gaining the advantage: applying Cyber Kill Chain methodology to network defense, accessed 23 March 2023

- **Ransomware** prevents users from accessing their device or the data stored on it. This is usually achieved by encrypting the files. The attacker then demands a payment in return for decrypting the files. A more aggressive 'double extortion' tactic involves the attacker stealing sensitive data and threatening to make it public. [8] Ransoms range from hundreds of pounds for individuals to millions for large organisations.[9] According to the NCSC, ransomware is the most significant cyber threat facing the UK. Cybersecurity firm Sophos estimates that just under 70% of cyber attacks in 2022 involved ransomware.[10]

- **Spyware** is designed to sit unnoticed on a device. It monitors the target user's activity and extracts data, enabling a third party to acquire sensitive information. Sophisticated spyware such as Pegasus, developed by Israeli firm NSO Group and licenced to state actors around the world, can remotely activate a device's camera and microphone.[11] Pegasus has reportedly been used to target politicians, journalists, and civil society activists, including in the UK.[12]

- **Bots** are computers infected with a malware that allows them to be controlled remotely. Groups of infected devices, called a 'botnet', can be used for various purposes such as carrying out Distributed Denial of Service (DDoS) attacks. In a DDoS attack, a bots attempt to access a target server at the same time, overloading the server and causing hosted websites to run slowly or crash.

## Vulnerabilities

Hackers gain access to IT systems by exploiting vulnerabilities. In this context an IT system includes devices, networks, and software applications. A vulnerability is a weakness in an IT system that allows it to be used in an unauthorised way.

Vulnerabilities often exist due to flaws in the system's coding – the series of instructions that governs how a system behaves. Modern IT systems depend on complex coding, and small mistakes or oversights can leave systems vulnerable to exploitation. In other cases vulnerabilities may be found in deliberate features in the system, especially features that automate certain tasks for the sake of convenience. User error can also be a source of vulnerability, such as misconfigured security settings.

8 CipherTrace, Double extortion ransomware jumped by nearly 500% last year, 18 April 2022

9 RUSI, Ransomware: a perfect storm, 29 March 2021, p5

10 Computer Weekly, Almost three-quarters of cyber attacks involve ransomware, 25 April 2023

11 Guardian, The Pegasus Project: What is Pegasus spyware and how does it hack phones?, 18 July 2021. NSO states that it only sells its software to "vetted government customers" to conduct cybersurveillance of criminal and terrorist groups.

12 BBC News, No 10 network targeted with spyware, says group, 18 April 2022

In each case the vulnerability allows the attacker to insert their own malicious code into the system, and have it execute the instructions without them being recognised as malicious.

### 1 The race to find vulnerabilities

Developers of IT systems (called 'vendors') are constantly trying to find and fix vulnerabilities before they can be found and exploited by malicious actors. Known vulnerabilities are added to public databases such as the Common Vulnerabilities and Exposures (CVE) list, maintained by the MITRE Corporation. There are currently over 200,000 records on the CVE list.

Independent cybersecurity researchers also search for vulnerabilities. Some vendors run bounty schemes that reward 'ethical hackers' for disclosing vulnerabilities. However, because their activities are difficult to distinguish from malicious hackers, independent researchers can be vulnerable to prosecution. For more information on this see section 4.1 below.

A vulnerability that has been identified by malicious actors but not by the vendor is called a 'zero day' vulnerability, because the vendor has had zero days to work on a fix.

Once discovered, it is good practice for software vulnerabilities to be publicly disclosed so that users can take mitigating measures. For most users this will simply involve installing a software update distributed by the vendor. Organisations with more resources may have cybersecurity teams dedicated to proactive penetration testing: attempting to breach their own IT systems using a database of known vulnerabilities.[13]

## Delivery methods

There are various ways in which malware can be delivered to and deployed on a target's system. Broadly speaking the attacker will try to either trick a user into running malware or gain access to the system directly and run it themselves.

Polling carried out by the thinktank Demos found that a quarter of UK citizens believe that no security measures they can take will stop a hacker who has decided to access their data.[14] In fact, most cyber attacks are relatively unsophisticated and can be stopped with basic cybersecurity precautions. According to IBM, human error is a major contributing cause in 95% of cyber breaches.[15] Human error, in this context, involves:

'Active' failures of decision-making, such as:

13 NCSC, Penetration testing, 8 August 2017

14 Demos, The great cyber surrender, November 2020, p13.

15 IBM, Cyber security intelligence index 2014 [PDF], p3, accessed 9 December 2022

- Clicking malicious attachments;
- Entering login credentials on malicious websites.

'Passive' failures to take adequate cybersecurity precautions, such as:

- Using default or easy-to-guess passwords;
- Not installing security updates;
- Poorly configured access and security settings.

### Methods exploiting decision-making

The most common method for delivering malware is through emails with malicious attachments or links. Cyber attackers use a range of more or less sophisticated social engineering techniques to trick targets into opening attachments or following links. This technique is known as 'phishing' or, if it is tailored to a specific target, 'spear-phishing'. Attacks that target high-value individuals such as politicians are also known as 'whaling.'

An advisory note by the NCSC details the spear-phishing approach as used by two hacking groups, known as Seaborgium (based in Russia) and TA453 (based in Iran):

> Using open-source resources to conduct reconnaissance, including social media and professional networking platforms, SEABORGIUM and TA453 identify hooks to engage their target. They take the time to research their interests and identify their real-world social or professional contacts.
>
> They have also created fake social media or networking profiles that impersonate respected experts, and used supposed conference or event invitations, as well as false approaches from journalists.
>
> Having taken the time to research their targets' interests and contacts to create a believable approach, SEABORGIUM and TA453 now start to build trust. They often begin by establishing benign contact on a topic they hope will engage their targets. There is often some correspondence between attacker and target, sometimes over an extended period, as the attacker builds rapport. [...]
>
> Once trust is established, the attacker uses typical phishing tradecraft and shares a link, apparently to a document or website of interest. This leads the target to an actor-controlled server, prompting the target to enter account credentials.[16]

Research has found that targeted phishing emails can be highly effective, even if the target has a good awareness of the 'cues' that indicate a suspicious email.[17] Cues include poor spelling, grammar, and formatting; use of manipulative language such as time pressures or emotional appeals; and

16 NCSC, SEABORGIUM and TA453 continue their respective spear-phishing campaigns against targets of interest, 26 January 2023

17 Computer Weekly, Two-thirds of all 2022 breaches resulted from spear phishing, 24 May 2023

executable file attachments. One study, for example, found that people interpret and respond to cues differently depending on how well the email aligns with their workplace context. If the premise of the email appeared legitimate, users were less likely to attend to suspicious cues. Rather, they:

> tended to be more concerned with potential consequences that could arise from not clicking: failing to act, seeming unresponsive to an email, or not addressing a legitimate issue.[18]

By contrast, there is less evidence to suggest that people from certain demographic groups or with certain personality traits are more likely than others to fall for phishing emails.[19]

The world's most popular password is 'password'.

### Methods exploiting poor cyber hygiene

'Cyber hygiene' refers to various steps that individuals and organisations can take to reduce cybersecurity risks, such using strong passwords and multi-factor authentication, installing security updates, and limiting the number of users with administrator access to systems and networks.

Attackers can exploit poor cyber hygiene to gain access to devices and systems. For example, weak passwords can be guessed using readily-available tools that try common passwords until they find the correct login credentials. This trial-and-error approach is known as a 'brute force' attack. NordPass, a password management service provider, analysed data from 30 countries and found that of the top 200 most commonly used passwords, over 80% could be cracked in less than a second. The most popular password was 'password,' followed by '123456.'[20]

A related method, called 'credential stuffing', exploits that fact that most people use the same password across multiple devices and accounts. Cybercriminals can purchase login credentials leaked in a breach of one website's account data and attempt to use them to access other accounts.

It was reported in 2017 that a cyber attack on Parliament had attempted to gain access to email accounts with weak passwords.[21]

A failure to install security updates similarly leaves organisations and individuals vulnerable to cyber attacks exploiting known vulnerabilities. The WannaCry ransomware attack that affected 81 NHS Trusts in 2017 was successful because a security update that would have closed the vulnerability had not been installed.[22]

---

18 Kirsten Greene and others, User context: an explanatory variable in phishing susceptibility, Proceedings of the Network and Distributed Systems Security Symposium, accessed 7 December 2022

19 Yaniv Hanoch and Stacey Wood, The scams among us: who falls prey and why, Current Directions in Psychological Science, 2021, vol 30(3) [PDF]

20 NordPass, Top 200 most common passwords 2022, accessed 7 December 2022

21 Guardian, Cyber-attack on parliament leaves MPs unable to access emails, 25 June 2017

22 NAO, Investigation: WannaCry cyber attack and the NHS, 27 October 2017

The National Audit Office has highlighted the risks of public sector organisations using outdated software and operating systems. Developers will eventually stop supporting older systems when they have been superseded by new versions and are no longer widely used. Systems that no longer receive security updates from the developer are vulnerable if new exploits are discovered.[23]

Other methods of attack target internet-connected networks directly, so are only likely to be stopped by system-level cybersecurity precautions. Methods include SQL injection which exploits how web servers communicate with databases. For example, when a user enters their login details the server request the relevant account information from a database. The database will read the inputted username and password, and if they are both correct it will return the requested result. Threat actors can exploit this by inserting commands into a field that the database will read. As a simple example, adding 'OR 1=1' in the password field will tell the database to return the account information if either the password is correct or 1=1. As 1=1 is always correct, the actor would gain access to the user's account regardless of whether the password is correct.[24]

In June 2023 data belonging to companies including the BBC and British Airways was stolen in an attack that reportedly involved SQL injection.[25]

## 2 Technological and human defences

In its guidance on defending against phishing attacks, the NCSC provides a real-world example of the importance of both system and user-level defences. 1,800 emails containing malware were sent to a financial services firm, claiming to be regarding an invoice that needed urgent attention.

- 1,750 emails were blocked by the firm's email filtering system, which detected the presence of malware in the attachment.
- Of the 50 emails that reached employees' inboxes, 36 were ignored or reported. 14 attachments were clicked on, releasing the malware.
- 13 of the attempted malware installations were blocked because the user's system had the latest security updates.
- Malware successfully infected one device. It was detected and the device was quarantined before the malware could spread.

23 NAO, Modernising Defra's ageing digital services, 6 December 2022

24 Rapid7, SQL Injection Attacks, accessed 5 June 2023

25 BBC News, MOVEit hack: BBC, BA and Boots among cyber attack victims, 5 June 2023; Heimdal Security, The MOVEit hack affected BBC, British Airways, and Boots, 6 June 2023

### ‘Zero-click’ attacks

Common cyber attacks methods like phishing require some form of action on the part of a user. By contrast, zero-click attacks do not require any user interaction. They work by exploiting vulnerabilities in the way operating systems and software applications validate and process data. Email and messaging apps are often targeted, because they are designed to process data coming from unknown sources without any input from the device owner. Zero-click hacks have exploited the way Apple’s iMessage app processes GIFs and the way WhatsApp processes incoming video call data. In both cases, the exploit tricked victims’ devices into reading malicious code which installed spyware.[26]

Vulnerabilities like this are rare. Identifying them and developing ways to exploit them requires a high level of technical sophistication. Hacking groups can sell them for a high price on the black market.[27] Consequently, they tend to be acquired by state actors or state-sponsored groups to target high-profile individuals for espionage purposes. The WhatsApp exploit, for example, was reportedly used to install spyware on devices used by Catalan politicians and civil society figures in Spain.[28]

Because zero-click attacks exploit unknown vulnerabilities (also known as ‘zero-day’ vulnerabilities because the vendor has had zero days to work on a fix) and require no user action they are difficult to defend against. Mitigations advised by cybersecurity experts include using a separate device for sensitive information, deleting old messages, and leaving mobile devices out of the room during important face-to-face conversations.[29]

## Next steps

What happens once the attacker has gained access to an IT system depends on their motivations and exploitation method. The attack may end with the individual device that was initially targeted, for example if the goal was to infect it with ransomware for the purpose of extortion.

In other cases the attacker may seek to use the initial target as an entry point into connected networks and devices. This is known as ‘lateral movement’ and includes:

- Using the compromised user account to access confidential databases and other information;
- Sending phishing emails from the compromised account with a view to access accounts with greater system access (‘privilege escalation’);

26 Kaspersky, What is zero-click malware, and how do zero-click attacks work?, accessed 20 June 2023; Kaspersky, A matter of triangulation, 1 June 2023

27 Forbes, Windows 10 Zero-Click Security Exploit Wanted. Reward: $3 Million, 21 November 2021

28 New Yorker, How democracies spy on their citizens, 18 April 2022.

29 Guardian, Mobiles are ‘potential goldmines’ for hostile states, MPs warned, 17 November 2022

- Scanning networks to which the compromise device is connected to look for vulnerabilities (unsecured ports, applications without the latest updates, devices with default passwords).[30]

A threat actor may try to keep the initial access point open for future access, establishing what is known as an Advanced Persistent Threat (APT). This allows them to monitor the system and extract information over an extended period of time. Remaining undetected in a network requires time and sophistication. Cybersecurity firm Crowdstrike states that, as a result, APT attacks are typically carried out by "well-funded, experienced teams of cybercriminals that target high-value organizations".[31]

## 3 The role of cryptocurrencies

Cyber criminals typically demand that ransoms are paid in the form of cryptocurrency. Cryptocurrencies are a digital means of financial exchange. They were originally intended to overcome limitations of existing currencies and financial transactions. Unlike traditional currencies, which are created and guaranteed by governments and central banks, cryptocurrencies are decentralised.

