DEBATE SECURITY

London, 26 February 2019

Event sponsored by

#becrypt

GARRISON

Debate Security Panel

London, 26 February 2019

The first Debate Security briefing took place on 26th February 2019 in Canary Wharf in London, bringing together senior executives across multiple industries to spark a cyber-risk discussion that compared and contrasted approaches between government and the private sector. Below is an overview of the panel debate. For more information about the panel or about Debate Security events, please contact events@debatesecurity.com.

A decade of cyber attacks

The discussion was opened by a keynote on the topic of the evolution of cyber attacks. A decade ago, the cyber risk landscape comprised of specific actors, particularly nation states, targeting specific government organisations; and commercial organisations facing minor attacks from low profile, low resource hackers.

Two things have changed. Firstly, that in an environment where information is the new gold, commercial organisations are as likely to be a target as nation states, with major breaches becoming regular news. Secondly, that where Government historically hid behind traditional “air gaps” that security approach is no longer sustainable: Government organisations need to use the Internet; to use open-source software; and to collaborate online with other groups. This has represented a major move for Government, with investments in new security approaches designed to avoid the historic “security says no” experience, and investments in new technologies to enable it.

There is evidence therefore both of a convergence of the threat, and of a convergence of the business requirements. Yet despite this, the security practices of Government and the Private Sector remain dramatically different, with the differences arising in two particular (but related) areas. First, that while both sectors have invested significantly over the past decade in solutions to “detect, respond and recover” from cyber attacks, Government focus on solutions to “protect” remains much greater. Secondly, that when it comes to “protect” solutions, Government places far more emphasis than the private sector in assessing whether the products they deploy actually deliver the security benefits they claim.

Indeed, it was brought to light that it is common for National Security Organisations to spend years of effort evaluating a security product, but it is rare for a financial institution, for example, to go beyond a basic penetration test and overall product evaluation. Purchasing decisions are mainly feature focused and many neglect even to identify the actual security of a product as a selection criterion.

Understanding the difference

With broad agreement amongst panellists and the audience that this did indeed represent a significant difference between the two sectors, it was suggested that the difference likely contributes to the widely shared experience that despite significant private sector investments in cyber security technologies, few CISOs have any real confidence about which of those investments are actually delivering value.

The difference in approaches can be traced ultimately to the fact that government structures identify a specific role for NCSC, a part of GCHQ (in the UK) as the National Technical Authority, and that this provides a locus for cross-government product assurance activities. Without such a natural structure in the private sector, the debate turned to whether there are market mechanisms that might allow private sector organisations to get a better idea of the true levels of security delivered by different products on the market. There was widespread agreement that the current market was failing to deliver, with senior buyers paying attention above all to analyst reports that score security products on the basis of features rather than security.

At the heart of the question is, as one panellist put it, the key question: "who pays?" Indeed, one attendee recounted that having tried to run a product assurance group within a large bank, their activities were constrained by budget, by a lack of career progression for staff – and by the terms and conditions under which they were able to get access to technology products (much of their activity having been conducted in secret to avoid potential legal issues).

Over the course of a spirited discussion, various potential approaches were discussed including:

- Improved definition of security requirements – the discussion highlighted that currently security requirements are barely even stated, and where they are, they are not clear enough to be useful. One panellist commented however that restrictive regulation could be constraining, and this type of new policy would struggle to be adopted if it became a hindrance to purchasing
- Terms and conditions in contracts – by penalising poor security products, vendors would have more incentive to improve their security offering. An example was provided of one buyer of telecommunications products whose contract included a financial penalty clause in the event that a "back door" was discovered in the products
- Insurance – the discussion revolved around the effectiveness of insurance not as a means of making money back (large organisations cannot get enough cover to make this worthwhile), but rather as backing for a product warranty, providing an incentive for the insurance provider to carry out an independent assessment of the product vendor's security claims

The role of government

Much of the discussion centred purely on failings within the commercial market and potential means of remediating the perceived market failures, but there was also discussion about whether there was a role for government to work with the private sector in this area. While there was support for the view that much could be learnt from the way that governments approach buying security products, the challenge is making this useful: indeed one question from the floor suggested that perhaps a list of "bad" vendors should be provided by government organisations as a reference to help buyers, but many felt that government would be unlikely to be bold enough to make such statements given the risk of likely legal action. It was also suggested that in a global market, a national authority may not have sufficient weight or trust for a global organisation, particularly given that the role of national technical authorities as both poachers and gamekeepers could create a perception of conflict of interest (even if denied).

Conclusion

While there are undoubtedly many private sector organisations for whom cyber security is not a top priority, there are many company boards who do profess significant concern: in the World Economic Forum Global Risk Survey from November 2018, cyberattacks were rated as the biggest risk to businesses in Europe, North America and Asia. The lack of clarity among buyers as to which security products actually deliver security benefit is a significant barrier to improving the situation.

The chair closed the discussion by seeking a high level summary of practical steps that buyers could take in order improve matters. The resulting conclusions were:

- Firstly, that they should ask the right questions – buyers should question vendors on their security and make it a formal part of the procurement process. Buyers could seek to use commercial mechanisms such as Terms and Conditions to set up the right vendor incentives
- Secondly, get involved in the discussion. The Cyber Growth Partnership (CGP) is a ministerial led group which has launched an initiative to look at how UK Government can support product security assurance, and for this to be productive, the involvement of commercial buyers is critical
- Finally, organisations could take a collaborative approach to addressing market failings by grouping together to resource and fund initiatives that are unaffordable at the level of the individual firm. A more active approach could help to guarantee that their cyber budget is well spent, and their organisation truly protected.

DEBATE SECURITY

Event sponsored by

#becrypt

GARRISON