ALL-PARTY PARLIAMENTARY GROUP ON CYBER SECURITY & BUSINESS RESILIENCE DINNER 22ND MAY 2024 -

STRONGER TOGETHER

What is the Digital Sense of the Future?

No matter what is going on in the nation, the importance of cybersecurity remains a constant. This point was emphasised by James Morris MP, who began the discussion with a powerful statement: "Whatever the colour of the new government, there will be a complex web of issues which have to be sorted out."

Casey Ellis, Founder of Bugcrowd, representing the cybersecurity industry, opened by reminding us that hackers are "people who like to turn things upside down." Characteristically, when dealing with new things, they "instinctively take them to bits, see how they work, put them back together according to what they want." This means that hacking isn't inherently criminal—there is the good, helpful type as well."

Casey went on to state that "cybersecurity is a human problem first, accelerated by technology, and therefore, humans will always play a key role in cyber defence." He explained that malicious hacking is driven by a number of different factors based on individuals' motivation and making a decision to hack. This can include hacktivism, financially motivated attacks, and nation-state attacks. We should understand that the incentives to hack with malicious intent are manifold and multi-faceted. They are also becoming more so in the current fluid geopolitical and technological environment.

The Human Factor

The cybersecurity industry has evolved hugely over a relatively short lifespan. Ultimately, the industry is all about people and our control of technology. Several examples of innovation outpacing security concerns were discussed which left cybersecurity teams to play catch-up. For example, cloud computing and AI were emerging technologies that needed controls and considerations to keep end-users safe. The human factor is a key component of this.

We all need to protect our personal information, and this needs to become part of the culture. We have to interact with technology, and people need to be brought up to speed to use it properly. Technology will not solve the problem by itself! We would not walk down a dark alley at night in a strange town. Similarly, we were all warned by our parents not to talk to strangers, so why do we do so online? We need to instil the same sense of caution into all of us when dealing with technology and, importantly, make these kinds of decisions easier for non-technical internet users.

UK, EU, and US Cyber Relations

The divergence of regulations and policy between the UK, the EU, and the US was also raised as a concern, as was the urgency of pursuing harmonisation of legislative positions across AUKUS and NATO. We are not on the same page. The EU tends to legislate for both consumers and businesses, as well as platforms that do not have an HQ in a member state. The US tends to take a "first principles" approach, and the UK often finds itself somewhere in between. The number of laws: DORA, MICA, and NIS2 are good examples of this, and reform of the CMA to align with the US CFAA charging rule changes to legalize the work of hackers operating in good-faith, and thus reduce the chilling effect on this type of work, was called out as an example.

ALL-PARTY PARLIAMENTARY GROUP ON CYBER SECURITY & BUSINESS RESILIENCE DINNER 22ND MAY 2024 -

STRONGER TOGETHER

The UK has asked the Financial Conduct Authority to look at cybersecurity. Evidence suggests that the lack of a robust legal framework makes one a target.

The Regulatory Environment

The legal and regulatory framework is not fit for purpose in the UK. For example, the Department for Energy and Net Zero has only had a single breach report since the requirement came into force in 2018. Effective cyber legislation tends to lag behind technological development and cyber attacks. We have seen this in the IoT sector, where products have been launched with very weak security. Legislation tends to be reactive and therefore too late. There is an economic incentive to get products to market first. We have also seen, for instance, a cyber attack such as Mirai in 2016, which did not have any legislative response in the UK.

Commercial Considerations

Casey also reminded the dinner that technology has raced ahead of security. IoT is a great example of this; manufacturers have produced at the lowest cost and often put security at the bottom of the list. AI, and particularly GenAI, have been "dumped into our human consciousness." Bugcrowd is working with the US Government to address cybersecurity issues around AI through policy advisory into the White House.

Dave Gerry told the dinner that a large-scale healthcare breach at UnitedHealth Group caused the company's stock to go up. The market took the view that the attack showed the group was big enough to matter.

The answer suggested was a "secure-by-design" policy, with its focus on security as a first principle and "doing the basics well." This would blend security with the need to get to market quickly. Another suggestion was that, at least for public sector procurement, the onus for cybersecurity should be put on the prime contractor. The prime contractor would then have to cascade down the necessary requirements through their supply chain. If this was made a requirement for procurement, it would weed out non-compliant bidders. James Morris MP commented that this was similar to IR35 requirements. The onus for checking who should be taxed under IR35 requirements is on the top-tier employer.

The International Scene

There are fears that control of technological development has been lost to China, especially in the area of "great power" technologies such as AI and quantum. This is reflected in China's increasing political supremacy as well. Taking quantum computing as an example, both China and the US are well ahead of the UK and the EU. The UK is good at developing new technologies, but China is adept at copying them. Thus, we are losing control of our intellectual supremacy. Power has shifted away from the UK and Europe to the east.

UK universities have a role to play in this. They have used foreign students as a way of boosting income. This has contributed to the loss of our technological lead. Dave from Bugcrowd commented that "Universities are not supplying a breadth of skills and experience for computer science students; courses tend to be too narrow and siloed."