While traditional financial transactions of any significance tend to generate a set of traceable records, once funds have been converted into cryptocurrencies, the public blockchain records transfers but does not link them to identified users. The global nature of the market means that funds may also enter and leave in different jurisdictions, further complicating efforts to follow the money.

Speaking at an event hosted by the Royal United Services Institute (RUSI), Will Lyne of the National Crime Agency said that before cryptocurrencies, moving ransom payments from one jurisdiction to another could cost 60-80% of the profits. Moving cryptocurrencies is much quicker and only costs "a couple of percent".[32]

Further detail can be found in the Commons Library briefing, Cryptocurrencies (February 2023).

The Government is seeking to strengthen law enforcement powers with regards to cryptocurrencies through the Economic Crime and Corporate Transparency Bill 2022-23. See section 5 of the Library's briefing on the Bill for more information.

30 Kaspersky, Lateral movement, accessed 23 May 2023
31 Crowdstrike, What is an Advanced Persistent Threat?, 28 February 2023
32 Will Lyne, speaking at RUSI, The societal impact of ransomware, 1 November 2022, 8:20-8:55

## 1.3 The scale and impact of cyber attacks

Understanding the true scale of cyber attacks in the UK – in terms of the number of attacks and the cost to victims – is difficult because the available data is largely based on self-reporting. The Government's Cyber Breaches Survey and Cyber Security Longitudinal Survey provide annual reports of UK businesses' cybersecurity experiences. Various private companies who provide cybersecurity services publish their own annual reports. These are often based on surveys of their clients, so their results differ based on the type of customer they work with. In addition, it can be difficult for victims to estimate the actual cost of a cyber attack, particularly indirect effects such as reputational damage.

The financial impact of cyber attacks can increase considerably with the size of the target organisation and the sophistication of the attack. In 2016, for example, a hair salon in Cheltenham was reported to have paid £1,600 ransom after their computers were encrypted in a ransomware attack.[33] At the other end of the scale, recovering from a ransomware attack in October 2020 is reported to have cost Hackney Council £12 million.[34] Capita, the UK's largest business process outsourcing firm, has estimated that responding to a ransomware attack in March 2023 will cost it £20 million.[35]

### Cyber Breaches Survey

The Cyber Breaches Survey reported in March 2023 that around a third of business and a quarter of charities had experienced a cyber attack in the previous 12 months. The larger the organisation the more likely they were to have experienced an incident: 69% of large firms and 76% of charities with annual incomes over £5 million reported breaches. This may in part be because larger organisations have more capacity to identify attacks. The survey notes that these figures likely under-report the true scale of the issue given that it is based on self-reported incidents.

The surveys show a long-term decline in the proportion of businesses affected by cyber attacks, down from 46% in the 2017 survey to 32% in 2023. The survey notes that this runs counter to qualitative evidence, which indicates a rising threat. As the decline is primarily driven by micro and small businesses, it speculates that attackers may be changing their behaviour to focus on larger targets, or that smaller businesses have become less able to identify and report cyber attacks. Separately, there have been reports of threat actors shifting their focus to countries in the Global South in search of less well defended IT systems.[36]

---

33 ITV News, Cyber thieves demand ransom after hacking salon's system, 27 June 2016

34 Wired, The untold story of a crippling ransomware attack, 30 January 2023

35 Times, Recovery from Capita hack to cost up to £20m, 10 May 2023

36 RUSI, Ransomware now threatens the Global South, 12 August 2022; Deutsche Welle, Ransomware: Cyber criminals are coming for the Global South, 28 August 2022

Of the businesses that had experienced a cyber attack, 24% reported that it had resulted in a direct negative outcome such as loss of money or data. Again, large businesses are more likely than average (33%) to report a negative impact.

The 2023 survey estimated that, among businesses that reported a breach with a negative outcome, the average cost of the single most disruptive attack was £2,950 for small and micro businesses and £15,800 for medium and large businesses. Costs include IT consultant fees, replacement systems or devices, insurance excesses, PR costs, and lost staff time.

It was estimated in the 2022 survey that the average cost per business for all cyber attacks they had experienced in the past 12 months was £4,200. A separate survey by Vodafone found that most SMEs with 0-49 employees would struggle to pay for an attack costing £4,200, with 19% saying that it "would likely destroy the business".[37]

## Other sources of data

Industry-specific surveys reveal similar results to the Cyber Breaches Survey. For example, MakeUK (which represents manufacturers in the UK) found that half of manufacturing businesses had experienced cybercrime in the year to May 2021. 63% said they lost up to £5,000 and 6% lost over £100,000.[38]

A survey of mid-sized companies (100-5,000 employees) by cybersecurity firm Sophos found that, on average, it cost UK organisations $1.08 million (currently £880,000) to rectify a successful ransomware attack.[39] IBM's survey of 550 global organisations found that ransomware attacks cost them $4.54 million (£3.7m) on average, not including the ransom itself.[40] Large-scale data breaches (up to 102,000 records compromised) cost a similar amount. IBM estimated (based on a very small sample) that a 'mega breach' involving tens of millions of records could cost organisations up to $387 million (£314m).[41] Both surveys include direct and indirect costs.

Looking at cyber crime more generally, a 2016 report for the Cabinet Office estimated an economic cost to UK businesses of £21 billion per year.[42] The majority of the cost was due to intellectual property theft and industrial espionage. The report estimated that the theft of customer data cost £1 billion per year and extortion £2.2 billion. It estimated that cyber crime cost UK individuals £3.1 billion per year, primarily from identity theft and online scams.

37 Vodafone, The business of cyber security, 15 February 2023, p9
38 MakeUK, Cyber resilience – the last line of defence, 4 May 2021
39 Sophos, The state of ransomware 2022, April 2022
40 IBM, Cost of a data breach 2022, 27 July 2022
41 IBM, Cost of a data breach 2022, 27 July 2022, p46
42 Detica, Cost of cyber crime, May 2016

# 1.4 Evolving cybersecurity challenges

The National Cyber Security Centre's (NCSC) 2022 Annual Review identified two main future cyber threat challenges facing the UK: the proliferation of cyber capabilities and supply chain attacks. ENISA, the European cybersecurity agency, has published a report predicting cyber scenarios in 2030 in which it also identifies the rise of connected products and artificial intelligence as emerging threats.

## Hacking 'as-a-service'

The NCSC report foresees a growing market for 'as-a-service' models whereby malware developers sell or lease cyber attack tools and services to other cyber criminals. For example, hacking groups offering ransomware-as-a-service may provide services such as:

- Ransomware files or its source code;
- Customization tools — for example for selecting the target's operating system, writing a custom ransom note, etc;
- Other malicious tools, such as programs that extract data before encryption;
- Instructions and technical support;
- Private forums for information exchange;
- Help negotiating ransoms.[43]

This business model extends cyber attack capabilities to organisations and individuals who would not otherwise have the know-how to carry out attacks themselves. According to the World Economic Forum, ransomware attacks increased by 435% in 2020, in part because ransomware-as-a-service has lowered the barriers to entry.[44] An investigation by the Sunday Times revealed that LockBit, the world's largest criminal hacking group, operates a franchise model whereby individual hackers can access LockBit's software and technical support in return for 20% of ransom fees they collect. The Times accessed LockBit's website and found "a job description, code of conduct, salary expectations and even a commitment to diversity" for would-be applicants.[45]

The NCSC report mentions the growing use of hacking services in corporate espionage and by 'hacktivists' with political motivations. For example, another Sunday Times investigation alleged that a hacker-for-hire group

43 Kaspersky, Ransomware-as-a-service (RaaS), access 7 December 2022
44 World Economic Forum, Global risks report 2022, 11 January 2022, ch 3
45 Times, How hackers are recruiting on the dark web, 7 May 2023

based in India has been paid to target UK citizens including Philip Hammond, while he was Chancellor of the Exchequer, and the BBC political editor, Chris Mason.[46] The group used phishing emails to gain access to confidential information. Similarly, Crowdstrike has reported a rise in access brokerage services, whereby a threat actor gains access to an organisation then sells this access to other threat actors such as ransomware groups.[47]

ENISA's assessment is that more sophisticated and comprehensive (and therefore expensive) 'as-a-service' groups are likely to be clients of nation states, who may use them to outsource their cyber operations. This trend, it says, will "certainly make the threat landscape more complex" by making attribution of responsibility to state actors more difficult and rapidly expanding cyber capabilities, including for purposes such as the surveillance of journalists and civil society.[48]

## Supply chain attacks

Many organisations now rely on digital systems to manage internal IT services and processes. As these systems become increasingly complex organisations may purchase them from third party suppliers, known as Managed Service Providers (MSPs), rather than developing and managing them in-house. This creates an interconnected digital supply chain. The National Cyber Strategy 2022 highlights the associated cyber risks:

> This increasingly complex landscape will make it even harder for states, businesses and society to understand the risks they face and how they can and should protect themselves. Increased dependency on third party suppliers of managed services, which often have privileged access to the IT systems of thousands of clients, is creating new risks that need to be addressed.[49]

Respondents to a 2021 call for evidence on supply chain cyber security highlighted various factors that were a barrier to managing cyber risks from their supply chain. These included limited visibility into supply chains and a lack of expertise or tools to understand supplier cyber risks.[50]

Digital supply chains have come to prominence in recent years following high profile attacks on MSPs. In a March 2020 attack, attributed to Russian state-affiliated group Nobelium, hackers inserted malware into a piece of IT monitoring software developed by SolarWinds, an MSP. The malware was unintentionally distributed to SolarWinds' clients when the company sent out a software update. As the malware was distributed as part of a legitimate update from a trusted source it escaped detection by users and anti-virus

46 Times, Exposed: the global hacking network that targets VIPs, 5 November 2022; Times, Caught on camera: confessions of the hackers for hire, 5 November 2022

47 Crowdstrike, Global threat report 2023, March 2023, p9

48 ENISA, Threat landscape 2022, 3 November 2022, p37-38

49 Cabinet Office, National Cyber Strategy 2022, 15 December 2021

50 DCMS, Government response to the call for views on supply chain cyber security, 15 November 2021

software.[51] In July 2021 a similar attack on another provider, Kaseya, spread ransomware to an estimated 800-1500 of its direct and indirect clients.[52]

At present there are few mandatory cybersecurity requirements for MSPs operating in the UK. In January 2022, the Government launched a consultation on amending the Network and Information Systems (NIS) Regulations 2018, the main piece of legislation governing the cybersecurity of the UK's critical national infrastructure.[53] The consultation proposed bringing MSPs into scope of the NIS Regulations if they provide an IT service to providers of essential services (such as health, transport, energy, and communications) that gives the MSP regular and ongoing access to IT systems. The proposals are discussed in more detail in section 4.3 below.

The Government Cyber Security Strategy 2022-2030 states that the Government aims to become an "exemplar" in managing the cyber risks from commercial products and services in supply chains by making cybersecurity "part of every procurement process."[54]

## Connected products and places

Connected products are any product that can connect to the internet and receive and transmit data. These products include a wide range of 'smart' consumer tech such as smart speakers and home security cameras. There are also an increasing variety of 'enterprise connected devices', from network-connected printers to devices that automate business processes. These products, in consumer and enterprise form, may also be described as internet of things (IoT) devices because they are designed to communicate with other smart devices.

ENISA's report on 2030 cyber threat scenarios notes that with a significant increase in the number of smart devices, consumers, manufacturers, and cybersecurity professionals could find it increasingly difficult to manage the 'cyber-physical ecosystem'. This, the scenario predicts, will increase the risk of cyber attacks that exploit misconfigured settings and outdated security software.[55]

An investigation by consumer charity Which? found that popular smart tech products from leading brands, including Amazon's Echo and Google's Nest doorbell, were easily hackable.[56] In most cases this was because the product had been superseded by a new version and the manufacturer was no longer releasing security updates for it.

Lack of support can be a particular problem for larger appliances that consumers expect to last for many years. A separate Which? survey found

51 Tech Target, SolarWinds hack explained: everything you need to know, 29 June 2022
52 ZDNET, Updated Kaseya ransomware attack FAQ: What we know now, 23 July 2021
53 DCMS, Proposal for legislation to improve the UK's cyber resilience, 19 January 2022
54 Cabinet Office, Government Cyber Security Strategy 2022 to 2030, 25 January 2022, paras 41-44
55 ENISA, Cybersecurity threats for 2030, 29 March 2023, p14
56 Which?, Smart products from the biggest tech brands easily hacked in Which? tests, 1 June 2022

that some smart washing machines, for example, would lose manufacturer security support after two years, despite having an estimated lifetime of 13 years.[57]

The NCSC says that this lack of security makes connected devices a "hugely attractive target for different types of threat actor".[58] While the smart device itself might not be a valuable target for cyber attackers, the fact that they are connected to the internet means that they can be targeted a means of accessing other devices and data on the same network (see Box 4).

