Input to the Commission on Enhancing National Cybersecurity

Christopher W. Folk

National Institute of Standards and Technology

[Docket Number: 160725650-6650-01]

Information on Current and Future States of Cybersecurity in the Digital Economy

Comments Due: September 9, 2016 5:00 PM Eastern Time
Submission: cybercommission@nist.gov

Christopher W. Folk is a third year student at Syracuse University College of Law. Christopher is a Research Assistance for Professor William C. Snyder who works within the Institute for National Security and Counterterrorism (INSCT). The views and opinions of this are the author's alone. All of the opinions expressed herein are solely and wholly those of Christopher and do not reflect the official policy, or position of INSCT, SU College of Law, or Professor Snyder. Assumptions made within this analysis are not reflective of INSCT, Syracuse University College of Law, or Professor Snyder.

INTERNET OF THINGS

The phrase "Internet of Things" was first used back in 1999 by Kevin Ashton while giving a presentation on radio frequency identification ("RFID") at Procter & Gamble.[1] With the advent of smartphones, implantable medical technology, smart appliances, self-driving cars, smart-wearable devices, drones, etc., the IoT has become a reality as we live in a world filled with "connected" devices. Information flows into and out of these devices via various proprietary and open protocols and each of these information flows carries with it cybersecurity challenges.

CURRENT AND FUTURE TRENDS AND CHALLENGES IN THE INTERNET OF THINGS

As the size of devices decrease and their ubiquity increases it becomes increasingly difficult to "bake" in security protocols to tiny chipsets where cost and functionality are often primary drivers. We live in a world where people just want their devices to function and to work with each other and security is often seen as a roadblock or hurdle which must be managed in order to achieve interoperability. So long as security is an afterthought or an add-on and is not a seamless and cohesive element of a product or protocol users will continue to circumvent security and choose usability, and functionality over security. This sets a dangerous precedent and may result in information leaks and exfiltration merely because the user "just wants it to work" and presumes that the device hardware and software will make everything "secure enough."[2]
This is of even greater concern in the area of implantable medical devices where remote monitoring and control are possible. Here, these devices which are critical to basic life functions (e.g. a pacemaker with built-in defibrillator) are designed for near field communication and remote access capabilities so that health-care professionals can make changes without the need for a surgical procedure. Therefore, the implementation of solid, robust security protocols in

[1] Kathleen Aguilar, *Getting up to Speed on the Internet of Things*, ACC DOCKET, October 2015, at *27.

[2] Daniel E. Harmon, *Keeping an Eye on the IOT in the Balance: Convenience vs. Privacy & Security Threats*, LAW. PC, Nov. 1 2015, at 1.

these devices could literally mean the difference between life and death.[3] Additionally, the data that is generated by IoT devices is fast becoming the new currency as we dive deeper into and embrace the information age, individuals, companies, and governments are deeply invested in the harvesting and extraction of data that can be used to create relevant, and meaningful information.

PROGRESS BEING MADE TO ADDRESS THE CHALLENGES

In the realm of implantable medical devices, NIST revised the standards for infusion pump cybersecurity guidance in 2016.[4] This was a good first step however it might be more prudent to take a step back and try to envision a world where information is the most paramount item and every precaution should be taken to 1) secure information flows; 2) establish trusted identities; and 3) permit information exchanges only between trusted identities. The truth is, that is the world we live in, where information can be leveraged for a myriad of reasons and information then becomes the core needed to access command and control systems.

THE MOST PROMISING APPROACHES TO ADDRESSING THE CHALLENGES

There has been generous debate with respect to encryption and the myriad issues that use of and obfuscation through it raise. However, in the context of IoT devices, basic encryption should be viewed as the most basic and fundamental step. This will not prevent every breach or attack but would serve to limit the vulnerabilities and should be baked into the IoT products. It is no longer sufficient to ask "why would anyone want to access this" as we must now ponder "how and when will they try to access or manipulate this device?" Furthermore, there has been some discussion that IoT devices should not actively listen on any ports and that communication should be initiated directly from the IoT device. This would eliminate a huge vulnerability and would ensure that the IoT device has performed at least base-level trust in order to initiate

[3] Mathias Cousin, Tadashi Castillo-Hi, & Glenn Synder, *Devices and Diseases: How the IoT is Transforming MedTech*, Deloitte University Press (Sep. 11, 2015), http://dupress.com/articles/internet-of-things-iot-in-medical-devices-industry/.

[4] Marianne Kolbasuk McGee, *Why NIST Is Revising Infusion Pump Cybersecurity Guidance* (Mar. 7, 2016), http://www.healthcareinfosecurity.com/interviews/nist-revising-infusion-pump-cybersecurity-guidance-i-3094?rf=2016-03-09-eh&mkt_tok=3RkMMJWWfF9wsRonvq3Kd%2B%2FhmjTEU5z16esrWKC0hIkz2EFye%2BLIHETpodcMTcFqNb%2FYDBceEJhqyQJxPr3FKdENwM10RhPhDw%3D%3D.

communication and data exchange. In so doing, the use of encrypted links and anti-spoofing protocols will also help maintain reliable and secure communication links from and to the IoT device to the "trusted" entities.

