CIONET
What's next.

EY
Building a better working world

Digital Leaders Forum

THE INTERSECTION OF CYBERSECURITY AND AI IN UK GOVERNMENT

January 2024

EY and CIONET join forces to bring you the Digital Leaders Forum, exploring end-to-end organisational transformation.

Digital Leaders Forum Event – January 2024
The intersection of cybersecurity and AI in UK government

A discussion dinner was held on the 17th of January, sponsored by EY UK&I as part of the Digital Leaders Forum for 2024, titled 'The intersection of Cyber and AI in UK government. Senior executives from several government departments attended. Paul Robertson and Rick Hemsley, Partners at EY UK&I, introduced the event. The session was moderated by Roger Camrass, Research Director of CIONET International.

Why is AI critical to cyber thinking?

Rick and Paul from EY said the rise of AI brings threats and opportunities. For government organisations, highly capable AI technologies can be used to help address talent shortages and reduce pressure on cyber teams. AI can also deliver automation, boost authentication, and power behavioural analysis that assists in cyber-monitoring activities.

However, AI can also be a powerful tool for criminals and nation-state actors. New AI tools are emerging that have fewer ethical boundaries and are positioned as aids that help errant individuals to hack or deploy malware. This AI-led automation can accelerate code-writing processes for the production of malware and deep-fake videos, which can be used to gain unauthorised access to systems. In combination, these powerful generative AI tools and the activities they enable present business leaders with a fresh set of intractable challenges.

The audience agreed with these observations and suggested that recent developments, such as the rise of ChatGPT, might affect consumer confidence in the provision of government services. Attendees in the room were also concerned about how AI might help criminals to outstrip UK cyber defences. In addition, attendees recognised that regulations and laws are often enacted reactively, following events rather than leading them.

Where does the government sit at the intersection between AI and cyber?

Government organisations are not always able to respond rapidly to technology-led developments, such as the rise of generative AI. Approaches taken by attendees varied. Some executives take a slow, regulated approach to adoption. Others wait and see how the technology landscape develops. A final group act as early adopters, developing trials and implementing strategies for emerging technologies.

The Cabinet Office has taken steps to introduce a 'secure by design' blueprint that helps departments draw on pioneering thinking around AI and cyber. However, a large proportion of government IT remains unmodernised and could be at risk from AI-led cyberattacks. An executive from Crown Commercial Services said the government is putting pressure on its strategic suppliers, such as Microsoft, Oracle and SAP, to provide effective defences against cyberattacks. This approach is now a mandatory element of the procurement cycle.

A combination of internal expertise across Government Digital Services, the Ministry of Defence and the Cabinet Office should help the UK pursue rapid innovation at the intersection of AI and cyber. According to a Cabinet Office official, experiments are being conducted to explore new technologies, including quantum computing. This kind of coordinated effort could support government departments that do not have the funds or expertise to keep up with recent developments in AI and cyber.

However, there is much work to be done. Attendees suggested collaboration across government departments is often driven by incident rather than intent. This reactive approach places the UK and other Western countries in a poor position relative to the speed and agility of cyber criminals and nation-state actors in places such as Russia, China and Iran.

How can the government benefit from AI-assisted cyber developments?

One executive at the event suggested the government should be more proactive in engaging private sector support. One area that must be addressed is customer service channels, which could be automated by using intelligent chatbots. Call centres belonging to HMRC, the NHS and the Police are often overwhelmed by demand from citizens and businesses. In the private sector, many retailers and banks are already experimenting with AI-enabled chatbots that help to reduce waiting times. These organisations are also taking steps to ensure any cyber risks are minimised as they adopt an AI-led approach.

A second area that must be addressed is productivity. Research suggests productivity within the civil service has declined by 17% since the start of the coronavirus pandemic. Organisations also have to contend with a small pool of in-demand cybersecurity talent. Help comes in the form of AI tools, which could augment existing cyber talent by acting as force multiplier that enhances productivity levels. However, while AI can automate workflows, the technology can also be used by hackers, increasing the prevalence of external cyber risks. AI can also be used to monitor individual productivity, especially home workers. It is important tools are developed that measure AI productivity gains in the longer term.

One executive at the event suggested the UK is already intelligence-led and can mobilise a proactive response to fresh dangers. The executive gave the example of the UK's experiences of foiling potential terrorist attacks. All attendees acknowledged the propagation of best practice is difficult because of the scale of the civil service. A delegate from the Police is hoping to hold an AI Summit to raise awareness of new threats and opportunities.

Where do we go next?

Paul and Rick from EY concluded the event by suggesting that AI brings big benefits to government teams, providing that inducements are in place to encourage adoption. Rick shared the view that cybersecurity should not be a blocker to AI adoption. Instead, executives need to explore and experiment in a safe and controlled manner by working with trusted partners that help drive strategy. Rick suggested a "carrot and stick" approach to driving the adoption of AI across departmental boundaries.

The automation of workflows and public interfaces has the potential to provide the productivity gains that are needed in the post-COVID age. However, progress in these areas will increase the breadth of attack surfaces across applications, data centres and at the edge. Careful planning is required to ensure the benefits of AI are balanced against cyber risks.

All delegates recognised the need for intensive cyber training across government. This training will help the UK to prepare for an increasing number of cyberattacks in the AI era.

It is clear from the event that the UK government is taking the evolution of AI and cybersecurity seriously, with some excellent initiatives already in place. Acting fast is essential: given the pace of development in AI, organisations must work in parallel to create policies, engage senior stakeholders, and develop new tools.

Roger Camrass
Research Director –
CIONET International

A pioneer of today's Internet as an ARPA research fellow at MIT in the seventies, Roger has spent over fifty years helping corporations harness the power of new technologies such as AI, cloud, mobile communications, e-commerce, voice recognition and satellite. He was a partner at EY responsible for e-commerce during the dot.com boom. He is a Cambridge University and MIT graduate and a visiting professor at the Hebrew University in Jerusalem.

rogercamrass.com

Rick Hemsley
Partner, EY UK&I Consulting

Rick Hemsley is a partner at EY UK&I Consulting. With over 25 years of consulting and industry experience, Rick has worked with a broad range of organisations, including governments. With Rick's guidance, clients have been able to enhance reporting and operating models. This has helped them gain an actionable and accurate picture of their cyber security posture and build a priority list of activities to further enhance cyber resilience. Rick joined EY in 2022 from a large global consulting organisation where he delivered key cybersecurity transformation projects for clients. Prior to this, he worked in leadership roles for leading cybersecurity organisations.

Dr. Paul Robertson
Partner, EY UK&I Consulting

Dr. Paul Robertson is a partner at EY UK&I consulting, specialising in cyber resilience, preparedness and response. He has worked across multiple sectors and been involved in the preparation for, response to and recovery from some of the largest and most high profile crisis and incident responses of the last few years, including major cyber events, pandemics and geopolitical tensions. Paul focuses on leadership, values and principles. These inform everything and getting any organisation to really back those values before, during and after a crisis is a game-changer for crisis capability. He is a noted speaker at national and international conferences.