The regulation of connected products is discussed in section 3.3 below.

### 4 The fish tank attack

As more products come with 'smart' functionality, an increasing number of devices are connected to wireless networks. This includes devices that users and manufacturers may not secure as well as they would a smartphone or laptop, because they do not hold valuable data.

One unusual example of how innocent-looking smart products can be targeted was reported by cybersecurity company Darktrace in 2017. According to Darktrace's CEO, Nicole Eagan, a casino in North America was hacked through a smart fish tank in its lobby.[59]

The fish tank was connected wirelessly to a PC that used sensors in the tank to regulate temperature, food, and cleanliness. Hackers used the internet-connect thermostat to gain a foothold in the casino's network They were then able to acquire customer data from the casino's servers and extract it through the thermostat to a server located in Finland.

## Artificial Intelligence

ENISA's report predicts a growing role for Artificial Intelligence (AI) in cyber activities. This includes AI as a target (attackers may try to manipulate the data sets used in legitimate AI applications, for example) and as a tool to enhance existing activities.

As discussed above, one common attack method is to use phishing emails to trick a target into downloading a malicious attachment or revealing their login credentials. According to insurance provider Allianz, attackers can use

57 BBC News, Smart appliances could stop working after two years, says Which?, 13 January 2023

58 NCSC, Organisational use of Enterprise Connected Devices, 10 May 2022

59 The Hacker News, Casino gets hacked through its internet-connected fish tank thermometer, 16 April 2018

AI applications to analyse publicly-available information about an individual or an organisation and use it to generate more convincing phishing emails.[60]

Allianz reports that these attacks are "increasingly" supplemented by AI-enabled deep-fake audio or video that mimics high-profile individuals.[61] Reports of this happening in practice are rare, however.[62]

AI may also help less sophisticated cyber criminals using mass, untargeted phishing techniques. Darktrace, a cybersecurity firm, has reported that threat actors have started using the AI chatbot ChatGPT to make phishing emails more sophisticated and engaging:

> We're seeing a big shift. 'Hey, guess what, you've won the lottery…' emails are becoming a thing of the past.
>
> Instead, phishing emails are much more about trying to elicit trust and communication. They're bespoke, with much more sophisticated language — the punctuation is changing, the language is changing. It's more about trying to elicit trust.[63]

60 Allianz, Cyber: the changing threat landscape, October 2022
61 Allianz, Cyber: the changing threat landscape, October 2022, p13
62 Tech Monitor, Will deepfake cybercrime ever go mainstream?, 31 October 2022
63 Times, AI used to write phishing emails, claims Darktrace, 9 March 2023

# 2 Cybersecurity policy

Cybersecurity has been on the policy agenda for over a decade: the 2010 National Security Strategy identified hostile attacks on UK cyberspace by other states and large-scale cybercrime as one of four 'tier one' (highest priority) threats to national security.[64] The Government published the UK's first Cyber Security Strategy in November 2011, and two more have followed. The current National Cyber Strategy (NCS) 2022 was published in December 2021.

This section provides an overview of the bodies with responsibilities for cybersecurity and of the NCS 2022. It then looks in more detail at two aspects of the NCS 2022: the Government's approach to improving the UK's cyber resilience and to international collaboration on cyber issues.

## 2.1 Roles and responsibilities

Cybersecurity is a cross-cutting and technical issue. As such, roles and responsibilities are spread across different government departments, agencies, and other organisations.

### Government departments

- **Cabinet Office** – has overall responsibility for cybersecurity policy. It publishes the National Cyber Strategy.
- **Department for Science, Innovation and Technology** (DSIT) – responsible for the implementation of the Network and Information Systems (NIS) Regulations 2018 (discussed in section 3.2 below) and other aspects of domestic cybersecurity policy.
- **Home Office** – responsible for policy on cyber crime.
- **Ministry of Defence** (MoD) – leads on work to "detect, disrupt and deter" adversaries operating in cyberspace, including terrorists, large cyber criminal groups, and state actors. Oversees the National Cyber Force.
- **Foreign, Commonwealth and Development Office** (FCDO) – has policy responsibilities for the UK's international cybersecurity activities. This includes administering the Conflict, Stability and Security Fund which is partly used to help partner countries improve their cyber resilience. The

[64] Cabinet Office, A Strong Britain in an Age of Uncertainty: The National Security Strategy, 18 October 2010, p27

FCDO also oversees the National Cyber Security Centre and (alongside the MoD) the National Cyber Force.

### Public agencies

- **National Cyber Security Centre** – the NCSC is part of GCHQ and is designated under the NIS Regulations as the UK's:
  - Single point of contact, responsible for liaising with national and international partners;
  - Technical authority, responsible for providing expert technical advice to Competent Authorities and other organisations; and
  - Computer Security Incident Response Team (CSIRT), responsible for monitoring and reporting on incidents, conducting threat assessments, and providing early warning about cyber threats.

  The general responsibilities of the NCSC are set out in the National Cyber Strategy 2022.
- **Competent Authorities** – responsible for the implementation of cybersecurity requirements in specific sectors. They designate organisations in scope of the NIS Regulations, work with the NCSC to produce sector-specific cybersecurity guidance, and monitor and enforce compliance. For each sector the competent authority is the relevant UK or devolved government department and/or regulator. They are listed in Schedule 1 to the NIS Regulations.
- **Information Commissioner's Office** – responsible for data protection rules, and regulates Digital Service Providers under the NIS Regulations.
- **National Cyber Force** – the NCF is a partnership between the MoD and GCHQ. It is responsible for conducting covert operations to "counter, disrupt, degrade and contest" cyber threats from terrorists, criminals, and state actors. The NCF has published information about how it approaches cyber operations in a "legal, ethical and responsible" manner.[65]
- **National Crime Agency** – law enforcement agency responsible for combatting serious and organised crime. The NCA's National Cyber Crime Unit focuses on tackling cybercrime nationally and internationally.
- **UK Cyber Security Council** – independent body funded by DSIT that acts as the Chartered Institute for the cybersecurity profession. It is responsible for developing and embedding a set of professional standards. It also accredits cybersecurity qualifications.

[65] NCF, Responsible cyber power in practice, 23 April 2023

### Critical national infrastructure and other organisations

- **Operators of Essential Services (OESs) and Relevant Digital Service Providers (RDSPs)** – organisations designated as having specific cybersecurity responsibilities under the NIS Regulations. OESs are qualifying operators in critical sectors (energy, water, transport, health, and telecommunications). RDSP are qualifying provides of online search engines, online market places, and cloud services.

- **Other businesses and organisations** – in general, organisations not covered by the NIS Regulations are not subject to specific cybersecurity standards, although they may have legal responsibilities derived from data protection and corporate governance rules.

In evidence to the Joint Committee on the National Security Strategy (JCNSS), FTI Consulting and Clifford Chance LLP argued that the large number of Government bodies involved in cybersecurity "can hinder effective governance". They stated that, apart from the overarching National Cyber Strategy, there appeared to be "limited ministerial oversight and direction".[66] RUSI similarly argued in its evidence to the JCNSS that there has, to date, been a "lack of ministerial" interest in cybersecurity at the Cabinet Office, Home Office, and DSIT.[67]

## 2.2 National Cyber Strategy 2022

### Background: the National Cyber Security Strategy 2016

The Government's second National Cyber Security Strategy (NCSS) was published in 2016. Over the five-year lifetime of the NCSS the Government committed £1.9 billion (more than double the £860m spent on the 2011 National Cyber Security Programme)[68] to cyber security measures, "defending our systems and infrastructure, deterring our adversaries, and developing a whole-society capability – from the biggest companies to the individual citizen."[69]

The JNCSS's 2018 report, Cyber Security of the UK's Critical National Infrastructure, criticised the Government for failing to set out in the 2016 NCSS what, specifically, it wanted to achieve, or how it intended to monitor progress. It recommended that the Government resume publishing annual reports for the investment programme (which had occurred for the 2011-16

66 FTI Consulting LLP and Clifford Chance LLP, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114499, 20 December 2022

67 RUSI, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114435, 16 December 2022

68 The original amount quoted in the 2011 UK Cyber Security Strategy was £650 million. By the publication of the 2016 strategy the figure was £860 million.

69 The £1.9 billion was first announced in the National Security Strategy and Strategic Defence and Security Review 2015.

version) to improve transparency and external scrutiny, as well as committing to a programme-wide audit of the NCSP by the National Audit Office (NAO).[70]

The NAO published its report, Progress of the 2016-2021 National Cyber Security Programme, in March 2019. It found that despite more recent improvements in the Programme's management and delivery record, it was established with insufficient baselines for allocating resources, deciding on priorities, or measuring progress. The report recommended that future strategies should clearly set out a division of labour, and that the Government should consider a mixture of shorter programmes (rather than one five-year programme) in order to be more responsive to changing risks.[71]

## From cybersecurity to cyber power

The Government published the National Cyber Strategy 2022 in December 2021.[72]

Compared to the NCSS 2016, the NCS 2022 is far more wide-ranging. The 2016 strategy had looked at cyber as a security issue, with actions aimed at defending the UK from cyber attacks, deterring hostile actors, and developing the UK cybersecurity industry.

While cybersecurity is at the heart of the NCS 2022 it is part of the broader concept of 'cyber power', defined as "the ability to protect and promote national interests in and through cyberspace".[73] The Integrated Review 2021 had recognised that the importance of cyber power for achieving the UK's national goals in the "contested domain" of cyberspace. The NCS 2022 builds on this, predicting that cyberspace will be increasingly used by states to exert influence and project power It specifically highlights Russia and China as "systemic competitors" promoting an alternative, authoritarian vision for cyberspace.[74]

As noted by the Carnegie Endownment, the result of this broader perspective is a more comprehensive and strategic document that considers the UK's role in international cyberspace.[75] The NCS 2022 sets out the Government's vision for the UK as a "responsible and democratic cyber power":

> Our vision is that the UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals:

70 Joint Committee on the National Security Strategy, Cyber Security of the UK's Critical National Infrastructure, 19 November 2018, HL Paper 222, HC 1708 2017-29, p17-18

71 National Audit Office, Progress of the 2016-2021 National Cyber Security Programme, 15 March 2019, HC 1988 2017-2019, p 13-14

72 Cabinet Office, National Cyber Strategy 2022, 15 December 2021; HCWS484 15 December 2021 [National Cyber Strategy 2022]

73 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p11

74 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p30

75 Carnegie Endowment, The UK's Cyber Strategy is no longer just about security, 17 December 2021

- a more secure and resilient nation, better prepared for evolving threats and risks and using our cyber capabilities to protect citizens against crime, fraud and state threats
- an innovative, prosperous digital economy, with opportunity more evenly spread across the country and our diverse population
- a Science and Tech Superpower, securely harnessing transformative technologies in support of a greener, healthier society
- a more influential and valued partner on the global stage, shaping the future frontiers of an open and stable international order while maintaining our freedom of action in cyberspace.

## A 'whole-of-society' approach

The NCS 2022 argues that cyber power is "more distributed" than other types of power and that governments must "work with partners in order to attain and exercise it."[76] The strategy therefore takes a 'whole-of-society' approach to cybersecurity. This involves recognising that the Government needs to:

> build an enduring and balanced partnership across the public, private and third sectors, with each playing an important role in our national effort.[77]

In the national effort of keeping cyberspace secure, the NCS 2022 identifies a set of general roles across society:

- The UK Government is responsible for setting and enforcing laws and standards, actively countering the threat from hostile actors, facilitating intelligence sharing among different groups, and providing technical guidance.
- Major technology companies and the cybersecurity sector have a "crucial role" in ensuring that the cyber environment in which organisations and individuals operates is "secure by default" and resilient to emerging threats and challenges.
- Businesses and organisations have a responsibility to manage their cyber risks, protecting data and digital assets while maintaining services.[78]

By boosting the capabilities of and incentives for these groups to fulfil their roles effectively, the NCS 2022 aims to "remove as much of the burden of cyber security from citizens as possible".[79] However, it acknowledges that it is not possible to stop all cyber attacks. Individual citizens therefore have a personal responsibility to take reasonable steps to secure their own devices

76 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p20
77 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p11
78 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p37-38
79 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p36

and data. In this they will be supported by advice from Government and civil society organisations.

## Objectives of the NCS 2022

The strategy is structured around five pillars, each of which has 3-5 objectives. The objectives set out the steps the Government will take to achieve its 'vision' of the UK continuing to be a leading cyber power in 2030. In turn, each objective has a set of outcomes that the Government has committed to achieve by 2025.

