DIGITAL REVOLUTION

# STRENGTHENING CYBER RESILIENCE FOR BUSINESSES

FUTURE OF THE ECONOMY
WHERE BUSINESS BELONGS

British Chambers of Commerce
DIGITAL REVOLUTION

# CONTENTS



# INTRODUCTION AND EXECUTIVE SUMMARY

**Shevaun Haviland**
Director General,
British Chambers
of Commerce

**The opportunities that a digital environment can present to businesses are endless. Better connectivity, more efficient processes, and employees skilled in how to use Artificial Intelligence, can help businesses grow.**

However, recent cyber attacks, targeting important organisations and everyday services, have highlighted the scale of the cyber threat that faces the UK. Businesses of all sizes have been the victim of cyber attacks with significant impacts. In addition, there is a technical skills gap, with many businesses lacking the resources they need to be protected against cyber attacks. Ensuring confidence in the cyber security of the UK's digital infrastructure is vital for the country's security, investment and growth.

The BCC's Cyber Resilience report examines the scale of the cyber threats facing the UK and assesses recent steps by government to address these risks, including the National Cyber Strategy and the recently announced Cyber Security and Resilience Bill. It also considers the progress made to improve collaboration between the Government and industry, such as through the Government-backed Cyber Essentials scheme, which demonstrates the role that our Chambers of Commerce can play in supporting businesses to be more cyber secure.

The report includes a series of recommendations to strengthen engagement between businesses and the Government to help make the UK more cyber resilient. The recommendations will help support businesses to take the right steps to be more cyber secure. It also makes the case for a reinsurance pool to underwrite cyber risk and promote cyber security practices.

Through increased collaboration between businesses and the Government, we can strengthen the UK's cyber security and make the UK one of the safest places for businesses to grow.

# UNDERSTANDING THE SCALE OF THE PROBLEM

## Threat facing the UK

The UK faces a wide range of cyber threats, including from hostile states, organised criminal groups, hacker activists and individuals. Cyber attacks can take form in a variety of ways, including through the use of malicious software (malware), the theft of data or targeting a vulnerability in an IT system.[i]

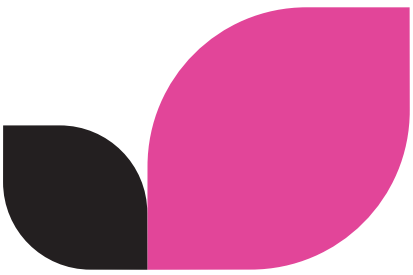
According to the National Cyber Security Centre (NCSC), ransomware attacks pose the most immediate threat to the UK's Critical National Infrastructure. As the NCSC highlights, "any organisation relying on digital technology, directly or through its supply chain, is at risk of a cyber incident. [...] criminals will exploit weaknesses in an organisation without any regard for the sector it operates in, its size, or who is impacted."[ii]

There have been a number of significant cyber attacks on services and organisations in the UK, which have had severe and wide-ranging impacts on services and individuals. This includes a ransomware attack on the NHS in June 2024, which affected services in major London hospitals, resulting in over 4,900 acute outpatient appointments and over 1,300 operations being postponed, along with significant concerns about data security. Following the incident, the founding CEO of the UK NCSC, Professor Ciaran Martin, warned that the NHS remained vulnerable to further attacks if updates were not carried out to its systems. [iii]

In September 2024, a cyber security incident took place on Transport for London, and it was estimated that around 5,000 customers' sort codes and bank account details may have been accessed by hackers through the incident. Other data such as names, addresses and contact details had also been accessed, and an individual in the UK was arrested on suspicion of Computer Misuse Act offences.[iv]

In addition, the Ministry of Defence has also been targeted, where a malign actor gained access to parts of the Armed Forces payment network, affecting service personnel. The system targeted contained personal data of Armed Forces personnel, including names, bank details and addresses. When giving a statement to the House of Commons about the incident, the then Secretary of State for Defence, Grant Shapps, said that there were "indications that this was the suspected work of a malign actor, and we cannot rule out state involvement. The incident is further proof that the UK is facing rising and evolving threats."[v]

These high-profile attacks on vital institutions and services in the UK demonstrate the wide range of attacks affecting the UK, their impact on everyday life, and how they can come from a range of sources—including individuals based in the UK, and malign actors, possibly abroad. This shows the magnitude of the threat of cyber attacks facing the UK.



