ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

The Cyber Shield Act

Is the Legislative Community Finally Listening to Cybersecurity Experts?

April 2017

By: James Scott, Senior Fellow, The Institute for Critical Infrastructure Technology

The Cyber Shield Act

Is the Legislative Community Finally Listening to Cybersecurity Experts?

April 2017

Authored by: James Scott, Sr. Fellow, ICIT

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Upcoming Events

The Annual ICIT Forum

June 7, 2017, The Four Seasons Washington D.C.

www.icitforum.org

Visit the ICIT Library to view additional research and publications

https://www.amazon.com/James-Scott/e/B01IPLQKSQ/ref=dp_byline_cont_pop_ebooks_1

Meaningful, solutions-based cybersecurity legislation that cuts to the core of critical infrastructure cyber defense is virtually absent from congressional conversations. As the partisanship tug-of-war eclipses timely and actionable policies, few in Congress have allocated efficient time to consult the experience and guidance of actual cybersecurity experts who are on the frontlines of the public/private digital space. Industry experts and federal agencies such as NSA, NASA and NIST have repeatedly pushed for the implementation and standardization of the bare essentials of Information Security, such as security-by-design, cyber-hygiene training, and layered defenses, to be recognized as crucial topics on the Hill. Until now, this expert guidance and promotion of meaningful action has fallen upon deaf ears in Congress. The Cyber Shield Act introduces meaningful dialog between industry and Congress in a manner that shifts the conversation away from counterproductive, bureaucratic partisanship and that inspires and catalyzes a true and actionable cultural transition towards impactful critical infrastructure cyber resiliency.

The Cyber Shield Act is an excellent idea for improving informed consumer decision making concerning electronic devices that store, process, or transmit data. The crux of the bill will ultimately depend on three things: industry interaction, consumer reception, and effective implementation. Even though the program is voluntary, it will require sufficient incentives to entice industry leaders to participate and drive market forces towards widespread adoption. One way to ensure the development of market forces is to include industry leaders for target sectors in the working group. That said, while industry leaders' input will be valued, considered, and incorporated, the working group should not be led by industry. Doing so could result in a weak framework and meaningless certification or in a lopsided framework that unfairly benefits one organization over others. Organizations may shy away from adhering to best practices because doing so increases their bottom line (hence the current threat landscape). Alternately, large organizations may economically weaponize the framework as an entry-barrier or leveraging point against smaller organizations. Even though Cyber Shield will be voluntary, if it is as successful and widely adopted as hoped, then non-adoption could have considerable economic impact. Ideally, the working group will be driven and led by technology proficient and informed government personnel, such as NIST, or by an objective third-party.

Consumer reception can be the easiest or most difficult aspect of Cyber Shield. The Act would be more impactful if it is preceded by a general cybersecurity and cyber-hygiene education and awareness campaign. NIST, NASA, and other agencies are working on efforts to increase public cybersecurity awareness and training [1] [2]. At the moment, consumers only retroactively care about cybersecurity. They only think about it after an incident or exploitation has already happened [3]. For Cyber Shield to succeed, consumers will need to be retrained to think about long-term cybersecurity at the time of purchase. This is a daunting effort; however, it is a cultural shift that needed to happen years ago but lacked the right fulcrum. An education provision of

Cyber Shield will also provide a significant secondary victory, even if industry does not widely adopt the certification or if implementation proves difficult.

Implementation does not have to be challenging, it just requires creativity and adaptability. The main difficulty with assigning measurement criteria or cybersecurity scores to individual devices is that the threat landscape is fluid. A seemingly secure device one day could become incredibly vulnerable overnight if a vulnerability or exploit is made publicly available [3]. Perhaps worse, inherent vulnerabilities could be covertly exploited by sophisticated adversaries while consumers falsely believe their devices secure due to the Cyber Shield rating [3]. The first step to successful implementation of Cyber Shield is requiring security-by-design throughout the development lifecycle of each and every device, according to NIST 800-160 [2]. At a bare minimum, manufacturers must harden device security be requiring consumers to change default credentials. Rather than devices shipping with default open ports, etc. manufacturers should harden devices as much as possible because the burden of security should not be on consumers. Consumers know little about security and they are paying for a product that they expect to be able to plug in and use without hours of digging through minute settings and hidden menus [3]. Manufacturers should not be permitted to gauge their own devices because that could lead to intentionally undisclosed vulnerabilities and false ratings. The next challenge is to set meaningful criteria for security ratings. NIST and industry leaders can help set technical and non-technical metrics for device security and usability, though objective third-party opinions and public comments are equally as important. One critical aspect to consider is that even secure devices can be breached with the right exploit and enough adversarial determination and resources. Another critical consideration is that many devices are breached laterally from other infected networked devices [4]. Further, every device will have diminishing cybersecurity over time because as it ages, technology advances, its updates become less frequent, etc. [5]. Cyber Shield should embrace these concerns and incorporate the scenarios into a robust metric system. For instance, rather than a certification sticker denoting a specific rank or score, devices can be labeled with a QR code that corresponds to a dynamic database that calculates the score in real time according to the current threat landscape, recent vulnerabilities relevant to that device or software, etc. If Cyber Shield stakeholders include NIST, DHS, ISACs, and industry leaders, then the relevant information can be regularly provided in real time and incorporated into the scoring system. An artificial intelligence system 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. Since many companies manufacture outside the United States or incorporate subsystems and components that were manufactured outside the U.S., rating devices according to security benchmarks and penetration testing should occur post-production (i.e. near at market) on a random sample of devices. The working group or leading commission will need to be notified of any changes in production, in

software, or of any updates delivered to devices. In fact, Cyber Shield could serve as a secure conduit to facilitate update and patch delivery. This ensures that registered connected devices are regularly updated without consumer interaction. Manufacturers benefit from protected reputations, fewer data breaches, and decreased legal fees. That said, the dynamic measurement system and any update channels will need to be secured against cyberattack with the utmost security measures to ensure that ratings are accurate, that no incidental data can be exfiltrated, and to ensure that threat actors do not distribute poisoned updates or malware to connected devices via the network.

Overall, Cyber Shield is an excellent idea and could facilitate a much-needed cultural shift in secure device manufacturing and upkeep (especially if it compels more organizations to incorporate security-by-design throughout the development lifecycle) [2] [3]. The main caveat is that rating electronic devices for cybersecurity is not the same as rating a car for security or a device for energy footprints. Cybersecurity is significantly more dynamic. A determined, well resourced, and sophisticated adversary can compromise any device. Any meaningful and lasting rating system must be built around that fundamental truth. It should be about device resiliency and trust as much as security. Minimizing unnecessary data collection and storage and protecting consumer identity and privacy (especially by eschewing the unnecessary collection of PII) is crucial to protecting consumers from being used as cybersecurity crash-test dummies and cyber-risk bearers for manufacturers that desire all of the profits and none of the liability, risk, or developmental costs. If developed and implemented meaningfully, Cyber Shield could be a catalyst to incite responsible cybersecurity adoption and implementation throughout multiple manufacturing sectors.

ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources

[1] J. Scott and D. Spaniel, "ICIT Bulletin: America is Under Siege: Now is the Time for NASA to Unleash Gryphon-X", Icitech.org, 2016. [Online]. Available: http://icitech.org/gryphonx/. [Accessed: 14- Apr- 2017].

[2] J. Scott and D. Spaniel, "NIST SP 800-160: For the Rest of Us – An ICIT Summary", Icitech.org, 2016. [Online]. Available: http://icitech.org/800160/. [Accessed: 14- Apr- 2017].

[3] J. Scott and D. Spaniel, "ICIT Publication – Rise of the Machines: The Dyn Attack Was Just a Practice Run", Icitech.org, 2016. [Online]. Available: http://icitech.org/icit-publication-the-rise-of-the-machines-the-dyn-attack-was-just-a-practice-run/. [Accessed: 14- Apr- 2017].

[4] J. Scott and D. Spaniel, "The Cybersecurity Show Must Go On: Surpassing Security Theatre and Minimal Compliance Regulations", Icitech.org, 2017. [Online]. Available: http://icitech.org/the-cybersecurity-show-must-go-on-surpassing-security-theatre-and-minimal-compliance-regulations/. [Accessed: 14- Apr- 2017].

[5] J. Scott and D. Spaniel, "ICIT Analysis: Hacking Elections is Easy! Part 1: Tactics, Techniques, and Procedures", Icitech.org, 2016. [Online]. Available: http://icitech.org/publications. [Accessed: 14- Apr- 2017].