As with the NCSS 2016 the Government said that it would not publish a 'performance framework' measuring progress against its objectives "due to the sensitive information contained". However, it did say that it would publish annual progress reports.[80] No report has been published at the time writing, though the first is due in the summer.[81]

### Pillar 1: Strengthening the UK cyber ecosystem

Objectives under the first pillar are intended to ensure that the UK has "the right people, knowledge and partnerships" to deliver a 'whole-of-society' approach to cybersecurity. The NCS 2022 marks a transition away from the Government's previous approach of directly funding centrally managed skills and innovation programmes. Instead, the Government said that it would act as a facilitator:

> Overall we will take on a more strategic role where we facilitate the coming together of industry leaders, academics, innovators, law enforcement, the national security community and others who want to collaborate on making the UK more resilient against cyber threats. We will align all the levers of government to support the cyber ecosystem, from how cyber is taught in schools to how economic regulations drive up standards, to ensure that the UK grows the vital capabilities necessary to secure ourselves against future threats. [82]

This, according to the Strategy, will ensure that the cyber ecosystem is "self-sustaining, not dependent on government interventions".[83]

Outcomes under this pillar to be achieved by 2025 include establishing a National Cyber Advisory Board to bring together industry, academia, and citizens; expanding the post-16 educational and opportunities in cybersecurity, including for underrepresented groups; developing and embedding professional standards in the cybersecurity industry; and growing the UK cyber sector faster than the global average.

80 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p115
81 HL6927, 13 April 2023
82 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p49
83 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p49

### Pillar 2: Building a resilient and prosperous digital UK

The Government aims to shift the cybersecurity burden from end users to organisations.

The second pillar seeks to boost cyber resilience across society. It considers cyber resilience in terms of three aspects: understanding the nature of the cyber risk; securing systems against cyber attacks; and ensuring that systems are able to minimise the impact of successful cyber attacks and recover quickly from them. The Government says that it will "set clear expectations" regarding cyber resilience "underpinned by the right framework of incentives, support and regulation".[84] The approach will be tailored to different audiences, from individuals to critical national infrastructure.

One of the Government's primary aims is to "transfer the burden of cyber security risk away from end users and towards those best placed to manage it."[85] That is, the burden of taking cyber security measures will be moved 'upstream' by ensuring that organisations make data, devices, and software more resilient to cyber attacks. For example, the strategy proposes to work with tech companies to build basic cyber protections into their products and services.

The Government's approach under this pillar was set out in greater detail in the Cyber Security Regulation and Incentives Review 2022, which is discussed in section 2.3 below. The NCS 2022 also acknowledges that efforts to build cyber resilience in the UK depend on cyber resilience in other countries. This is discussed in section 2.4 below.

## 5 Government Cyber Security Strategy 2022-30

Pillar 2 of the NCS 2022 included an ambition for the UK public sector to be an "exemplar of best practice" in terms of cyber resilience.

In support of this, the 2022-2030 Government Cyber Security Strategy was published in January 2022. Its central aim is to "significantly harden" critical government functions to cyber attack by 2025, and for the whole public sector to be "resilient to known vulnerabilities and attack methods" by 2030.

The strategy sets out various actions to achieve this. It includes adopting the NCSC's Cyber Assessment Framework (see Box 6 below) and establishing a Government Cyber Coordination Centre tasked with sharing threat intelligence and coordinating action across public bodies.

### Pillar 3: Taking the lead in the technologies vital to cyber power

Technologies vital to cyber power include: 5G; AI; blockchain; semiconductors; cryptography; Internet of Things devices; quantum technologies.

84 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p66
85 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p66

The objectives in this pillar that are directly relevant to cyber security revolve around ensuring that the UK is "at the forefront of the safe and secure development" of emerging technologies. This includes shaping the global consensus on technical standards and the deployment of new technologies.

### Pillar 4: Advancing UK global leadership and influence

The fourth pillar is concerned with using the UK's global influence to advocate for a "free, open, peaceful and secure cyberspace" against states that would pursue an "authoritarian vision for cyberspace".

Objectives include reinforcing the UK's existing alliances and work with multilateral organisations, and building deeper relationships with partners in Africa and the Indo-Pacific.

In particular, the Government says that it will demonstrate to partner countries that it is possible to address cybersecurity issues without adopting authoritarian methods.[86]

### Pillar 5: Detecting, disrupting and deterring our adversaries

In the final pillar, the NCS 2022 turns to offensive cyber capabilities and the UK's ability to 'detect, disrupt and deter' adversaries in cyberspace. It states that, with the NCSC, NCF, and national NCA-led law enforcement now established, the UK's approach will "shift to a more integrated and sustained campaign footing". The aim will be to increase the costs and risks of conducting cyber attacks against UK entities.

## 6 The NCS 2022 and the devolved administrations

While cybersecurity is a cross-cutting issue most of the policy areas it touches upon are reserved to the UK Government: national security, foreign affairs, telecommunications, product safety, and consumer protection. However, areas of devolved responsibility such as education impact the first two pillars of the NCS 2022. The devolved administrations therefore have their own cyber strategies, which are aligned with the UK Government's national strategy.[87]

The Welsh Government published its Cyber action plan for Wales in May 2023. It covers the cyber 'ecosystem', cyber skills, and cyber resilience.

The Scottish Government's Cyber Resilient Scotland contains four action plans for 2021-23, which cover cyber resilience in the public, private, and third sectors, and cyber skills.

In Northern Ireland, the Department of Finance's Cyber Security: A Strategic Framework for Action 2017-2021 was closely aligned with the NCS 2016. An updated overarching strategy has not yet been published. The Department for

86 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p194
87 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p38

the Economy's strategy, 10x Economy, includes measures to support Northern Ireland cyber industry and cyber skills. The UK Government has also provided funding through its New Deal for Northern Ireland.[88]

### Response to the NCS 2022

Commentators broadly welcomed the NCS 2022. RUSI, for example, welcomed the shift to a 'whole-of-society' approach to cybersecurity and the strategy's "impressively strategic and wide-ranging approach to cyber".[89] In particular, RUSI commended the NCS 2022 for its recognition that cybersecurity is so broad that it needs to be "hardwired into mainstream policymaking of all kinds" including education, industrial strategy, and foreign policy, and that it cannot be addressed by government and the NCSC alone.

However, RUSI did point to a lack of clarity on how the wide range of initiatives mentioned in the NCS 2022 would come together to achieve the "aspirational" objectives it sets out. BAE Systems stated that the broad aims relating to 'whole-of-society' engagement and international influence would require effective coordination across government departments and the private sector.[90] An article on the Strategy, Defence and Foreign Affairs website specifically argued that the initiatives to increase the supply of cybersecurity experts were "not encouraging" given the scale of the skills gap.[91]

An article by the Carnegie Endowment focused on the international aspects of the strategy.[92] The article notes that as cyberspace is an emerging realm of international politics, the best use of policy tools such as 'naming and shaming' states for malicious cyber activity is uncertain and should be continually assessed.

## 2.3 Approach to improving cyber resilience

Cyber resilience refers to an individual's or organisation's ability to resist cyber attacks and to recover quickly from successful attacks. The second of the NCS 2022's five pillars – building a resilient and prosperous digital UK – describes the Government's ambition to improve the cyber resilience of

88 Northern Ireland Office and DSIT, Minister of State announces UKG investment for NI's Cyber Security industry, 22 February 2023

89 RUSI, The UK Government's new Cyber Strategy: a whole of society response, 15 December 2021

90 BAE Systems, UK National Cyber Strategy: BAE Systems response, December 2021

91 SDAFA, The UK's National Cyber Strategy 2022 explained, 21 November 2022. Research by Ipsos MORI, commissioned by DCMS, estimated that the UK needed around 17,500 new cyber professionals each year but was only training 7,500: Understanding the cyber security recruitment pool, 23 March 2021

92 Carnegie Endowment, The UK's Cyber Strategy is no longer just about security, 17 December 2021

critical national infrastructure, public services, businesses and organisations, and citizens.

The Government's written evidence to the JCNSS inquiry on ransomware, in December 2022, stated that improving resilience was "key" to combatting the threat of cyber attacks: "People and organisations are not getting the basics right – poor configuration of devices and networks, poor patching of software, default passwords, and weak passwords."[93]

The Government set out more detail about its approach to improving cyber resilience in the wider UK economy in the Cyber Security Regulation and Incentives Reviews (RIRs) published in 2016 and 2022.[94] The main change between the two RIRs is the greater emphasis in the RIR 2022 on enabling and incentivising organisation to invest in cybersecurity. This follows from the NCS 2022's 'whole-of-society' approach to cybersecurity and its general aim of shifting the burden of managing cyber risks from individuals to organisations.

## The RIR 2016: regulation and guidance

Most individuals and organisations, in most of their activities, are not subject to statutory cybersecurity standards. The Government argued in the RIR 2016 that introducing statutory cybersecurity standards for the wider economy (that is, beyond providers of critical national infrastructure) would not be proportionate:

> It should ultimately be for organisations to manage their own risk in respect of their own sensitive data (e.g. intellectual property) and online presence. The Review findings also suggest that the impact of other regulation would anyway be limited, and unlikely to be effective enough to outweigh the burden on business. Imposing specific requirements could also encourage a 'compliance' culture rather than proactive cyber risk management.[95]

Instead, the Government said that it would pursue non-regulatory interventions to support organisations to improve cyber resilience voluntarily. The RIR 2016 concluded that data protection regulation (implemented in 2018) alongside voluntary action would be sufficient to "catalyse significant change in cyber risk management" in the wider economy.[96]

## 7 The NCSC's cybersecurity guidance

The NCSC publishes a wide range of guidance, including general guidance aimed at organisations of different size and individuals, and specific guidance

93 HMG, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114408, 16 December 2022, para 28

94 DCMS, Cyber Security Regulation and Incentives Review, 21 December 2016; DCMS, 2022 cyber security incentives and regulation review, 19 January 2022

95 DCMS, Cyber Security Regulation and Incentives Review, 21 December 2016, p3

96 DCMS, Cyber Security Regulation and Incentives Review, 21 December 2016, p11

covering topics such as phishing. It's main schemes for promoting cyber resilience are:

- **Cyber Aware** – a public information campaign (formerly called Cyber Streetwise) aimed at informing the public and small businesses about the cyber threat and how to protect themselves. The website includes a tool where people and businesses can check how secure they are online.
- **Cyber Essentials** – sets out five basic controls that organisations of all sizes can take to strengthen they defences against common cyber attacks: firewalls; secure settings; malware protection; user access control; and security update management. Through Cyber Essentials Plus organisations can have an auditor independently assess whether they meet the standards.
- **10 Steps to Cyber Security** – collection of guidance primarily aimed at medium to large organisations. It sets out how organisations can manage cyber risks by: understanding the risks they face, implementing appropriate mitigations; and preparing for cyber incidents.
- **Cyber Assessment Framework** – a collection of detailed guidance aimed at providers of essential services.
- **Active Cyber Defence** – a suite of tools and services designed to help organisations proactively defend themselves against common, untargeted cyber attacks. For example, the 'Exercise in a Box' tool provides resources allowing non-specialists to test their organisation's response to a cyber attack.

The Cyber Breaches Survey revealed that awareness of Government guidance and initiatives on cyber security had increased over time. In 2022, for example, 16% of businesses said they were aware of the Cyber Essentials scheme, compared to 8% in 2017. Survey results also showed an increase in the proportion of businesses that saw cybersecurity as a high priority, from 69% in 2016 to 82% in 2022.

However, awareness of cyber threats does not necessarily result in behavioural change.[97] Assessing the implementation of the 2011 and 2016 National Cyber Security Strategies, the RUSI argued that despite a decade of "publicity, exhortation, advice and engagement" there had only been limited change in the level of cybersecurity across the private sector, including in critical national infrastructure.[98]

97 Tommy van Steen and others, What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?, Journal of Cybersecurity, Vol 6 No 1, December 2020

98 RUSI, The UK Cyber Strategy: challenges for the next phase, 27 June 2019, p10

## The RIR 2022: a more proactive approach

The NCS 2022 acknowledged that there was a need to "drive up the level of private sector engagement and investment in cyber resilience".[99] In the RIR 2022, the Government noted that targeted regulation and the provision of advice and guidance by the NCSC have not, on their own, been sufficient to incentivise the necessary improvements to cyber resilience:

> It is clear to the government that its previous approach, set out in the 2016 Regulation and Incentives Review, is not delivering the requisite change at sufficient pace and scale. Government cannot leave cyber security solely to the marketplace to deliver widespread improvements in cyber resilience. In order to improve cyber resilience across the economy and society, the government needs to be more proactive and interventionist.[100]

Part of the more interventionist approach is regulatory, with reforms proposed to the NIS Regulations and the corporate governance framework. Alongside this, the Government is proposing to be more proactive in terms of enabling behavioural change by creating incentives and placing more responsibility on business leaders to "effectively manage cyber security as part of broader business continuity and operational resilience risk management".

The RIR 2022 states that the Government will:

- **Improve its understanding of why public messaging is not having the impact it needs.** For example, the Government says that it will work to develop and make available "impact information", defined as the direct and indirect, short- and long-term cost of cyber incidents. This, it says, will address the perceived lack of commercial rationale for investing in better cybersecurity and help organisations build a business case for investment. It has also commissioned Ipsos MORI to research a methodology for calculating the cost of cyber breaches.

  To help drive investment, the RIR 2022 promises work to develop cross-government policy interventions aimed at professionals whose position means that they can "normalise" cyber security investment. This includes procurement professionals and cyber insurance companies as well as boards, investors, and shareholders.

- **Increase uptake of the Cyber Essentials scheme.** The RIR 2022 states that DCMS (now DSIT) is working with the NCSC to understand the barriers faced by organisations in accessing the scheme, and to evaluate the scheme's effectiveness given the evolving threat landscape.

- **Improve resilience of essential services and digital services.** While the RIR 2022 argues that the NIS Regulations have been successful in boosting the resilience of essential services, it also acknowledges an increase in ransomware attacks on essential service providers and their

99 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p35

100 DCMS, 2022 cyber security incentives and regulation review, 19 January 2022

supply chains. The RIR 2022 therefore proposes to strengthen the NIS Regulations and to provide more guidance on supply chain cyber security. Regulatory proposals are discussed in section 4.3 below.

- **Drive greater accountability for cyber security in business.** The RIR 2022 says that the Government will consider ways to mandate large companies to "appropriately assess and address the cyber risks they face". The Government has since introduced two relevant proposals: a 'cyber duty to protect' that would apply to organisations who manage online accounts and reforms to corporate governance. These are discussed in section 4.3 and 4.4 below respectively.

- **Support the cyber security profession.** The RIR 2022 states that prospective and existing cybersecurity practitioners and the organisations hiring them need more support to navigate the professional qualification and certification landscape more effectively. Work in this area is being undertaken by the UK Cyber Security Council. The Council has published a tool to help cyber professionals map existing certification to sixteen core cybersecurity specialisms. It is also working on its own cyber accreditation scheme.[101]

In their evidence to the JCNSS, FTI Consulting and Clifford Chance LLP contrast the UK approach – where the NCSC publishes a "wealth of guidance" but it is "largely the responsibility of private organisation to seek it out" – with that of the US:

> Acknowledging that "partnerships between the public and private sectors that foster integrated, collaborative engagement and interaction are essential to maintaining critical infrastructure security and resilience", the Cybersecurity and Infrastructure Security Agency (CISA) have created formal partnerships to share critical threat information, inform risk mitigation strategies and share other vital information and resources. ...
>
> The proactive nature of US federal bodies' engagement with the private sector manifests itself in many forms, including CISA's regular invitations to private sector organisations to informational calls which provide detail about newly-discovered vulnerabilities and mitigation strategies, the widespread issuing of CISA Alerts regarding new exploits, and the frequent publishing of joint advisories with the FBI who regularly assist with providing intelligence around Threat Actor groups to a range of cross-sector organisations and provide post-incident support.[102]

They acknowledge that the NCSC's engagement with some sectors is relatively deep (notably financial services, as discussed in section 3.2 below) but that the agency is not resourced to "act in a proactive capacity" more widely.

---

101 Computer Weekly, UK Cyber Security Council launches certification mapping tool, 2 May 2023

102 FTI Consulting LLP and Clifford Chance LLP, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114499, 20 December 2022

## 2.4 Support for victims

The NCSC operates a Cyber Incident Response (CIR) accreditation scheme which certifies private companies that offer support to organisations targeted by cyber attacks.[103]

The CIR standards are designed to ensure that incident response service providers are capable of providing support to organisations "who are typically at risk of sophisticated and bespoke cyber attack". It is therefore primarily aimed at large organisations such as national government, critical national infrastructure, and multinational corporations.

The level of support offered to smaller organisations has been criticised. Various respondents to the JNCSS's inquiry into ransomware argued that support from the NCSC and NCA for SMEs and non-profits could be "very light touch" and that as a result they felt "lost without adequate guidance and support".[104] RUSI's written evidence states that:

> [The] UK has in effect largely privatised ransomware response for most victims – there are no 'flashing blue lights'. Instead, victims rely primarily on a mixture of private sector specialists – technical incident responders, lawyers, crisis managers and, in some cases, ransomware negotiators – to guide their response. …
>
> Micro and small businesses without cyber insurance coverage find it difficult to access or afford the right capabilities and resources during a ransomware incident. At the same it, it is not always clear to victims how the NCSC and law enforcement can provide assistance and under what conditions such help is available.
>
> Although it is reasonable and prudent for the private sector to deliver much of the response and recovery support required by victims of ransomware, the balance may have shifted too far in this direction. Micro businesses, SMEs and non-profits, in particular, should not be left to largely fend for themselves against organised cybercriminals protected by hostile states. This may require resourcing incident management capabilities within the NCSC and law enforcement at greater levels, and more frequent on-site responses or more remote advice tailored to a victim's specific needs.[105]

The NCSC says that it is working on a 'Level 2' assurance standard that will certify firms to "deliver expertise for smaller companies and organisations across the UK, including local governments."[106]

---

103 NCSC, CIR - Cyber Incident Response, 18 March 2023

104 See, for example, the written evidence submitted by FTI Consulting/Clifford Chance, JUMPSEC, RUSI, and TechUK.

105 RUSI, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114435, 16 December 2022

106 NCSC, CIR - Cyber Incident Response, 18 March 2023

## 2.5 International enforcement and collaboration

A significant portion of the cyber threat to the UK originates oversees. This includes the direct threat from hacking groups based in other jurisdictions and the indirect threat to UK interests from global supply chains being hit by cyber attacks. International collaboration is therefore key to cybersecurity policy. Cooperation in this area may, for example, be aimed at:

- Improving threat awareness;
- Identifying and sharing information about vulnerabilities;
- Understanding the tactics and motivations of attackers;
- Sharing lessons learned and developing best practice;
- Coordinating responses to cyber incidents;
- Joint law enforcement and other cyber operations.

The UK participates in various multilateral policy forums, including at the UN, International Telecommunications Union, NATO, G7, and the Financial Action Task Force (which aims to prevent global money laundering and terrorist financing). Through the NCA and NCSC, the UK is also involved in various initiatives to combat malicious cyber activity:

- The Five Eyes Cyber Crime Working Group, a law enforcement partnership between the UK, US, Canada, Australia, and New Zealand;
- The International Cyber Crime Operational Working Group, a law enforcement partnership between Five Eyes and European partners;
- The Counter Ransomware Initiative, a taskforce involving over 30 countries set up in 2021 to tackle ransomware operations;
- The Countering Illicit Finance Working Group, a group within the Counter Ransomware Initiative focused on policy responses to illicit use of cryptocurrencies, which are a primary payment method for ransomware payments.

International efforts to combat malicious cyber activity relies on collaboration with international partners. This can complicate efforts to tackle actors based in countries who are unwilling to participate. RUSI has noted that the long-term disruption of Russian-based groups has been "almost impossible to achieve" (see Box 8).[107]

The Government has acknowledged that "criminal justice outcomes … are often unrealistic". Instead, the NCA:

> uses a variety of tactics and niche capabilities to identify and disrupt offenders. This includes monitoring their travel, dismantling wider criminal networks (including those developing and deploying ransomware), tackling criminal infrastructure and marketplaces, and targeting their financial flows.[108]

## 8 International sanctions: Evil Corp

Tackling the activities of cyber criminals can be difficult if they have the implicit or explicit support of the state where they are based.

A joint operation between the NCA, FBI, and the US Office of Foreign Asset Control (OFAC) targeted Evil Corp, a Russia-based ransomware group. In December 2019, OFAC announced sanctions against Evil Corp, including its alleged leader, Maksim Yakubets.[109] The sanctions mean that anyone engaged in transactions with Evil Corp, including victims paying ransoms and companies facilitating ransom payments, could be breaking US law.

However, Evil Corp and Yakubets (who allegedly has links to Russia's intelligence services) continue to operate.[110] According to research by cybersecurity firm Mandiant, Evil Corp has recoded and rebranded its malware so that victims do not know they are violating the sanctions regime by paying ransoms.[111]

The UK Government said in written evidence to the Joint Committee on the National Security Strategy that while Evil Corp continues to operate "due to the lack of Russian state action against them, their need to continually change is nonetheless an additional cost they must bear which previously was not the case."[112]

---

107 RUSI, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114435, 16 December 2022

108 HMG, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114408, 16 December 2022, paras 72 and 88

109 US Department of the Treasury, Treasury sanctions Evil Corp, the Russia-based cybercriminal group behind Dridex malware, 5 December 2019

110 Cyber News, Kremlin's most notorious hacker: will Yakubets ever face justice?, 21 December 2022

111 NBC News, Ransomware hackers sidestep U.S. sanctions with a new trick: rebranding, 2 June 2022

112 HMG, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114408, 16 December 2022, para 87

Some countries have considered making it illegal to pay ransoms to any cyber criminal, not just those on the official sanctions list. This proposal is discussed in section 4.2 below.

## International capacity building

In 2022, cybersecurity researchers reported a growing trend of cyber criminals targeting developing and middle-income countries.[113] Incidents in the Global South included two major ransomware attacks by Russian groups Conti and HIVE on essential services in Costa Rica, which led the country's government to declare a state of emergency.[114]

According to RUSI, the increased cyber resilience of high-value targets in G7 countries along with "more forceful responses" from intelligence and law enforcement agencies may have prompted cyber criminals to look for easier targets:

> Many developing and middle-income have **historically poor levels of cyber security**, owing to low dedicated expenditure. Consequently, organisations struggle to hire and retain skilled employees and often rely on legacy computer systems which have known vulnerabilities, or have low awareness of good cyber hygiene practices.[115]

The NCS 2022 states that the increasing cyber threat to lower and middle income countries presents an opportunity for states who "do not share the UK's values" to promote their "authoritarian vision for cyberspace" as the only way to ensure cybersecurity.[116] In addition, as a result of the globalisation of supply chains, IT platforms, and the internet, cyber resilience in other countries has a direct impact on UK interests. The NCS 2022 therefore contained an objective to support countries to address cybersecurity challenges.

The main source of funding for programmes to deliver on the NCS's commitment is the FCDO's Conflict, Stability and Security Fund (CSSF). The CSSF has a 'cyber portfolio' worth £90m for 2022-25. Activities include:

- Technical assistance to help governments develop national cyber security strategies and legislation;
- Building capacity to respond to cyber incidents including by establishing national CSIRTs;

113 Deutsche Welle, Ransomware: Cyber criminals are coming for the Global South, 28 August 2022
114 Wired, Conti's attack against Costa Rica sparks a new ransomware era, 12 June 2022
115 RUSI, Ransomware now threatens the global south 12 August 2022
116 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p194

- Building cyber resilience in critical infrastructure sectors, including communications campaign to increase user-level awareness;
- Provision of threat intelligence and technical solutions;
- Building capacity of law enforcement and judiciary to detect, investigate, and prosecute cyber crime.[117]

For example, £10 million of the CSSF has been used to fund Pillar 2 of the Digital Access Programme. The programme comprises sixteen cyber capacity building projects across Brazil, Indonesia, Kenya, Nigeria, and South Africa.[118]

[117] FCDO, Conflict, Stability and Security Fund: Cyber programme summary 2021 to 2022, 19 May 2023

[118] HM Government, UK Government's Global Digital Access Programme (DAP) -Pillar 2 Trust & Resilience project summaries, 18 November 2022

# 3 Regulatory framework

The UK's regulatory framework for cybersecurity consists of a patchwork of primary and secondary legislation. This section discusses the legislation that covers the cybersecurity of IT systems, internet-connected products, and personal data.

Cybersecurity legislation is risk-based. Legal obligations are aimed at sectors and organisations where cybersecurity breaches would have a significant impact on society, the economy, or individual rights.

The obligations imposed by cybersecurity legislation are typically principles-based. They set general expectations regarding cybersecurity but do not prescribe specific measures that responsible organisations must take.

This approach provides organisations with a degree of flexibility in how they meet their cybersecurity requirements. The Government regards this flexibility as important given the rapidly changing nature of cyber threats. To support organisations, relevant government departments and regulators publish guidance tailored to specific sectors.

## 3.1 Offences: the Computer Misuse Act 1990

UK Government policy has consistently been such that what is illegal offline is also illegal online. However, the Computer Misuse Act (CMA) 1990, was passed to specifically criminalise computer-dependent activities such as hacking. Sections 1 to 3A of the Act, as amended, contain the following offences:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or facilitate commission of further offences;
- Unauthorised acts with intent to impair the operation of a computer;
- Any unauthorised acts in relation to a computer that cause or create risk of serious damage to human welfare, including by disrupting essential services.
- Making, supplying, or obtaining articles for use in offences under the CMA 1990. This would include creating malware, for example.

According to the ONS's Telephone-Operated Crime Survey for England and Wales, in the year ending March 2022 there were 1.3 million offences related to unauthorised access to personal information (including data breaches and hacking). This is double the number reported in the year to March 2020.[119]

The CMA 1990 does not provide for any defences to the offences in sections 1 to 3A. Some have called for the introduction of a statutory that would protect legitimate cybersecurity researchers who may, in the course of their work, engage in activities prohibited under the CMA 1990. This proposal is discussed in section 4.1 below.

## 3.2 Cybersecurity of critical sectors

### Network and Information Systems Regulations 2018

The Network and Information Systems (NIS) Directive (2016/1148) was the first piece of EU-wide cybersecurity legislation. It was intended to develop a more consistent and strengthened approach to cybersecurity, with a focus on the IT systems of critical sectors. The NIS Directive requires member states to:

- develop national cybersecurity capabilities, such as by having a national cyber strategy;
- collaborate with other member states on cybersecurity;
- supervise the cybersecurity of 'operators of essential services' and 'digital service providers'.

The NIS Directive designated certain sectors as involving "critical societal or economic activities": energy, transport, financial services, health, drinking water, and telecommunications infrastructure. Organisations in these sectors that meet certain threshold criteria (such as the number of customers they serve) can be designated as Operators of Essential Services (OESs). When implementing the Directive, the UK Government chose to exempt financial services because it considered that the existing cybersecurity requirements imposed by the Financial Conduct Authority were equivalent.

In addition, the Directive identified three types of digital service providers (DSPs) with responsibilities under the legislation: providers of online marketplaces, online search engines, and cloud computing services.

The UK implemented the NIS Directive through the Network and Information Systems Regulations 2018. The NIS Regulations remain in force after Brexit, although they have been amended to reflect the fact that the UK is no longer

[119] ONS, Nature of fraud and computer misuse in England and Wales: year ending March 2022, 26 September 2022

a member state. The NIS Regulations impose duties on OESs and DSPs. Duties include:

- taking appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems;
- taking appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems;
- notifying the relevant Competent Authority about any incident which has a substantial impact on their services;
- meeting the inspection requirements under the NIS Regulations; and
- complying with information, enforcement, and penalty notices.

The Regulations themselves do not specify the actions that OESs and DSPs should take to ensure cybersecurity risks are 'appropriately and proportionately' managed. Instead, each critical sector has a designated 'competent authority' responsible for publishing technical cybersecurity guidance and monitoring implementation.[120] For OESs, oversight is proactive, meaning that competent authorities should:

> engage with industry, publish guidance, meet with representatives from OESs, and implement an assessment framework including an audit programme.[121]

DSPs, by contrast, are subject to post-incident oversight only.

### Reviews of the NIS Regulations

The Government has conducted two post-implementation reviews (PIRs) of the NIS Regulations, published in 2020 and 2022. The 2022 PIR found that, overall, the Regulations "are having a positive impact and that they are effective in driving behaviour". It noted that a lack of cybersecurity skills within regulated industries was a key constraint in terms of implementation.[122]

The PIR 2022 identified a number of areas for improving the NIS Regulations, including around supply chain risks and incident reporting duties. The Government's proposals for strengthening the NIS Regulations are discussed in section 4.2 below.

## Telecommunications sector

Providers of public telecommunications networks and services are under additional legal obligations. These are contained in the Communications Act

120 For example, Ofgem publishes guidance for Operators of Essential Services in the energy sector.

121 DSIT, NIS Regulations: Guidance for Competent Authorities, 20 April 2018, p6

122 DCMS, Second Post-Implementation Review of the Network and Information Systems Regulations 2018, 4 July 2022

2003 ss105A-105Z29, as amended by the Telecommunications (Security) Act 2021. The enhanced cybersecurity requirements for the sector followed the Government's telecoms supply chain review. During the review the NCSC highlighted identified four key risks associated with telecoms networks, including dependence on equipment supplied by 'high risk' vendors.[123]

The 2021 Act, and the associated regulations and code of practice, impose legally binding minimum security requirements on telecoms providers.[124] The requirements are more specific than for other sectors. Under regulation 5 of the Electronic Communications (Security Measures) Regulations 2022, for example, tools that providers use to monitor the operation of their network must not be located in or accessible from Russia, China, Iran, or North Korea.

Further information on the 2021 Act can be found in the Library's briefing on the Telecommunications (Security) Bill.

## Financial services

As noted above, financial services firms are exempted from the NIS Regulations. Instead, cybersecurity in the financial services sector is regulated by the Financial Conduct Authority (FCA) and the Bank of England's Prudential Regulation Authority (PRA) in line with their statutory duties to tackle financial crime and to protect the integrity of the UK financial system.

High level cybersecurity principles and guidance are set out in the FCA's Principles for Businesses and its financial crime rules. Neither specifically covers cybersecurity but are interpreted by the FCA to include it. For example, Principle 11 requires firms to disclose anything to the FCA that the regulator would reasonably expect be notified about. This includes 'material cyber incidents'.[125]

Since 2017 the FCA has convened quarterly Cyber Coordination Groups with the industry, NCSC, NCA, HM Treasury, and the Bank of England to discuss common cyber risks and best practice. The FCA publishes an overview of the discussions.[126]

Regulated firms are also required to participate in a penetration testing regime developed by the FCA, PRA, and HM Treasury called CBEST. It involves a simulated cyber attack based on current cyber threats in which an accredited penetration test company attempts to reach the point where they could steal, manipulate, or encrypt important data. CBEST is designed to test the firm's cybersecurity defences, assess its level of threat intelligence, and assess its ability to detect and respond to external and internal cyber attackers.[127] In addition, in 2022 the Bank of England ran its first, voluntary,

123 DCMS, Telecoms supply chain review, 8 November 2018, p24-26

124 DSIT, Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice, 1 December 2022

125 FCA, Good cyber security – the foundations, accessed 23 May 2023

126 See for example, FCA, Insights from the 2021 Cyber Coordination Groups, 8 December 2022

127 Bank of England, Operational resilience of the financial sector, accessed 23 May 2023

'cyber stress test' which tested participating firms' resilience to a successful attack.[128]

## 3.3 Cybersecurity of connected products and services

As set out in the NCS 2022, the Government's approach to the cybersecurity of connected products is to ensure, where possible, that they are 'secure by design'. Where this is not possible – due to the global nature of supply chains, for example – the Government says that it will "implement robust measures to mitigate risk, including domestic regulation and international collaboration on standards".[129]

### Secure by design

A system that is 'secure by design' is one that has been designed from the ground up to be secure against cyber threats. In March 2018, the Government published a report on this principle, arguing that a new approach was needed to shift the burden of cybersecurity from consumers to manufacturers.[130] The report noted the opportunities offered by increased use of consumer connectable products but highlighted their lack of security provision. The report set out two risks associated with this:

- Risks to the privacy and safety of consumers; and
- the wider threat of large cyber attacks.

The report argued that the UK Government had "a duty of care to UK citizens to help ensure that they can access and use the internet safely." It called for greater action in the area and said there was "a need to move away from placing the burden on consumers to securely configure their devices and instead ensure that strong security is built in by design."[131]

A Code of Practice for Consumer IoT Security, developed through engagement with industry, was published alongside the report. It provided 13 guidelines for manufacturers and others, setting out good practice for ensuring that connectable products were secure. These guidelines included:

- Ensuring that consumer connectable products do not have universal default passwords when they are sold;

128 Bank of England, Thematic findings from the 2022 cyber stress test, 29 March 2023
129 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p86
130 DCMS, Secure by Design report, March 2018
131 DCMS, Secure by Design report, March 2018, p4

- Ensuring the period of time for which the security on products will be updated is made clear to the consumer; and that

- Manufacturers and others should implement a vulnerability disclosure policy to ensure that security vulnerabilities are monitored, identified, rectified and reported to stakeholders.[132]

At the time of the publication of the Secure by Design report, the Government said that its preference would be for "the market to solve this problem" but if this did not happen, it would look to introduce these measures through legislation.

## Product Security and Telecommunications Infrastructure Act 2022

In May 2019, the Government published a consultation on introducing a regulatory approach to connectable products' security.[133] In the consultation document, the Government said that self-regulation had "not worked." It noted that there was a lack of information for consumers on the security of connected products and a lack of incentive for industry to provide this information to consumers.

Regulation was identified by the Government as the "best lever available to influence industry to meet these requirements"; one that would "force out the very worst practice we are seeing in the market."

The Government published its response to the consultation in February 2020.[134] This said that the Government intended to give the Secretary of State powers to introduce security requirements for devices on sale in the UK. The consultation had proposed making the Code of Practice for Consumer IoT Security mandatory. However, the Government acknowledged stakeholder feedback that this would place a heavy regulatory burden on the industry.

It said that after assessing the balance between protecting consumers and minimising the burden on industry, it concluded the top three guidelines from the Code of Practice should be the focus. These were that:

1. IoT device passwords must be unique and not resettable to any universal factory setting;

2. Manufacturers of IoT devices need to provide a vulnerability disclosure policy on how concerns about security can be reported;

132 DCMS, Code of Practice for Consumer IoT Security, March 2018

133 DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, February 2020

134 DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, February 2020

3. Manufacturers of IoT devices need to explicitly state the minimum length of time that the product will receive security updates.[135]

The response said that these requirements were easier to test from an enforcement perspective and that meeting these would give consumers protection.

The Government took powers to make cybersecurity regulations for connected products through the Product Security and Telecommunications Infrastructure Act 2022. Further information can be found in the Library's briefing on the Act. The regulations themselves have not yet been made.

### Other types of products and services

Besides the general requirements to be introduced under the PSTI Act 2022, certain types of products are (or will be) subject to more specific cybersecurity standards. Electric vehicle charge points, for example, must comply with the Electric Vehicles (Smart Charge Points) Regulations 2021. Schedule 1 sets basic security standards, including a requirement for charge points to have unique passwords and the ability to automatically check for security updates.

The Energy Bill 2022-23 would grant the Government powers to mandate cybersecurity standards for what it calls 'energy smart appliances', including heat pumps and electric vehicles. Further information can be found in the section 3 of Library briefing, Energy Bill [HL] 2022-23, parts 7-10.

In addition to regulation the Government has published guidance and voluntary codes of practice aimed at improving cybersecurity standards in various contexts. For example, the code of practice for app store operators and app developers sets out eight principles for protecting users' security and privacy.[136] It includes commitments relating to app design (such as not requesting permissions and privileges that are not required for the app to function) and processes (such as having a vulnerability disclosure policy).

## 3.4 Cybersecurity of personal data

Business, public bodies, and other organisations that collect, store, and process personal data are required to comply with data protection law. This will be the main source of statutory cybersecurity obligations for most organisation that are not covered by the NIS Regulations, PSTI Act, or other sector-specific regulation described above.

[135] DCMS, Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, February 2020

[136] DCMS, New rules for apps to boost consumer security and privacy, 9 December 2022

The UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 set out six principles for the collection and use of personal data. The sixth principles concerns security and requires that personal data is processed in a way that:

> ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[137]

The legislation does not specify which cybersecurity measures an organisation should have in place. Measures should be appropriate to the organisation and its activities:

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.[138]

Further information on the cybersecurity elements of data protection law can be found in the Information Commissioner's Office's guide to the General Data Protection Regulation and the NCSC's guidance on GDPR security outcomes.

A 2020 review of the impact of the GDPR on cybersecurity, commissioned by DCMS, found that "most organisations had improved their cybersecurity when measured against the National Cyber Security Centre (NCSC) security outcomes".[139] 82% of organisations said that changes in their cybersecurity could be attributed to the introduction of data protection laws "at least to a small extent". However, the review found that a large minority of organisations (36%) felt that GDPR had resulted in an "excessive" focus on data protection, to the detriment of other aspects of cybersecurity.[140]

137 UK GDPR, Article 5(1)(f)

138 UK GDPR, Article 32

139 RSM Consulting, Impact of the GDPR on cyber security outcomes: final report, August 2020, p2

140 RSM Consulting, Impact of the GDPR on cyber security outcomes: final report, August 2020, p70-72

# 4 Proposals for regulatory reform

This section discusses some proposals for reforming cybersecurity law. It starts by looking at two key points of debate among cybersecurity stakeholders: the degree to which 'ethical hackers', legitimate cybersecurity researchers who use illegitimate hacking techniques, should be protected from prosecution; and whether ransomware payments should be prohibited.

It then turns to three proposals upon which the UK Government has consulted: strengthening the NIS Regulations, introducing a cyber duty to protect, and reforming corporate responsibility rules.

Finally, it ends with a discussion of Russia's proposal at the UN for a new international cybercrime treaty.

## 4.1 'Ethical hacking'

Criminal hackers and cybersecurity professionals working for vendors and users of IT systems will typically use the same hacking techniques and tools. In legal terms, the difference is that the activities of in-house cybersecurity teams are authorised by the IT system's owner.

Between these two groups there is a large community of independent cybersecurity researchers, sometimes called 'ethical hackers'. Like in-house teams they look for vulnerabilities with the intent of improving the security of the system they are testing. However, like malicious actors they often operate without authorisation from the system's owner. The Electronic Frontier Foundation (EFF) a non-profit organisation that campaigns for civil liberties in the digital world, explains how this leaves security researchers vulnerable to prosecution under anti-hacking legislation:

> Almost by its nature, discovering security vulnerabilities requires accessing computers in a manner unanticipated by computer owners, frequently in contravention of the owners' stated policies. The work involves trial and error, as researchers look for vulnerabilities in complex systems. Sometimes researchers employ a chain of techniques that seek to leverage one basic flaw to discover more serious vulnerabilities or demonstrate access to more sensitive data, and often it is the initial stages of their work that involves forms of "access" of uncertain legality.[141]

[141] Electronic Frontier Foundation, Amicus brief in support of petitioner in Van Buren v United States, August 2020, p19

The CMA 1990 does not include any defences to the computer-related offences it created.[142] One protection against prosecution is the guidance published by the Crown Prosecution Service (CPS), updated in February 2020.[143] The guidance states that the following factors should be taken into account when deciding whether it is in the public interest to bring a prosecution under the CMA 1990:

- The financial, reputational, or commercial damage caused to the victim(s);
- The offence was committed with the main purpose of financial gain;
- The level of sophistication used, particularly sophistication used to conceal or disguise identity (including masquerading as another identity to divert suspicion);
- The victim of the offence was vulnerable and has been put in considerable fear or suffered personal attack, damage or disturbance;
- The mental health, maturity and chronological age of the defendant at the time of the offence.