ALL-PARTY PARLIAMENTARY GROUP ON CYBER SECURITY & BUSINESS RESILIENCE DINNER 22ND MAY 2024 -

STRONGER TOGETHER

New Technology

On the topic of AI, it is early days yet, so we can have a proper dialogue on how to secure this sector. Casey discussed the different dimensions of AI security as a tool for attackers and defenders. It provides a fresh and novel attack surface that we're in the early stages of learning how to defend. It is also a threat, given the multitude of potential unintended consequences associated with integrating AI into existing technology, people, and process, and the rapid rate of adoption of AI happening in the market at present. There was a lot of discussion around the potential future security and safety implications of wholesale AI, while the near-term risk discussion was mostly focused on how AI puts sophisticated techniques within easy reach of otherwise unsophisticated threat actors.

Quantum was called out as a looming and understated future threat, with progress on post-quantum resilience slowed by the sudden distraction of generative AI. Quantum is a transitional issue and levels of security may vary considerably. Will the UK adopt NIST? We should avoid walled garden solutions for security and aim for the largest possible adoption of standards at the same time. If we fail with securing quantum and break PKI, then our communications infrastructure will be in trouble. We do need to recognise that we are under attack already. It is a safe assumption that current cryptography will fail. We should work on the basis that current systems are broken and design accordingly.

The Way Forward

James Morris MP asked if the threats are too great or if there are any sunny uplands.

The UK has a lot of expertise in the cybersecurity field. It is, however, caught between two large markets, the US and EU, who are both increasingly legislating in competition with BRICS, et al. These are also legislating to suit their own requirements. The consensus was that trying to do things alone will not work; we must make a choice: work together or work alone. We need a dialogue with our friends and neighbours as well as working protocols. The government needs to ensure that UK products and services are not left out of the EU.

The UK has a relatively small market compared to the EU and the US. A potential role for us is to be a feeder into both markets from the other one. We also have good universities and a history of innovation.

The big picture is how to deal with the autocracies – China, Russia, etc – which are going in the opposite direction. Is there a willingness to talk about cybersecurity? It is easier to co-operate over a threat when it is live and in front of you. We need to start co-operation much earlier. Regulation must be sensible and beneficial.

In terms of dialogue with the EU, the view was that this should be continuous and built into the system. When developing cyber policy, the EU has to deal with the lowest common denominator member state in cyber terms. The best route is to work back from the desired outcome, although this is usually more difficult. There is also a need to be sector-specific. Some sectors, like aviation, are already back on track. It helps that this is an international sector.

In the US, the regulatory line between speed and the social good is a problem. We need to talk with our allies and create a fruitful dialogue. The US is very loose in regulatory terms, whereas the EU is very granular. Industry and government are still trying to work out how to co-operate. There is no shortage of desire to work together.

International vendors have a strong role to play in cross-border co-operation. The UK Ministry of Defence leads on commercial partnership with US companies. Moreover, 80% of what the MoD deals with is common across all sectors. We need to stop working in silos and co-operate. The NCSC is leading on this and is beginning to see results.

Summary of Findings

Findings that emerged from the session included:

- Organisations, corporate and governmental, are struggling with cyber resiliency. Many of these difficulties now revolve around AI, particularly AI safety and AI security. There is not enough security talent on the market to meet the new AI-driven threat landscape. A failure to recruit in sufficient numbers is leading organisations to look beyond the pool of computer science graduates. They need to tap into people who are motivated, intelligent and with some level of technical aptitude. Crowdsourcing security is helping to bridge this talent gap.
- There needs to be greater collaboration and sharing among governments to address new AI-led threats. While the US and the UK have a strong relationship, there is not enough sharing of information on a proactive basis. Cybersecurity must match other forms of physical security and national security in this respect.
- There needs to be a fundamental shift in the thinking of organisations everywhere around incentivising security, treating it as a measure of quality and as a business outcome. This must stem from a board-level perspective as well as create an environment where technologists and workers at the coalface jointly consider some of the business considerations of security. Evidence is already emerging that cybersecurity resilience is becoming a competitive differentiator. In future it could be as important to an organisation’s brand and reputation as, say, environmental or diversity policies.
- The right kind of policymakers are trying to drive a better security regulatory environment for their constituents. By getting policymakers and technologists to collaborate, the result will be an approach to regulation and policymaking that's as effective as it could possibly be.
- In the new paradigm of AI security, the timeline from vulnerability identification to exploitation has been significantly reduced. Historically, this lag would be measured in days, maybe a week before you would see a vulnerability being exploited in the wild. That is now a matter of hours. AI is empowering adversaries as well as making the defender far more efficient and faster in their response to attacks. The adversary is suddenly an expert, able to build malware using AI and advancing at a much higher rate than they historically would have been able to achieve.
- AI is a multi-dimensional issue and can be seen as a tool, target and threat. AI is a tool that is already being used in cybersecurity for attack and defence.

AI is a target – like any software, LLMs contain vulnerabilities that bad actors will seek to exploit. AI is a threat, which raises a number of fundamental safety issues including around privacy and data protection but also around issues of social equity and fairness. AI could amplify existing inequalities or be prone to bias when used in decision-making, e.g. by companies using AI tools to shortlist candidates.

Conclusion

It was clear from the dinner, attended by industry, academic, and civil service representatives as well as parliamentarians, that the incoming government will have both to foster a climate of co-operation with our allies and find a role for the UK between the US and the EU markets. Going solo is not an option; co-operation is the watchword.

Notes:

An All-Party Parliamentary Group is an informal body which operates in the UK Parliament to bring together parliamentarians, industry, academic, and NGOs around a given topic. APPGs are registered with Parliament and operate under a set of rules governed by Parliament. APPG membership is open to members of both houses and all political parties.

9 July 2024