Former army intelligence analyst and CISO slams proposed cyber reserve force

Dan Raywood

December 04, 2012

The proposed cyber reserve force has been criticised over a lack of preparation and being too reliant on specialists working voluntarily.

Mark Brown, director of information security at Ernst & Young, former CISO of SAB Miller and winner of the 2011 SC award for information security person of the year, said that the creation of the reserve force was not enough to deal with modern cyber issues.

While he welcomed the Government's announcements on the use of private sector capability to help the public sector tackle cyber security risks, he said that a dedicated and full time capability, fulfilling the needs of both private and public sector, working in partnership with those professionals at the 'coalface' in industry as well as the government nerve centres, such as GCHQ, was needed.

Brown said: "However, the creation of a cyber reserve and a UK Computer Emergency Response Team (CERT) does not go far enough. The level of threat continues to grow at a pace that cannot be met through part time action.

"Cyber criminals are redefining the term 'organised crime' and in many respects, are more organised than the community seeking to protect businesses from cyber crime and information security. A reserve force, made up of retired information security professionals, runs the risk of being unable to keep pace with the changing technologies and risk mitigation practices necessary to maintain a strong defence.

"At the same time information security professionals employed in business are unlikely to be able to dedicate the time to provide the necessary support."

Speaking to SC Magazine, Brown referred to the recent Ernst & Young survey, which claimed that UK firms have concentrated on short-term fixes for security problems, rather than looking at overall threats, mainly due to a lack of people with specialist security skills.

Brown said: "In that survey, 85 per cent of UK businesses feel that the information security function is not serving the needs of business. Businesses are fed up with information security not meeting business demands as there is even less time to be giving up time for the government's goal. This is not going to work.

"I understand the case, information security does take time and our team at SAB Miller worked 24/7 across the globe. If you look back at the 1990s and the move to mass outsourcing, most operational IT security was done by system integrators while now it is strategists and 'do-ers' and the skills other companies require from IT security is keeping information secure and understanding where it is outsourced to."

Brown was also critical of the £650 million fighting fund, as he said that this is split across five years and nothing has been seen of it yet, mainly as the achievement aims of the Cyber Security Strategy are the mission statement of GCHQ.

Former army intelligence analyst and CISO slams proposed cyber reserve force

"Is this government getting security done on the cheap?" he asked. "In this time of austerity, is government doing parts that are required? It can only be a stepping stone. This needs to engage the whole of UK plc."

The 'Cyber Reserve' force was announced in a statement from to Francis Maude, minister for the Cabinet Office and Paymaster General, marking the first year of the Cyber Security Strategy. The concept is to draw on the wider talent and skills of the nation in the cyber field.