Campaign group CyberUp has argued that this does not provide sufficient protection for legitimate cybersecurity research. They have called on the Government to amend the CMA 1990 to introduce an explicit public interest defence. Which?, the consumer charity, has similarly called for a defence for researchers where their actions "can be proven to be in the fair public interest of raising concern over a clear risk to civil society that the company has failed to act on".[144]

## Risks and benefits of reforming the CMA 1990

According to the EFF, writing in support of a researcher facing legal action in the United States, the benefits provided by independent security researchers are widely recognised:

> Decades of experience have shown that independent auditing and testing of computers by members of the security research community—often in a manner unanticipated and even disapproved by the computers' owners—is particularly effective at discovering serious vulnerabilities in widely used software and devices. Just as the drafter of a legal brief can overlook even the most glaring typo, the original developers of software may simply miss their own errors, which can be more apparent to outsiders. For similar reasons, existing products that gain wider adoption are exposed to new use cases and more attention from researchers, leading to the discovery of new flaws … In

142 For background information on why the CMA 1990 criminalises all unauthorised hacking see Audrey Guinchard, Transforming the Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime, Journal of Information Rights Policy and Practice 2(2), March 2018, p20-24

143 CPS, Computer Misuse Act, updated 5 February 2020

144 Which?, Response to Computer Misuse Act 1990: Call for Information, 8 June 2021

> addition, independent researchers may be able to develop specialized techniques to uncover flaws.[145]

An article reviewing the academic literature concludes that independent security researchers "play an integral part" in the "race against criminal hackers" by providing a cost-effective source of additional perspectives and skills, and by generally contributing to a culture of openness about the security of digital products.[146]

However, ENISA, the European cybersecurity agency, notes that the threat of prosecution can have a "chilling effect" on cyber researchers which "adversely affects security". Similar language has been used by the former head of the UK's National Cyber Security Centre.[147] According to a survey by CyberUp, a group campaigning to reform the CMA 1990, around 80% of cybersecurity professionals in the UK have worried about breaking the law during their work. 40% of organisations said that this has inhibited them from preventing harm to a business or individual, and 20% said it had inhibited them from preventing a threat to national security. [148]

Government cybersecurity agencies and international cybersecurity standards consistently advise that developers and owners of IT systems adopt policies that encourage independent researchers to report security vulnerabilities.[149] The UK's National Cyber Security Centre (NCSC) states that reports provided by independent researchers can provide organisations with "valuable information that [they] can use to improve the security of [their] systems". [150]

Voluntary disclosure policies give security researchers some reassurance that they will not be prosecuted for their actions. However, researchers can still face legal action because organisations can choose to change, ignore, or disapply their disclosure policies.[151] If that happens there are no statutory defences under the CMA 1990 based on the intent of the actor. CyberUp argues that security researchers need the legal certainty and clarity that a statutory defence would provide.[152]

---

145 Electronic Frontier Foundation, Amicus brief in support of petitioner in Van Buren v United States, August 2020, p9

146 Audrey Guinchard, Transforming the Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime, Journal of Information Rights Policy and Practice 2(2), March 2018, p7-9

147 CyberUp, UK cyber laws 'out of date', former cyber chief warns, 15 March 2022

148 CyberUp, Time for reform? Understanding the UK cyber security industry's views of the Computer Misuse Act, November 2020

149 For example ETSI EN 303 645 Cyber security for consumer Internet of Things, June 2020, section 5.2

150 NCSC, Vulnerability disclosure toolkit, 14 September 2020

151 Real-world examples are discussed in CyberUp, Submission to the Product Security and Telecommunications Infrastructure Bill Committee, accessed 21 March 2023; and Audrey Guinchard, Transforming the Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime, Journal of Information Rights Policy and Practice 2(2), March 2018, p14-16

152 CyberUp, Protecting legitimate cyber security activity, October 2021

Introducing such an exemption is complicated by the following risks:

- **Risk of abuse** – The primary concern is that an exemption for security research activity could be used as cover for malicious or offensive cyber activities. It is difficult to distinguish ethical and malicious hacking activities except in hindsight by reference to the intent of the actor. Malicious actors caught in the early stages of an attack could, in principle, claim that they were just conducting research. Similarly, information obtained while conducting supposedly ethical hacking activities could be used for malicious purposes.

- **Risk of harm** – The methods and tools used by ethical hackers are similar to those used by malicious hackers and can therefore cause harm, for example in the form of confidential data being compromised or systems becoming inoperable. ENISA notes concerns that decriminalisation could over-incentivise security research, which could increase the risk of harm being caused by less-skilled security researchers or by researchers using more harmful techniques. It could also cause harm indirectly if vendors misallocate scarce resources to a) deal with ethical hacking activities that are initially indistinguishable from malicious cyber attacks, and b) fix a large number of minor vulnerabilities rather than focusing on critical ones.[153]

- **Rights and responsibilities of system owners** – In April 2022, the Government said in response to a Westminster Hall debate on the CMA 1990 that it was right for the law to protect system owners from unauthorised access, particularly given their legal responsibilities regarding cyber and data security: "We encourage firms to agree to having their systems tested for vulnerabilities by third parties but the fundamental point is that it is the choice of the legal property owner to determine that".[154] This approach gives vendors more control how vulnerabilities are discovered and disclosed. ENISA notes that vendors tend to prefer 'coordinated' disclosure where they have the opportunity to verify the vulnerability and work on a fix before it is made public by the discoverer.[155]

CyberUp argues that these issues can be mitigated by an appropriately-worded defence alongside industry standards for cyber researchers, and that with mitigations in place the benefits of supporting ethical hacking outweighs the risks. It has proposed a public interest defence which would apply where the following principles are met:

- The (prospective) benefits of the act outweigh the (prospective) harms, including where the action caused harm that was necessary to prevent greater harm;

153 ENISA, Good Practice Guide on Vulnerability Disclosure, para 4.2.7

154 HC Deb 19 April 2022 vol 712 c18WH

155 ENISA, Good Practice Guide on Vulnerability Disclosure, para 2.5.1

- Reasonable steps were taken to minimise the risk of causing harm;
- The actor demonstrably acted in good faith, honestly, and sincerely;
- The actor is able to demonstrate their competence, expertise, and general capacity to act in a way that minimises the risk of harm.[156]

Based on consultation with industry professionals it has published a report outlining the types of cyber research activity that it believes ought to be legitimate under a reformed CMA.[157]

The group is also arguing that the CMA 1990's definition of 'unauthorised access' should be amended to exempt activities that the system owner would have reasonably consented to had they been aware of the actor's motivations. These proposals are discussed in detail in a report by the Criminal Law Reform Now Network (CLRNN) and CyberUp's response to the Home Office's May 2021 call for information on the CMA 1990.[158]

## UK Government policy

The Home Office announced a review of the CMA 1990 in May 2021 and issued a call for information.[159] It primarily sought views on the offences and enforcement powers contained in the CMA 1990 and whether they adequately cover all forms of cyber-dependent crime. However, respondents were also asked whether they thought legitimate cyber security activity was adequately protected by the Act.

The Government confirmed in a debate on the Product Security and Telecommunications Infrastructure Bill in October 2022 that it was "listening to and considering concerns that the Computer Misuse Act is constraining activity that would enhance the UK's cybersecurity":

> We understand that if you want to test cybersecurity you have to be able to test its breaking point. We are trying to strike the right balance between providing suitable reassurances for well-meaning individuals who want to identify vulnerabilities and not allowing malicious actors to access devices without consent. There are risks here. It is very nuanced, and the Government do not want to rush into legislative change without clear evidence to justify any such change to existing law.[160]

A response to the call for information was published in February 2023. It said that further work was needed to consider the risks and benefits of introducing statutory defences for legitimate cyber activity:

156 CyberUp, Protecting legitimate cyber security activity, October 2021
157 CyberUp, Legitimate cyber security activities in the 21st Century, 15 August 2022
158 CLRNN, Reforming the Computer Misuse Act 1990, January 2020, paras 5.1-5.30; CyberUp, Call for Information response, updated 18 November 2021, questions 7-9
159 Home Office, Computer Misuse Act 1990: call for information, 11 May 2021
160 HL Deb 12 October 2022 vol 824 c794

> the Government believes that we need to consider whether and what defences, including both legislative and non-legislative solutions, should be introduced in the context of how the cyber security industry can be supported and developed to help protect the UK in cyberspace. As part of that work we need to consider what activity that may conflict with the CMA is legitimate for cyber security companies to undertake, and what standards and training cyber security professionals must have in order to be qualified to undertake such activity. We will take this work forward as part of the wider work to improve our national cyber security.[161]

Separately, in the Autumn Statement 2022 the Government announced a series of reviews into the regulation of emerging technologies. The first report, covering digital technologies, was published alongside the Government's response in March 2023. The review, led by Sir Patrick Vallance, recommended:

> amending the Computer Misuse Act 1990 to include a statutory public interest defence that would provide stronger legal protections for cyber security researchers and professionals, and would have a catalytic effect on innovation in a sector with considerable growth potential.[162]

The Government's response points to the Home Office's existing programme of work looking at the benefits and risks of reform.[163]

## 4.2 Should ransomware payments be banned?

One of the law enforcement tools available to governments tackling oversees cyber criminal groups is the sanctions regime. The Cyber (Sanctions) (EU Exit) Regulations 2020 grant the Government powers to impose asset freezes on designated persons. Under the Regulations, it is an offence to make funds available to persons subject to an asset freeze, including through ransom payments.[164] The aim of the regime is to discourage the payment of ransoms, thereby cutting off a key source of income for cyber criminals.

Some countries, including Australia and the United States, have considered going further by banning all ransom payments. Media reports state that the policy is being considered as part of the International Counter Ransomware Initiative, of which the UK is a member.[165]

---

161 Home Office, Review of the Computer Misuse Act 1990: consultation and response to call for information, 7 February 2023

162 HM Treasury, Pro-innovation Regulation of Technologies Review: digital technologies, 15 March 2023, p13

163 HM Treasury, HM Government response to Sir Patrick Vallance's Pro-Innovation Regulation of Technologies Review, 15 March 2023, p9

164 Office of Financial Sanctions Implementation, Ransomware and sanctions, February 2023

165 Cybersecurity Dive, White House considers ban on ransom payments, with caveats, 8 May 2023; Coin Telegraph, Push to ban ransomware payments following Australia's biggest cyberattack, 12 April 2023

A ban, as suggested by US deputy national security advisor for cyber Anne Neuberger, could include a waiver covering cases where, for example, a ransomware attack is preventing the delivery of critical services.[166] Proponents say that ransomware is a financially motivated crime, so "less payments equals less ransomware".[167] They argue that businesses may regard paying ransoms as the "easy way out", especially if it is covered by insurance. Paying off cyber criminals may be the rational response for an individual firm, but it is argued to be collectively irrational because it encourages further attacks.[168]

Critics of the proposal argue that banning ransom payments would criminalise victims, including those who have invested in appropriate cybersecurity measures.[169] They also point out that threat actors would adapt to new laws. For example, attacks could become more aggressive to force organisations to pay ransoms despite the legal consequences, or threat actors could stop publicly announcing breaches and deal with victims directly.[170] In Italy, where paying extortionists is illegal under existing anti-kidnapping laws, 43% of organisations still admit to paying off ransomware groups, according to a survey by Sophos.[171]

A direct consequence of a ban, according to the Brookings Institute, would be to push the activities of ransomware groups further underground, making them harder to track and understand.[172]

Finally, an article in Infosecurity Magazine argues than banning ransom payments would discourage organisations from taking out cyber insurance, which can be used to cover the financial impact of a cyber attack.[173] The Association of British Insurers and the International Underwriting Association have advised against a ban, which they say "is likely to have an adverse effect" on businesses unable to access insurance cover.[174] While insurance providers have been criticised for facilitating payments, RUSI has argued that the cyber insurance industry is a potential source for incentivising better cybersecurity practices.[175]

166 Cybersecurity Dive, White House considers ban on ransom payments, with caveats, 8 May 2023
167 Brett Callow, threat analyst at cyber firm Emisoft, quoted in Cybersecurity Dive, White House considers ban on ransom payments, with caveats, 8 May 2023
168 Telemachus, Is it time to ban ransomware payments?, 16 February 2021; Brookings Institute, Should ransomware payments be banned?, 26 July 2021
169 Brookings Institute, Should ransomware payments be banned?, 26 July 2021
170 Forbes, Banning ransomware payments could create new crisis situations, 8 June 2021
171 Sophos, The state of ransomware 2022, April 2022, p4. By comparison, a separate survey found that 63% of UK victims paid ransoms: Hiscox, Cyber readiness report 2022, April 2022, p5
172 Brookings Institute, Should ransomware payments be banned?, 26 July 2021
173 Infosecurity Magazine, Should we make ransomware payments illegal?, 24 February 2023
174 ABI and IUA, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114418, 16 December 2022, para 24
175 RUSI, Cyber insurance and the cyber security challenge, 28 June 2021

### UK Government policy

Summarising a G7 meeting on ransomware, the Home Office stated that while it was important to reduce ransom payments in order to disrupt the criminal business model, "we must ensure that we are careful not to inadvertently re-victimise the victim".[176] Anonymous sources told The Record that in 2021 the Home Office led a government-side 'sprint' to improve understanding of ransomware and decided that it would not prohibit ransom payments.[177]

The Office of Financial Sanctions Implementation's guidance states that:

> Ransomware payments to criminal actors perpetuate the threat and sustain the criminal marketplace. Payment of a ransom further encourages the targeting of UK business and does not remove criminal actors' access to networks leaving them open to future attacks. This has a negative impact on UK national security and the economy and further encourages the targeting of UK individuals and entities.
>
> The payment of a ransom does not guarantee a victim will regain access to their data or computer and increases the likelihood they will be targeted in the future.

