DEVELOPING A SEAMLESS NATIONAL CYBERSECURITY POLICY

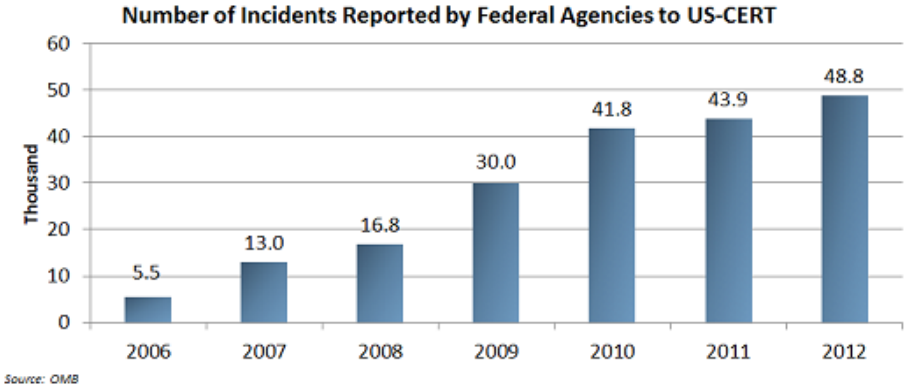
An AIAA Information Paper

ABSTRACT

The American Institute of Aeronautics and Astronautics (AIAA) recognizes that the topic of cybersecurity is a complex and rapidly changing area that involves both policy and technology challenges. Cybersecurity implications impact a variety of areas from Personally Identifiable Information (PII) and identify theft, all the way to threats to our national security through the loss of Intellectual Property (IP) and interruption of key infrastructure and military capabilities. As more industries and segments of our critical infrastructure move applications and key databases online, the potential for intrusion, disruption, or even loss of capability dramatically increases. Additionally, the proliferation of the availability of hacking tools and know how, coupled with a reliance on standard hardware and protocols in the development of critical systems on the ground, in the air, and in space, threatens to increase the amount of backdoors through which systems can be compromised. As the threat from cyber attacks has grown, so has the industry looking to build its business around protecting companies and nation states. Monitoring of key cyber skills and technology, intended to be protective in nature, must be done to prevent their use against the United States, our allies, and our interests, both here and abroad. As usually happens with an industry moving at such a fast pace, resources and policy tend to lag behind the day-to-day developments. While it may never be possible to successfully "get out in front" of the cyber challenges we face, it is imperative to focus on the development of an adaptive, nimble, and seamless national cybersecurity policy.

ISSUE BACKGROUND

Cybersecurity is both an external and internal threat. Individuals and nation states attempt to penetrate systems and either steal information or disrupt operations for both political and economic benefits. Additionally, policies, limited IT resources, and even what vendors we use contribute to the scope and vagueness of the problem. The development and rapid growth of the cybersecurity industry also introduces additional challenges as companies and federal agencies struggle to adapt to changing attacks.



While attacks on the power grid, financial institutions, and retailers have become common place, recent events have pointed to directed attacks against key space-based hardware vital to national security as well as Earth observation. Beyond the denial of use of the platform, there is the potential for lost IP as well as

commanded destruction of the asset. Incidents over the past several years point to increased hacker capabilities as well as vulnerabilities, which, while identified, sometimes are not addressed for months or years. In 2011, the U.S.-China Economic and Security Review Commission issued a report highlighting two incidents, one in 2007 and one in 2008, where "hackers gained access to the satellites through ground control systems at the Svalbard Satellite Station in Spitsbergen, Norway. The attackers gained enough access on one occasion that they could have taken control of one of the satellites, but chose not to do so." Additionally, in 2012, South Korea experienced a protracted cyber attack and GPS disruption that resulted in 553 aircraft flying in and out of South Korea's airports reporting GPS failures, as did hundreds of ships and fishing boats in the West Sea. With both commercial and military operations highly dependent on GPS, protection and reliability are key issues.

Beyond direct attacks by hackers, the introduction of counterfeit hardware and malicious code through an unsecured supply chain introduces additional vulnerabilities that are extremely difficult and costly to monitor. The drive for cost and schedule savings by using off-the-shelf solutions in hardware, software, and protocols has resulted in several examples of compromised hardware and software ending up as part of critical guidance and sensing components of U.S. military hardware, including the F-35 Joint Strike Fighter. Beyond direct purchasing or production of hardware in foreign countries, the global economy and the push for faster and cheaper results leads to multi-level sourcing of hardware and software—usually from the cheapest bidder, which results in questionable and difficult to trace origins.

Being able to address cybersecurity threats will require action on both the policy and technology front. Beyond developing and implementing more secure supply chains, the ability and willingness to share information on threats and compromises openly must be improved and actively supported. Limited resources, both in people and funding, are being spread over multiple groups as each tries to become a significant player in cybersecurity to the overall detriment of industry and the nation. What is needed is a national roadmap as it pertains to cybersecurity issues within the key infrastructure and national security assets, which includes clear and unambiguous policies and procedures for not only addressing internal vulnerabilities, but also those being introduced from external sources.

In addition to policy intended to address acquisition and development issues, the overall support of STEM initiatives geared around cybersecurity must be amplified to the level where sufficient numbers of operators with adequate training and vetting are able to be introduced into the pipeline. For cybersecurity, the workforce pipeline includes people and resources to address issues that have been noted by recent GAO reports and unaddressed for several years, as well as individuals who are able to support defensive and offensive cyber capabilities.

Many aspects of cybersecurity are addressed on an ad hoc basis depending on the particular public or private group's desire for publicity and scrutiny. Aspects of our national infrastructure that the population relies upon to be safe and available at all times are under constant threat of compromise and destruction based upon a possible "cyber Pearl Harbor." As more systems, many of them not designed with cybersecurity in mind, shift to network-based operations, band-aided security will not be sufficient to prevent determined parties from accessing the information. Beyond attacks, the introduction of backdoors through software and hardware add additional points of access to our infrastructure and key national security assets. Collaboration and cooperation must occur across all levels of the private and public industry to develop policy, technology, and operations to address the ever-growing threat from cybersecurity.