**Government and tech industry collaborate to improve cyber security**

On 23 July 2018, DCMS and NCSC held a roundtable on firmware security with senior representatives of leading hardware and software firms. The purpose of this was to build on recent collaboration across industry.

All those present highlighted the value of existing industry collaboration in providing stable updates to firmware across a wide range of devices, and under significant time pressure. The identification of recent high-profile vulnerabilities had catalysed unprecedented collaboration.

It was clear from discussions that all participating firms recognise the challenges in quickly providing stable updates to firmware. There is also a challenge to maintain end-users’ trust that update processes are robust and that updates can be deployed with confidence.

The meeting discussed the challenges with automated security patching. Though this comes with advantages, particularly for non-professional and non-expert users, it poses risks and technical challenges, and would not be appropriate in all cases.

Significant progress has already been made throughout the ecosystem, and this progress will continue. We have a shared aim to make it easier for end-users to keep their devices secure and up to date - reducing the burden on business and the general public.

All those present agreed there is a role for government in convening the ecosystem more widely, identifying and highlighting good practice, and producing cyber security advice and guidance for a range of audiences.

The participants agreed to reconvene in early 2019.

Agreed by organisations represented at the 23 July roundtable. Including AMD, Apple, ARM, Dell, HP Inc, Intel, Microsoft, Qualcomm, Samsung, DCMS, techUK and NCSC.

**Supporting quotes**

**Samsung**

“Samsung views the security of its customers as of paramount importance, which is why we have developed our world leading device security and why we are committed to working with the British Government to protect British consumers and businesses.”

Aleyne Johnson, Director of Government & External Relations, Samsung

**Microsoft**

“Microsoft places a very high priority on the security of our customers.  We have rigorous processes for updating firmware, working closely with industry partners, but are keen to work with the UK government and others to make improvements where we can.”

Hugh Milward, Director  Corporate External and Legal Affairs, Microsoft

**AMD**

“AMD shares the UK Government’s position for continuous improvement of cyber security, and we prioritise the work we do independently and collectively across our ecosystem to enhance the security of our products. We also share the recognition that often the design of security mitigations to new threats require a combination of software and hardware that can introduce complexity to the development, testing and deployment process across the ecosystem. AMD is committed to focusing our engineering and technology teams on improving product security technologies while working collaboratively with others in the industry to quickly mitigate new cyber threats as they emerge.”

Darren Grasby, President, AMD EMEA

**ARM**

“As companies and citizens of an increasingly connected and data-driven society, we have a shared industry responsibility to ensure users can trust their devices. While the advantages of a fully-connected world vastly outweigh the threats, we must react quickly when these threats emerge. To do so effectively, continued collaboration across the industry is essential.”

Simon Segars, CEO, ARM

**HP**

“As we navigate an increasingly complex world of cyber threats, it’s important industry leaders convene and inform the government on the best security solutions out there. “Building on our extensive history of device security innovation, HP supports this initiative and is committed to providing the highest level of security for our customers and partners.”

Ansgar Baums, Head Global Strategy Program, HP

**Intel**

"The security of our products and our customers’ data is a top priority for Intel. We appreciate the opportunity to participate in the industry roundtable and we look forward to ongoing collaboration with industry and dialogue with government on this important topic. We believe this collaboration will support Intel’s long-standing and ongoing efforts to decrease patch validation time for our partners and effectively deploy patches to customers."

Adrian Criddle, Vice President Sales and Marketing Group, Intel

**Qualcomm**

“Qualcomm thanks the UK government for the opportunity to participate in this roundtable discussion on firmware patching and we welcome future cooperation on strategic security and policy matters.

“Qualcomm is committed to timely and accurate exchange of security information between technology suppliers and integrators, and to enabling our customers to provide regular security updates.”

Anne-Lise Thieblemont, Senior Director, Government Affairs, Qualcomm

London, 23 July 2018

|  |  |  |
| --- | --- | --- |
| Press contact | NCSC Press Office | DCMS Press Office |
| Address | National Cyber Security Centre 160 Victoria St, Westminster London SW1E 5LB | Department for Digital, Culture, Media & Sport100 Parliament St, WestminsterLondon SW1A 2BQ |
| Telephone | 07468838893 | 02072112210 |
| E-mail | pressoffice@ncsc.gov.uk |  |
|  |  |  |