The NCSC and ICO similarly do not "encourage, endorse nor condone the payment of ransoms".[178]

## 4.3 Strengthening the NIS Regulations

The Government published a consultation on reforming the Network and Information Systems (NIS) Regulations in January 2022. According to the Government, the proposals are intended to address "the evolving cyber security threats the UK faces".[179] Its response was published in November that year.

The main proposals, which the Government said it will take forward once a "suitable legislative vehicle" is found, are to:

- Bring managed service providers, additional critical sectors, and organisations upon whom critical sectors are dependent into the scope of the NIS Regulations;
- Introduce a more proactive supervisory regime for the most critical digital service providers;

176 Home Office, Chair's summary from the G7 Interior and Security Senior Officials' Extraordinary Forum on Ransomware on 15 and 16 December 2021, 24 December 2021

177 The Record, Ransomware incidents now make up majority of British government's crisis management 'Cobra' meetings, 18 November 2022

178 ICO and NCSC, ICO and NCSC stand together against ransomware payments being made, 8 July 2022

179 DMCS, Proposal for legislation to improve the UK's cyber resilience, 19 January 2022

- Expand incident reporting duties to include incidents that do not directly affect service continuity.

## Expanding the scope

A key focus of the proposed reforms is resilience to supply chain attacks. As discussed above, supply chain attacks are a form of cybersecurity threat that has risen to prominence in recent years. In a supply chain attack, threat actors target third parties with access to an organisation's IT systems, rather than the organisation itself. The consultation proposed imposing cybersecurity responsibilities on third party providers of certain business-to-business IT services, called a managed service provider (MSP).

Following the consultation the Government defined an MSP as a third party that provides a service to another organisation, where the service:

- Is related to the provision of IT services; and
- Is reliant on the use of network and information systems; and
- Provides regular and ongoing management support, active administration, and/or monitoring of IT systems.

The response clarified that non-IT services, such as outsourced HR or payroll services, would not be in scope. Service providers who have access to IT systems on an ad hoc basis, such as consultants, are also not in scope. In line with the existing NIS Regulations, small and micro businesses are exempt, although the Government said that the ICO will be able to designate such entities as in scope if they are deemed "systemically critical".

MSPs would have the same duties under the NIS Regulations as digital service providers (DSPs).

Besides MSPs, the consultation considered two other expansions to the scope of the regulations:

- Additional critical sectors and sub-sectors. The consultation noted that the scope of the NIS Regulations is limited to those sectors and sub-sectors that were deemed critical in 2016, when the EU Directive was finalised, and 2018, when it was transposed into UK law. It argued that with increasing digitalisation additional critical sectors could become vulnerable to cybersecurity threats, including education, manufacturing, and waste water. Various energy sub-sectors related to decarbonisation, such as heat pumps and electric vehicles, were also mentioned.
- Critical sectoral dependencies. The consultation argued that organisations in critical NIS sectors may be dependent on third party services, without which they could not operate. This would include specified outsourced services that are not currently in scope of the NIS Regulations and that would also not be captured by the definition of MSPs.

The Government is not currently proposing to add these sectors to the NIS Regulations. Rather, it is proposing to take powers that would allow it to amend the NIS Regulations through secondary legislation, including adding to their scope.

Separately the EU is implementing a similar expansion to the scope of the NIS Directive to include ICT services and systems in the supply chains of essential services. The new NIS2 Directive will bring sectors such as medical devices manufacturing, waste management, communications providers, food, and public administration into scope.

## Supervisory regime for digital service providers

As noted above, DSPs are currently subject to reactive (ex post) supervision. The consultation proposed implementing a two-tier regime, with the most critical DSPs becoming subject to proactive (ex ante) supervision, meaning that they would be required to proactively demonstrate their compliance with the NIS Regulations. Other DSPs would remain under ex post supervision.

In its response, the Government noted concerns from stakeholders that defining appropriate criteria for a two-tier regime would be problematic. Instead, it said it was considering a more flexible, risk-based approach. This would involve the Information Commissioner identifying the DSPs "which play the most critical role in supporting the resilience of the UK's essential services" and supervising them accordingly.

## Incident reporting duties

At present, organisations covered by the NIS Regulations are required to report all incidents that affect the continuity of the service they provide. Incidents that do not affect service continuity do no need to be reported. This would include, for example, unsuccessful attacks or attacks where personal, rather than business-critical, files were affected. The Government argued in the consultation document that such breaches could leave organisations open to follow-up attacks. Reporting how the breach took place would also allow regulators and other organisations to prepare for similar attacks in the future.

The consultation proposed a new reporting duty covering any incident which:

> has a significant impact on the availability, integrity, or confidentiality of networks and information systems, and that could cause, or threaten to cause, substantial disruption to the service.

The Government said that it would work with stakeholders to clarify the new threshold before introducing it.

## 4.4 A 'Cyber Duty to Protect'?

In the National Cyber Strategy 2022 the Government said that it would remove as much of the cybersecurity burden as possible from individual civilians by "placing more responsibility on manufacturers, retailers, service providers and the public sector to raise cyber security standards".[180] One of the strategy's objectives was to ensure that UK businesses and organisations are better able to understand and address the cyber risks to their customers, "including how the data they hold could be used to facilitate crimes like fraud, identity theft or extortion".[181]

As part of this approach, the Home Office published a call for information in September 2022 asking for views on possible measures to "reduce the burden of cyber security on citizens and reduce harms to citizens from unauthorised access [to online accounts] and associated harms".

The call for views did not contain firm policy proposals. However, it suggests in general terms that relevant organisations could be subject to a 'cyber duty to protect' their customers:

> The Home Office believes cyber crime, and the offences facilitated by it, could be substantially reduced via more widespread implementation of secure-by-default principles to protect user accounts and their personal information.
>
> The Home Office also intends to explore options to ensure that providers of online services and accounts, as well as processors and holders of UK citizens' personal data, exercise an appropriate and proportionate degree of responsibility for the protection required of the data, and access to it. This would mean exploring supplementing the current approach to the protection of data, under the Data Protection Act and GDPR, with a greater understanding and consideration of the risk to individuals of the compromise of their data held by organisations.[182]

'Secure by default' refers to the principle that the default settings should be the most secure. Responding to the call for information, consumer charity Which? pointed to research suggesting that there is a gap between the number of people who are aware of cybersecurity measures and the number who actually take protective actions.[183] For example, its survey found that half of respondents were aware of two-factor authentication but only a fifth had enabled it for their main email account.

Which? welcomed the principle of shifting the burden of protecting consumers from computer misuse to businesses. It acknowledged that there could be a

---

180 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p35

181 Cabinet Office, National Cyber Strategy 2022, 15 December 2021, p69

182 Home Office, Call for information: Unauthorised access to online accounts and personal data, 1 September 2022, paras 19-20

183 Which?, Response to the Home Office's' Call for information: Unauthorised access to online accounts and personal data', October 2022, p3

financial impact on SMEs for meeting any new requirements, but said that the Government should support rather than exempt them.[184]

## 4.5 Corporate governance and accountability

The RIR 2022 was critical of large organisations' transparency about the cyber risks they face. It pointed to research into the annual reports published by FTSE 100 companies which found that the majority made either no mention of cyber risk (13%) or included only 'simple' references to it (48%). The Cyber Breaches Survey 2021 similarly suggested a lack of transparency and board engagement: only 37% of businesses reported their most serious cyber incident externally, and 50% did not regularly report to senior managers about cyber risks.

As part of wider reforms to the corporate governance and audit regime, the Government has proposed to introduce a new statutory Resilience Statement for Public Interest Entities. The Resilience Statement would require directors to report on matters that are a "material challenge to resilience", including;

> The company's ability to manage digital security risk, including cyber security threats and the risk of significant breaches of its data protection obligations.[185]

The requirement would apply to companies with both 750 or more employees and an annual turnover of £750 million or more.

The Government set out the benefits in terms of cybersecurity in the RIR 2022:

> The collective cyber resilience of the largest UK companies is of greatest importance to the resilience of the UK economy and to individuals. … As part of wider reforms of corporate governance and reporting, we aim to drive greater accountability for and transparency of organisations' cyber resilience. This would support higher standards, provide greater protection to individuals and organisations and drive further investment in improving organisation's cyber resilience. It will also encourage shareholders to hold their Boards and executives to account for cyber security.

According to the Government's response to the consultation there was broad support for the proposals for a Resilience Statement. The Institute of Chartered Accountants (ICAEW) says that it is widely acknowledged that the existing Going Concern and Viability Statements, which the Resilience Statement will replace, often lack sufficient detail to explain how a company could deal with business shocks, including from cyber incidents.[186]

Legislation to enact the proposals has not yet been introduced.

---

184 Which?, Response to the Home Office's' Call for information: Unauthorised access to online accounts and personal data', October 2022, p3

185 BEIS, Restoring trust in audit and corporate governance: government response, May 2022, p51

186 ICAEW, The Resilience Statement – everything you need to know, 27 July 2022

## 4.6 UN cybercrime treaty

The 2001 Budapest Convention was the first multilateral treaty for combating cybercrime. Drawn up by the Council of Europe, it sought to harmonise domestic cyber legislation and create a framework for cooperation between states. 68 states are parties to the Convention, including the UK and a number of non-Council of Europe states such as the US, Canada, and Japan. Russia is not a signatory, despite being part of the Council of Europe.

In December 2019 the UN General Assembly adopted a resolution to begin negotiations for a new international treaty on cybercrime.[187] The resolution was proposed by Russia, with the support of countries including China, Iran, and North Korea.

The UN's Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes first met for negotiations in February 2022. Its concluding session is expected to end on 9 February 2024.

The proposed treaty put forward by Russia has been criticised by civil society groups.[188] ARTICLE 19, an international human rights group, highlighted in its submission to the Ad Hoc Committee the large number of offences in the negotiating document (34 compared to the Budapest Convention's 9). They include content-based offences such as sharing material that incites 'sedition'.[189]

ARTICLE 19, the Electronic Frontier Foundation, and Human Rights Watch argue that the wording of many of the offences is "vague and open to abuse" by governments seeking to suppress freedom of expression.[190] The Lowy Institute has linked the treaty to Russia's broader efforts to strengthen state control over the internet, noting that the content-based offences in the treaty would give governments "the freedom to designate anything online as a cybercrime".[191]

The UN's Human Rights Office argued in its submission that the treaty should focus on cyber-specific crimes (such as unlawful access to data and systems)

187 AP News, UN gives green light to draft treaty to combat cybercrime, 28 December 2019

188 Association for Progressive Communications, Proposed international convention on cybercrime poses a threat to human rights online, updated 28 April 2023

189 Article 19, Comments on the Consolidated Negotiating Document, January 2023

190 Human Rights Watch, Cybercrime is dangerous, but a new UN treaty could be worse for rights, 13 August 2021; Electronic Frontier Foundation, Speech-related offences should be excluded from the proposed UN cybercrime treaty, 6 June 2022

191 Lowy Institute, The hypocrisy of Russia's push for a new global cybercrime treaty, 7 March 2022

rather than content-based offences, which it says have been used to restrict free speech.[192]

However, an article by Chatham House cautions that developing countries stand to lose out if states cannot reach an agreement on the scope of the treaty:

> Most developed countries have systems, resources, expertise and capabilities in place which enable them to tackle cybercrime. Western countries, for example, have a long history of working on cybercrime issues nationally but also regionally and internationally. They are state parties to the Budapest Convention and have good cooperation mechanisms within regional bodies such as Europol.
>
> However, the same cannot be said about developing countries. As some delegations have highlighted during the negotiations, often international cooperation on cybercrime does not fail due to lack of will but rather lack of capacity. ...
>
> [T]he process currently underway presents an opportunity for many delegations from the developing countries to have a tool that would facilitate international cooperation on cybercrime and help them tackle the challenge.[193]

A study by Queen Mary University, commissioned by the FCDO, found that a lack of cross-border collaboration was "a limiting factor in any country's ability" to handle cyber threats.[194]

The UK Government states that it promotes the Budapest Convention as an "effective template for international cooperation". Alongside its allies, the Government opposed the original resolution but says that it is now "actively participating" in the treaty negotiations.[195]

192 UN Office of the Human Rights Commissioner, OHCHR key-messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes, 17 January 2022

193 Chatham House, Can a cybercrime convention for all be achieved?, 31 March 2022

194 Queen Mary University, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware – 114428, 16 December 2022

195 HMG, Written evidence to the Joint Committee on the National Security Strategy's inquiry into ransomware - 114408, 16 December 2022, para 84

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary