securityweek.com

Cyber Shield Act: A New Legislative Approach to Improving Cyber Security

Tags: NEWS & INDUSTRY Security Infrastructure

7-9 minutes

The Cyber Shield Act is a legislative proposal designed to cut "to the core of critical infrastructure cyber defense." It is proposed by Senator Edward J. Markey, Massachusetts -- but you won't find a draft bill anywhere yet.

Markey is taking the unusual route of working with the Institute for Critical Infrastructure Technology (ICIT) to test his ideas, locate problems and seek solutions. James Scott, ICIT senior fellow, told *SecurityWeek*, "Sen Markey's office is proposing the Cyber Shield Act, and we are introducing it for them... His office briefed us a few times and we were giving some advice on how they could make it more doable."

Whether it is, in fact, doable remains to be seen. Currently, there are only two sources for further information: a YouTube discussion of Markey taking and answering questions on his ideas; and an analysis by ICIT. Scott is certainly bullish about its potential: his analysis is sub-titled 'Is the Legislative Community Finally Listening to Cybersecurity Experts?'

The proposal is fundamentally different to most cyber security legislation. That legislation often seeks to impose minimum

standards of security behavior on business -- such as the proposed Cybersecurity Disclosure Act of 2017, which will force cyber responsibility into the boardroom.

Instead, the Cyber Shield Act seeks to give the consumers of security products better and more accurate information on which to base their purchasing decisions. With more accurate information informing decisions, the theory is that manufacturers and vendors will build better security into their products. Two particular aspects of the proposed Act highlight this.

The first is a requirement for "security-by-design throughout the development lifecycle of each and every device" in accordance with NIST 800-160. An example, suggests the ICIT analysis, is that at "a bare minimum, manufacturers must harden device security be requiring consumers to change default credentials."

The second is a rating system that will apply measurement criteria or cybersecurity scores to individual devices. Neither of these ideas are new, and both are fraught with difficulty -- and their acceptability is made both simpler and yet more difficult to achieve by Markey's insistence that adherence to the Act's provisions will be voluntary.

It is worth noting that the UK government launched a similar rating approach in 2013, based on the BIS Kitemark. The assumption was that business would rapidly adopt the voluntary scheme in order to demonstrate their quality and gain competitive advantage. David Willetts, minister of state for universities and science, announced at the time, "The cyber standard will promote excellence in tackling cyber risks, help businesses better understand how to protect themselves, and ultimately increase the nation's collective cyber security." It didn't fly. Even the BIS web site does not today display

its own kitemark on its home page.

ICIT is not unaware of the difficulties, especially with the rating system. It points out that even the highest rating will not guarantee security; that new attack vectors not necessarily considered in the original rating will evolve; that 'secure' devices can still be breached laterally from other devices; and that many IT components are manufactured outside of US jurisdiction. Nevertheless, it insists that it is achievable.

"An artificial intelligence system," suggests ICIT, "could even be trained to weigh the data and calculate accurate scores. Instead of a star system (i.e. 4/5, etc.), Cyber Shield might be more meaningful and effective with a confidence score (i.e. there is a 92% chance that this device collects, processes, and transmits data securely). In this manner, consumer action is limited, and consumer understanding (of the background technical processes) is minimized."

Security by design and ratings are not the only aspects of the proposed Cyber Shield Act; but they are perhaps the most difficult. Markey and the ICIT believe they can be achieved between government, NIST experts and the industry. One group not specifically included, however, are the CISOs and other security officers that rely on these products to secure their organizations.

SecurityWeek asked the ICIT if this was an omission, suggesting that perhaps the only group truly qualified and incentivized to adequately promote security are those who depend upon it; that is the CISOs. Legislation has a history of failing to achieve its objectives, while vendors have a history of lobbying government to reduce security requirements.

The suggestion, one in fact proposed by Martin Zinaich, the information security officer for the City of Tampa, is that what is needed is an information security professional association -- much like the medical industry has the AMA of medical practitioners.

Scott replied, "Right now what we need is legislation that makes sense and encourages organizations to be more cybersecurity-centric. This bill includes security by design, industry outreach and education. We do have CISO organizations, but unfortunately, they typically don't have the pull at their organization to do anything significant. This is the most doable legislation for cyber that I've ever seen, and its early enough in the life of it to be shaped and molded properly."

Zinaich, for his part, is not impressed. "This actually requires both ends of the political / practitioner spectrum," he told *SecurityWeek* "Think of the millions of model device types -- who could possibly pull something like this off? Only practitioners working in conjunction with government, to put out a standard and keep it up to date. And do we simply measure things without the infrastructure to correct it and/or keep it on course?"

He added, "I feel a bit like Nostradamus -- I said if the industry didn't professionalize the Government would. James Scott is right in his response to *SecurityWeek*; CISOs do not have the pull needed. And they will unlikely get it until either they professionalize or the government does it for them. Yet, this is another 'voluntary' program, and that is a fail. Information Security is not only the devices, although that is a big part of it, but it is how the devices are installed and used, and how the business is or is not a partner in Information Security."

Zinaich is clear -- business should not be left out of this Act; and it is the CISOs, preferably led by a professional CISO association, that should provide the voice of business.

The proposed Cyber Shield Act is an ambitious project. There will be those, like Zinaich, who will doubt it can be effective. Nevertheless, the ICIT remains positive. "Cyber Shield," it concludes, "could be a catalyst to incite responsible cybersecurity adoption and implementation throughout multiple manufacturing sectors." Time will tell whether Senator Markey, with the help and advice of the ICIT, will succeed in solving the problems involved.

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend: