Unsplash © Adi Goldstein

# MaddyFeed or what you need to know about Whitehall’s cyber security spending splash

Every week, Maddyness curates articles from other outlets on a topic that is driving the headlines. This week, we're talking about growing fears of cyber security and the government splash on tools and training to combat this.

---

## Data secured by UK think tank Parliament Street has revealed that the Cabinet Office has increased spending on cyber security training for staff members by nearly 500 per cent in the last year.

The information comes amidst numerous cyber security threats circulating in Whitehall after CCTV footage of former UK Secretary of State for Health and Social Care, Matt Hancock, breaching Covid lockdown legislation through an affair, was leaked to the UK press.

The FOI response not only revealed that the Cabinet Office spent a total of £274,142.85 on cyber security training for staff in the most recent financial year, but also the number of separate cyber training courses booked in the same year, at 428. In the 2019-2020 financial year, this number was only 35.

> *The amount of spending increased by a total of 483 per cent.*

The response also revealed that the most popular course, receiving a total of 332 bookings, was the NCSP Foundation e-Learning, provides introductory level training on how to prevent, detect and respond to cyber-attacks. Other popular courses included the Foundational Certificate in Cyber Security, another in 'the art of hacking,' and that to become a certified Lead Auditor.

Security specialist Edward Blake, Area Vice President EMEA, *Absolute Software* said, "It's encouraging to see the government levelling up its cyber defences, particularly at a time when recent CCTV leaks are raising fresh questions about security standards across Whitehall.

Read more via *Education Technology*.

## Security sweep in department offices

While the splash on cyber security and uptake of training courses was growing before recent news, the events of this week have no doubt escalated fears around the security of devices installed in government departments.

Security teams have since carried out sweeps within department offices, including the Department of Health and the Department of Justice.

Philip Ingram, retired Military Intelligence and Security Officer, told The Financial Times that leaked footage should prompt an even tighter grip on security.

"Now is the time for Whitehall to shake itself up and show it's taking security matters seriously."

Read more via *The Financial Times.*

# The security risks of a mobile phone

It’s not just inside government departments that the fear of cyber attacks are growing. This week, news emerged that Foreign Secretary, Dominic Raab’s mobile phone number was circulating online.

For government officials, having their numbers accessible online poses a particular security risk. This is because the device, as well as its data, calls, messages and functions including the microphone and camera, can be manipulated and invaded using sophisticated spyware technology.

A recent report from Citizen Lab revealed that even a mobile phone number is enough for such a cyber attack to occur. Read more via *The Guardian*.

# Why government ministers should not use private accounts for government business

It’s not only private devices, but also private accounts that are at risk of attack from outside.

After his resignation, government sources also revealed that Hancock had used personal email accounts to conduct official business. Not only does this undermine ministerial duties of responsibility and accountability, but using private accounts might also leave accounts open to cyber attacks.

Emails sent from a UK Defence of Foreign Affairs Minister, for example, are often subject to national security laws. Read more via *BBC News*.

---

Article by ABBY WALLACE