The Institution of Engineering and Technology

2025 Autumn Budget Representation

About the Institution of Engineering and Technology (IET)

The IET is a trusted adviser of independent, impartial evidence-based engineering and technology expertise. We are a registered charity and one of the world's leading professional societies for the engineering and technology community with over 158,000 members worldwide in 153 countries. Our strength is in working collaboratively with government, industry and academia to engineer solutions for our greatest societal challenges. We believe that professional guidance, especially in highly technological areas, is critical to good policy making.

Introduction

The impact of cybercrime is far reaching, not only in immediate costs for the primary business and supply chains, but it has an individual and societal impact as well. It is a national concern that requires resilience and prioritisation from businesses, government, and individuals.

Businesses must be incentivised to make systems secure by design and individuals made aware of how to protect themselves from cyberattacks. A public awareness campaign that outlines the key actions individuals can take to make themselves more resilient to attack would help support business and individuals to be more cyber aware. This will bolster the UK's defences against attack, reducing the potential cost to UK businesses.

Recommendations

1. **The IET is calling on the Treasury to cut business rates for small and medium sized companies that are investing in their cybersecurity training and systems.**

2. **The IET is calling on the Treasury to commit to £5-10 million funding in the Autumn Budget to run a public awareness campaign that outlines key actions individuals can take to make themselves more resilient to attacks.**

A recent survey by the IET found that over half of people fear being hacked and nearly one in seven have been a victim of hacking, (rising to a fifth of 25–34-year-olds) (Source: IET, Cyber Crisis: Is the UK public losing faith in cybersecurity and data protection?). The majority of people think hackers are becoming more inventive, for example, through fake QR codes in hospitals or museums; resulting in people falling victim to attacks in places they trust. The Government has invested in the Cyber Growth Action Plan and upcoming Cyber Security and Resilience Bill; however, the critical missing piece is greater investment in public awareness. Cyber Security Awareness Month brings attention to cybersecurity issues, but our research also showed that over a third of people are not aware of what actions to take to protect themselves after a cyberattack. Businesses should ensure that their products and services are secure by design, however, this can only go so far and even the most prepared organisations can still be targeted.

The IET is calling on the Treasury to commit to £5-10 million[1] funding in the Autumn Budget to run a public awareness campaign that outlines key actions individuals can take to make themselves more resilient to cyberattacks. Research from NESTA in 2024 showed that mass campaigns can cost £5 million over a 5-year period, providing government a benefit of £300 million every year (Source: NESTA, Fund and roll out mass media campaigns aiming to promote healthy eating). Funding greater awareness amongst the public of how to improve their security and become more resilient will bolster the UK's defences against attack. The widespread costs of cyberattacks far outweigh the cost of investment in prevention.

Cybersecurity needs a trifecta approach, combining efforts of businesses, government, and the public to enhance the UK's resilience. Current initiatives to support businesses are very welcome, however in a survey of engineering employers, SME's have told us that they still struggle to reskill and upskill in vital areas such as this. Compared to large organisations they are less likely to recognise cyber skills as an important skill for growth (45% of large companies vs 31% of SME's) (Source: IET, UK Engineering and Technology Skills). The IET is calling on the Treasury to cut business rates for small and medium sized companies that are investing in their cybersecurity training and systems.

Cybersecurity for businesses

There is no ceiling on the economic harm that a cyberattack could cause, instead that calculation is based on the depth and seriousness of the attack. According to research by ESET, cyberattacks cost UK businesses an estimated £64 billion annually, with £37.3 billion in direct costs and £26.7 billion in indirect costs (Source: ESET, The True Cost of Cyber Attacks: Balancing business protection and risk). In the case of the ransomware attack at M&S, it is predicted that the total cost of this breach will likely be between £270 million and £440 million across affected organisations (Source: Cyber Monitoring Centre, Cyber Monitoring Centre Statement on Ransomware Incidents in the Retail Sector – June 2025).

Ensuring UK businesses are informed and incentivised to strengthen cyber resilience should be a priority for government. Cyber, geopolitical, and Net Zero developments mean that investment in resilience and mitigation planning is vital for the UK's economic security. A brittle infrastructure can induce a negative chain reaction throughout the wider system. For example, the total engineering economy contributes up to 32% of the direct GVA annually to the UK economy (Source: RAEng, Engineering Economy and Place). A cyberattack such as the one on Jaguar Land Rover, has exposed the fragility of the UK's just-in-time (JIT) supply chains. As the engineering industry relies on JIT supply chains, another attack of this scale could potentially have massive repercussions to national infrastructure projects if they are disrupted in this way.

Communicating the potential threats and risks around cyberattacks will increase awareness, develop competence, and create the correct cybersecurity culture within an organisation. However, investment in one area does not necessarily mean resilience across the entire system. To create resilience, there needs to be a technical understanding of the issues, processes, and interdependencies when assessing risks with a whole-system engineering perspective informing decisions. (Source: IET, Spending Review 2025)

Cyber Essentials is a key initiative that businesses should engage with. IET research has found that, according to engineering employers, one of the most important digital skills in the next five years is cyber (38%), however it is one of the most difficult skills to recruit for (17%)

---

[1] Government funding for campaigns such as the "Great" Tourism campaign (Source: FT, Budget for UK's 'Great' tourism campaign cut by 41%) and the NHS "Better Health" campaign both cost around £10 million (Source: Campaign, Govt to launch reported £10m 'Better health' campaign to tackle obesity).

(Source: IET, UK Engineering and Technology Skills). Businesses must be encouraged to be secure by design in the delivery of products and services to protect individuals, but even the best prepared organisations can still be attacked, which is why it is important to strengthen public resilience, and simple measures will make a big difference.

Cybersecurity for the public

Cyber Security Awareness Month brings significant awareness to the issues that cyberattacks can cause, but IET research shows that 56% of those surveyed fear cyberattacks, with 14% of those surveyed having already fallen victim to cybercrime (Source: Cyber Crisis: Is the UK public losing faith in cybersecurity and data protection?). Concerningly even after being attacked only 50% of people monitor accounts more closely, while nearly 13% change nothing, and only 27% of 16-24-year-olds increase vigilance.

In conclusion, with the Cyber Growth Action Plan and upcoming Cyber Security and Resilience Bill there is an opportunity for the Treasury to support these initiatives and provide the funding required to communicate the potential threats and risks around cyberattacks. Government can encourage businesses, specifically SMEs, by cutting business rates for those who invest their cybersecurity training and systems. This, combined with a public awareness campaign to communicate the importance of key actions to make individuals more resilient to cybercrime, can demonstrably strengthen the cyber resilience of the UK.