## Businesses: Cyber Security Breaches Survey 2024[vi]

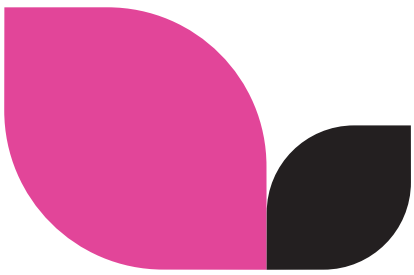
In relation to businesses, the Government's Cyber Security Breaches Survey 2024 found that cyber security breaches and attacks remain a common threat, with 50% of businesses and 32% of charities reporting having experienced some form of a cyber security breach in the previous 12 months. The most common type of breach or attack was phishing, followed by impersonating organisations, viruses and other malware.

The cost of cyber breaches or attacks to businesses can be severe. According to the same Cyber Security Breaches Survey, the single most disruptive breach from the last 12 months cost each business, of any size, an average of £1,205. For medium and large businesses, this was around £10,830. Particularly at a time when many businesses have been struggling with increased costs, the impact of cyber attacks on businesses, of all sizes and sectors, should be of great concern.

The survey also highlighted some of the challenges that smaller businesses specifically face with cyber security. When facing a cyber incident, smaller organisations have often found it harder to develop incident response plans, due to a lack of in-house expertise or capacity. Other challenges faced by smaller businesses include a lack of knowledge as to how to prepare, tighter budgets, and team capacity. This compares to some of the experiences of medium or large businesses, which have carried out simulation exercises or scenario tests.

Around the question of reporting cyber breaches, the survey also highlighted that many businesses do not report their most disruptive breach or attack, with the most common reason for this being that it was not considered significant enough to be reported. Other reasons highlighted included not knowing who to report it to, not having enough time to report it, or not believing that reporting will make a difference.

Following their most significant breach or attack, 23% of businesses said that they carried out additional staff training or communications. 9% said they changed or updated their firewall or system configurations and 8% said that they had installed, changed or updated anti-virus or anti-malware software. However, 39% of businesses reported that following their most disruptive breach or attack, no action was taken.



## Businesses: Supply Chains

Supply chains also present another challenge for businesses in relation to cyber security, through third-party access to systems, or phishing attacks originating from suppliers but with the impact spreading to businesses. While many organisations understand that there are cyber security risks through supply chains, some organisations, particularly smaller ones, often have limited formal procedures in place to manage these risks. According to the Cyber Security Breaches Survey, only 11% of businesses said that they review the risks posed by their immediate suppliers, and only 6% said that they look at their wider supply chain.

In relation to supplier risks, the Cyber Security Breaches Survey has shown how organisations address these risks in different ways. This includes a more formal approach, such as contractual arrangements, external accreditations (for example, ISO 27001), logging data flows and meeting with suppliers. However, there are also more informal approaches to supply chain cyber risk management, including emailing suppliers on an ad hoc basis to ask about cyber security measures.

## Businesses: Cyber Security Accreditation / Insurance

More widely, the British Chambers of Commerce published research in 2022 which showed that more than half of businesses believed that their IT systems were left more exposed to attack following the increase in people working from home during the pandemic. In addition, four out of five firms said that they did not currently have accredited cyber security measures in place to protect against attacks. This, and the shift to remote working have demonstrated the importance of having the right cyber security protections to ensure that businesses are cyber resilient.[vii]

Despite this, however, only 8% of businesses and 5% of charities had a specific cyber security insurance policy in place. This is higher for larger businesses, but remains very low, with only 25% of medium businesses and 26% of large businesses having a specific cyber security insurance policy in place.[viii]

## ISO 27001 Accreditation

However, there are also concerns with more formalised accreditation schemes. This includes ISO 27001, an information security management standard, which structures how organisations should manage risk associated with information security threats, including policies, procedures and staff training. Certification to ISO 27001 is recognised globally and indicates that an organisation's systems align with security best practices.[ix]

ISO 27001 is used by many businesses and public sector organisations as a core security and cyber security criterion for being accepted as a suitable supplier for procurement contracts. While achieving ISO 27001 certification can help SMEs to leverage a wider range of business opportunities and achieve growth and is not an expensive process, it is often found to be resource-intensive, requiring extensive policy development, staff training, and internal audit arrangements.

### RECOMMENDATIONS

**The Government should carry out a cyber security awareness and engagement programme for businesses, particularly smaller businesses. This could include:**

- Improving access to Government-approved cyber security training for businesses and their employees.
- Supporting businesses with carrying out cyber security risks assessments, including across the supply chain.
- Helping businesses to understand how to report cyber breaches or incidents.
- Supporting businesses to achieve ISO 27001 accreditation.

The British Chambers of Commerce network is well-placed to facilitate engagement with the Government, and promote cyber security practices to businesses of all sizes and in all sectors.

## Cyber Security Shortages in the UK

Like many sectors of the economy, businesses have faced significant skills challenges with both cyber security workers and employees skilled on cyber security. According to research on cyber security skills in the UK labour market published by the Department for Science, Innovation and Technology, the total shortage of cyber security professionals has grown each year due to the accumulation of unmet demand from previous years.

It is estimated that around 30% of cyber firms faced a problem with a technical skills gap in 2024. In addition, both recruiters and employers believe there is a significant amount of uncertainty about what the future will look like in the cyber skills landscape because of advanced technologies such as AI.

More widely, the Government has estimated that around 637,000 businesses have a 'basic technical cyber skills gap', with employees responsible for cyber security not having the confidence to carry out basic tasks in cyber security schemes, such as the Government supported Cyber Essentials scheme, which is explored later in this report.[x]

**RECOMMENDATIONS**

**The Government should examine a) how to address existing shortages of cyber security professionals in the UK, and b) how to support more businesses to upskill and train employees on cyber security measures.**

# GOVERNMENT ACTION

## Digital Infrastructure

Since coming into office, the new Government has provided key updates on the security of the UK's digital infrastructure. In September 2024, Chris Bryant, Minister of State for Data Protection and Telecoms, announced that the Government would designate UK data infrastructure as Critical National Infrastructure (CNI), placing this in the same category as energy and water. This recognised the importance of data infrastructure to essential services and the value of the data it holds, as well as the security threats it faces.

As part of designating this infrastructure as CNI, Minister Chris Bryant said that this would signal "the Government's intention to better partner with the UK's data infrastructure sector to work together to mitigate these." In addition, he said that he was confident that these measures, "taken together and implemented in close consultation with industry, will provide a high level of security and resilience for this increasingly critical infrastructure, giving confidence to the public and investors, and supporting the growth of the UK economy."[xi]

**RECOMMENDATIONS**

**The Government should work closely with businesses engaged in the UK data infrastructure sector to discuss what further measures may be needed to strengthen confidence in the UK's digital infrastructure. This may include incentives to encourage adequate investment in security capabilities as well as providing resources and assistance to businesses.**

## National Cyber Strategy[xii]

In 2022, the Government published its National Cyber Strategy. This set out a clear vision for the UK 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". In addition, the strategy set out five pillars to guide the specific actions that will be taken, as well as the outcomes that the Government intended to achieve by 2025:

**PILLAR 1**
Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry

**PILLAR 2**
Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected

**PILLAR 3**
Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies

**PILLAR 4**
Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power

**PILLAR 5**
Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers.

These pillars include vital steps to supporting the UK's cyber resilience, in particular deepening the partnership between government, academia and industry, as well as reducing cyber risks so that businesses are able to benefit from digital developments.

The Government also committed in the strategy to "more integrated and effective regional cyber networks across the UK, enabling stronger partnerships between government, businesses and academia to support sectoral growth and business resilience." As part of this, the Government said it would work with regional cyber clusters and the UK Cyber Cluster Collaboration (UKC3) to help strengthen regional links. UKC3 facilitates collaboration, knowledge and best practice sharing, as well as identifying new needs and opportunities, and is a key resource for cyber security organisations, particularly at regional levels.[xiii]

The Labour Party manifesto recognised the "growing emergence of hybrid warfare, including cyber-attacks and misinformation campaigns which seek to subvert our democracy. To ensure the UK is fully prepared to deal with these interconnected threats, Labour will conduct a Strategic Defence Review within our first year in government."[xiv]

Since taking office, the new Government has recognised the work of the National Cyber Strategy and has said that it is reviewing its national security and resilience priorities.[xv]

**RECOMMENDATIONS**

**The Government should publish an update to its National Cyber Strategy, to reaffirm its commitment to the five pillars guiding the UK's cyber security work. This should include updates on the progress to meeting the actions and outcomes by 2025.**

## Cyber Security and Resilience Bill

At the King's Speech in 2024, the Cyber Security and Resilience Bill was announced. In presenting the Bill, the Government highlighted recent cyber attacks by criminals and state actors and their impact on public services and infrastructure.

According to the Department for Science, Innovation and Technology, "the Bill will strengthen our defences and ensure that more essential digital services than ever before are protected, for example by expanding the remit of the existing regulation, putting regulators on a stronger footing, and increasing reporting requirements to build a better picture in government of cyber threats."[xvi]

This legislation, due to be formally introduced to Parliament in 2025, could be a welcome step to strengthening the UK's digital security, and has the opportunity to send a signal of confidence in the UK's cyber resilience.

However, despite the Bill having not yet been published, it has already been reported that this Bill will lead to increased compliance costs for businesses.[xvii] While these are likely to be important for their security, the Government should now ensure that reporting requirements do not represent an unnecessary burden for businesses, and that businesses are actively incentivised to report cyber breaches or attacks.

### RECOMMENDATIONS

**The Government must ensure full and extensive consultation with businesses with any proposed cyber security legislation, to ensure that the business community fully understands its requirements. This includes sharing, where possible, timely, actionable and meaningful intelligence identified from cyber breaches and attacks with the business community to indicate where further action may be needed.**

**The Government should also explore options to incentivise businesses to report cyber breaches or attacks, rather than penalise, so that reporting requirements are not regarded as an additional burden on businesses.**

# STRENGTHENING ENGAGEMENT BETWEEN THE GOVERNMENT AND BUSINESSES

The Government has acknowledged the importance of its role in strengthening cyber security in the UK and has also recognised the role that businesses need to play to boost cyber security. Below are two examples of how businesses and the Government can work together to address the serious cyber threat facing the UK.

## Cyber Essentials[xviii]

This is a Government-backed scheme that provides protection for organisations against cyber attacks. Cyber Essentials is the minimum baseline cyber security standard for organisations in the UK. The process of preparing for the assessment is an affordable and accessible way for organisations of all sizes to put in place the technical controls needed to protect themselves against the most common cyber threats.[xix] According to the NCSC's Annual Report 2024, businesses that have implemented Cyber Essentials are 92% less likely to make a claim on their cyber insurance.[xx]

The British Chambers of Commerce holds the Cyber Essentials plus accreditation. Members of participating Accredited Chambers of Commerce are eligible for a discount on a Cyber Essentials assessment alongside a training package, free cyber security guidance, and the Cyber Essentials Readiness Tool. This scheme is significant in demonstrating the important role that Chambers of Commerce play in supporting businesses to take steps to be more cyber secure. They are trusted and reliable sources of information and resources, helping businesses save time in adopting necessary measures.

## Cyber Reinsurance Scheme[xxi]

From its engagement with key stakeholders, the BCC understands that many insurance companies have been unwilling to offer cyber insurance. In cases where cyber insurance is offered, many businesses have reported finding the cost of insurance to be too high, or the application process to be too complicated.

A potentially disastrous cyber attack could have a huge financial impact on businesses, including bankruptcy. Cyber insurance can help strengthen resilience to attacks through incentivising businesses to take preventative measures, reducing the frequency of cyber attacks and the overall risk they pose.

The BCC recommends that the Government work with the insurance industry to create a reinsurance pool to underwrite cyber risk. This would help to promote effective cyber security practices for businesses in the UK. This could also help position the UK as a leader in cyber security insurance, increasing confidence in the UK's cyber resilience.

**RECOMMENDATIONS**

**The Government should explore working with the insurance industry to create a reinsurance pool that underwrites cyber risk and promotes effective cyber security practices for all UK businesses.**

# CONCLUSIONS AND RECOMMENDATIONS: HOW TO INCREASE BUSINESS CONFIDENCE IN THE UK'S DIGITAL INFRASTRUCTURE

1. The Government should carry out a cyber security awareness and engagement programme for businesses, particularly smaller businesses. This could include:
   - Improving access to Government-approved cyber security training for businesses and their employees.
   - Supporting businesses with carrying out cyber security risks assessments, including across the supply chain.
   - Helping businesses to understand how to report cyber breaches or incidents.
   - Supporting businesses to achieve ISO 27001 accreditation.
2. The Government should examine a) how to address existing shortages of cyber security professionals in the UK, and b) how to support more businesses to upskill and train employees on cyber security measures.
3. The Government should work closely with businesses engaged in the UK data infrastructure sector to discuss what further measures may be needed to strengthen confidence in the UK's digital infrastructure. This may include incentives to encourage adequate investment in security capabilities as well as providing resources and assistance to businesses.
4. The new Government should publish an update to its National Cyber Strategy, to reaffirm its commitment to the five pillars guiding the UK's cyber security work. This should include updates on the progress to meeting the actions and outcomes by 2025.
5. The Government must ensure full and extensive consultation with businesses with any proposed cyber security legislation, to ensure that the business community fully understands its requirements. This includes sharing timely, actionable and meaningful intelligence identified from cyber breaches and attacks with the business community to indicate where further action may be needed.

   The Government should also explore options to incentivise businesses to report cyber breaches or attacks, rather than penalise, so that reporting requirements are not regarded as an additional burden on businesses.
6. The Government should explore working with the insurance industry to create a reinsurance pool that underwrites cyber risk and promotes effective cyber security practices for all UK businesses.

# APPENDIX


i. House of Commons Library Briefing, Cybersecurity in the UK, 19 April 2024, https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf

ii. NCSC Annual Review 2024, https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf

iii. BBC News, 8 July 2024, https://www.bbc.co.uk/news/articles/czd9glyx414o

iv. BBC News, 12 September 2024, https://www.bbc.co.uk/news/articles/c4gqg2elkj4o

v. House of Commons Statement, Grant Shapps, 7 May 2024, https://hansard.parliament.uk/commons/2024-05-07/debates/56231312-9D57-4CB6-A649-EFA0621B7293/DefencePersonnelDataBreach

vi. The following paragraphs in this section make numerous references to the following survey: DSIT, Cyber Security Breaches Survey 2024, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024

vii. BCC News, 10 January 2022, https://www.britishchambers.org.uk/news/2022/01/bcc-finds-rising-cyber-attack-fears-in-hybrid-working-world/

viii. DSIT, Cyber Security Breaches Survey 2024, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024

ix. UKHSA, Approval standards and guidelines: data security, ISO 27001, https://www.gov.uk/government/publications/accessing-ukhsa-protected-data/approval-standards-and-guidelines-data-security

x. DSIT Research and Analysis, Cyber security skills in the UK labour market 2024, https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/

xi. HC Statement, Chris Bryant, 12 September 2024, https://questions-statements.parliament.uk/written-statements/detail/2024-09-12/hcws89

xii. Cabinet Office, National Cyber Strategy 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022

xiii. UK Cyber Cluster Collaboration, https://ukc3.co.uk/about/

xiv. Labour Party Manifesto 2024, https://labour.org.uk/wp-content/uploads/2024/06/Labour-Party-manifesto-2024.pdf

xv. HC, WQ, Abena Oppong-Asare, 2 September 2024, https://questions-statements.parliament.uk/written-questions/detail/2024-07-30/2299

xvi. DSIT, Cyber Security and Resilience Bill, https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

xvii. Business ITN, What businesses need to know about the Cyber Security and Resilience Bill, 22 July 2024, https://business.itn.co.uk/what-businesses-need-to-know-about-the-cyber-security-and-resilience-bill/

xviii. NCSC, Cyber Essentials, https://www.ncsc.gov.uk/cyberessentials/overview

xix. BCC, Member Benefits, Chamber Cyber Essentials, https://www.britishchambers.org.uk/join-the-chamber-network/member-benefits/

xx. NCSC Annual Review 2024, https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf

xxi. BCC Digital Revolution report: https://www.britishchambers.org.uk/wp-content/uploads/2024/06/Digital-Revolution-Challenge-Report-June-2024.pdf


British Chambers of Commerce | 65 Petty France, London, SW1H 9EU
britishchambers.org.uk | @britishchambers | 020 7654 5800