WHAT CAN OR SHOULD BE DONE NOW OR WITHIN THE NEXT 1 - 2 YEARS TO BETTER ADDRESS THE CHALLENGES

In the short-term, it is vitally important that security is put in the same position of relevance as price, and performance. Security has to have a place in the balancing equation so that companies can make conscious, well-reasoned decisions in the context of threats versus the bottom line. Thus, a short-term solution could be to limit the protocols used by IoT devices so that only near-field communication is possible over very short distances. This could decrease the ability of remote access or exfiltration while still balancing this with the need to input and extract information from IoT devices. Additionally, standards must be developed in such seemingly innocuous areas such as units of measure and time. With the worldwide production and use of IoT devices the lack of clearly defined standards could raise interoperability issues which will frustrate adoption and potentially prevent universal security protocols from being implemented.

WHAT SHOULD BE DONE OVER THE NEXT DECADE TO BETTER ADDRESS THE CHALLENGES

In the longer term scenario, IoT devices should be categorized and security applied accordingly. Some IoT devices will pose minimal information and cybersecurity risks, such as smart-appliances; others will have greater cybersecurity needs (e.g. smart thermostats/HVAC controls which could significantly impact a residential or commercial user), while still others will be deemed critical (e.g. implantable medical devices, IoT components in vehicles and manned and unmanned systems). As above, if every IoT device minimally uses end-to-end encrypted communication links and also requires that all communication be initiated by the IoT device, that may address the majority of the needs for the lower tier devices (e.g. appliances). Whereas, as one moves up the tiers towards the more critical IoT devices additional cybersecurity measures must be implemented.

IoT Device Categories:

- Tier I: Low Risk – devices such as smart appliances with access to and use of minimal information
- Tier II: Medium Risk – HVAC Controls, Home Monitoring Systems – devices that pose more significant risks to consumers and end-users
- Tier III; High Risk – implantable medical devices, manned/un-manned vehicle systems – significant risk to the population and/or end-users in the event of a security breach. Information may also be particularly sensitive.

Here too, it will be essential that cybersecurity is the default and requires no continual user interaction. In scenarios where the user is required to modify settings or update firmware, the device would be vulnerable and this should be the exception, not the norm in the world of IoT. To effect this, a model such as that used by major software vendors that involve updates tied to hardware IDs would ensure that the IoT device communicates securely, receives update(s) and self-upgrades and installs them devoid of user interaction. Given the criticality of some of these IoT devices, the software should be modularized such that security components can be updated independent of core OS functions. Consequently, allowing for remote software/firmware updates should be handled similarly to the way major hardware and software vendors do this currently. Software downloads and updates are linked to hardware IDs such that the IoT device software and firmware can be updated in a trusted exchange of information. Furthermore, either on or off chip modularization should be implemented such that security functions are separated from core OS functions so that security-related updates can be automated and remain independent of actual device functions. This would be particularly important in sensitive applications such as implantable medical devices and when deployed within vehicle systems or in grid applications (any Tier III device).

FUTURE CHALLENGES THAT MAY ARISE AND RECOMMENDED ACTIONS THAT INDIVIDUALS, ORGANIZATIONS, AND GOVERNMENTS CAN TAKE TO BETTER POSITION THEMSELVES TO MEET THOSE CHALLENGES

The growth rate and adoption of IoT devices is seemingly exponential as the number of applications where IoT can be introduced continues to rise. That being the case it is of paramount importance that security considerations be examined now as even at this stage of the IoT movement, there are a staggering number of unsecured and potentially unsecureable IoT devices within the marketplace. Consequently, it will be necessary to develop standards and frameworks and to categorize IoT device types so that more critical uses are required to have greater security protocols active with controls in place to prevent circumvention by end-users.

Individuals: will have to take more active roles in order to ensure that they understand the role IoT devices play within their lives and also understand the inherent risks and agree to hold manufacturers free from liability with respect to IoT data breaches. As litigation in the area of data breaches, continues to rise, a failure to absolve manufacturers of IoT data breach liability could prove disastrous to continued development and deployment efforts.

Organizations: in order to reduce liability organizations should take advantage of The Cybersecurity Information Sharing Act (CISA) of 2015 and enter into information-sharing agreements so that in the event that end-users or systems integrators have not limited companies' liability the companies can obviate this by utilizing information sharing under CISA 2015 to remove or reduce their liability for incidents.[5] Organizations will also need to ensure that their use of IoT is included within their IT policies and security protocols so that those IoT devices that are either nefarious or not yet in compliance (based on the suggestions in the previous sections) are unable to have a deleterious impact on an organization and are also unable to serve as conduits through which data exfiltration can occur. Here, just as the case where the IoT device should be required to initiate communication, a trusted broker within the network should be implemented to ensure that information flows to/from IoT devices are both trusted and sanctioned.

Governments: need to take a much broader role for in most instances, just as with organizations they will have multiple functions, as either users, or regulators, or in some cases manufacturers of IoT devices. Furthermore, governments have a far greater stake in a regulatory sense given the wide-ranging application of IoT devices within various branches of government, within critical infrastructure, as well as potentially the use of implantable IoT devices within key government personnel which raises national security considerations. Therefore, government

[5] Christopher W. Folk, *The Cybersecurity Information Sharing Act of 2015*, Feb. 2., 2016, http://blog.cybersecuritylaw.us/2016/02/02/the-cybersecurity-information-sharing-act-of-2015/ .

actors must be cognizant of the potential ramifications that a disruptive technology such as IoT may bring and standards and regulations must be developed and implemented to provide safeguards at multiple levels: 1) government and agencies therein; 2) grid and critical infrastructure; 3) in applications involving manned and unmanned systems; 4) within organizations – regulating the use and dissemination of information gather by or from IoT devices; 5) in consumer applications to help safeguard end-users. To effectuate this, both the Executive Branch as well as the Legislature will need to understand the cybersecurity concerns with respect to IoT and will need to develop rules and regulations within the Administrative Agencies and statutes and directives within the Legislative branch to create a common, and cohesive approach towards cybersecurity in general and specifically in its application within the realm of IoT. In so doing, the various agencies that have touch points (which ultimately may prove to be nearly every current Administrative Agency) will operate under a common theme with a common goal in mind. Otherwise, a scattered and independently adopted approach will provide holes and vulnerabilities within the IoT cybersecurity framework which will encourage and promote exploits. Ultimately, a lead agency should be designated or in the alternative a cabinet level position should be created solely focused on cybersecurity. While the Cyberspace Policy Review conducted in 2009 concluded that an executive branch cybersecurity coordinator should be implemented, in 2016 this has still not taken place.[6] In an effort to create a unified strategy with respect to cybersecurity this should be revisited as the various branches of government will necessarily end up looking to the executive branch to investigate, research, and report on the creation of a unified cybersecurity policy.

CRITICAL INFRASTRUCTURE CYBERSECURITY

CURRENT AND FUTURE TRENDS AND CHALLENGES IN CRITICAL INFRASTRUCTURE

The Department of Homeland Security includes a number of items within the critical infrastructure sector which include the following high-level areas:

- Chemical Sector

[6] *The Comprehensive National Cybersecurity Initiative*, White House Briefing Room, https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (last visited September 8, 2016).

- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

[7] As evidenced by the broad range of topic areas it is possible that the Executive branch could treat almost any incident as impacting critical infrastructure based on its inclusion within any of the expansive areas noted by DHS. In the absence of a clear and hierarchical structure within which cybersecurity falls, a number of agencies could be involved including both DoD and civilian facing which has additional implications in the context of a response to a domestic-based cyber incident.

PROGRESS BEING MADE TO ADDRESS THE CHALLENGES

The fact that all things cyber are now at the forefront of media coverage more and more attention is being paid to this growing area and both the White House as well as legislators are beginning to take steps to better understand the implications of our current and future vulnerabilities in a cyber world. If we confine the discussion merely to critical infrastructure with respect to energy, it becomes clear that the energy sector is vulnerable and these vulnerabilities have been exploited in the global context. For instance, the targeting of Ukraine's power grid in December of 2015 was in many respects a wake-up call for the Dept. of Energy.[8] However, the Department of

[7] The Department of Homeland Security: Critical Infrastructure Sectors, https://www.dhs.gov/critical-infrastructure-sectors (last visited Sept., 8, 2016).

[8] Christopher W. Folk, *Cyber Round Up: … US Assisting Ukraine Investigate Electrical Grid Hack*, http://blog.cybersecuritylaw.us/2016/01/20/cyber-round-up-japan-hosting-white-hat-

Energy's $34M initiative to improve cybersecurity in critical infrastructure may be indicative of the relative lack of importance that is being applied to securing vital resources such as our grid infrastructure.[9] Additionally, a report released by MIT in 2011 "The Future of the Electric Grid" underscores the potentially lethal ramifications of a cyberattack on the North American power grid.[10] In discussions with high-ranking persons within the Utility Sector, it is clear that cybersecurity is of growing importance however it is unclear what if anything has actually been done beyond research and training to ensure that our grid infrastructure is protected against cyberattacks.

THE MOST PROMISING APPROACHES TO ADDRESSING THE CHALLENGES

To begin, let us discuss approaches that are neither novel nor promising. Namely, recent legislation introduced in the Senate in 2016 called for a return to analog devices in grid infrastructure in order to sidestep potential cybersecurity issues.[11] A move such as this to regress to equipment from decades long since past, could represent a very limited and short-term solution to cybersecurity issues. This, however, is neither a logical nor responsible approach towards securing and reducing the vulnerabilities facing our grid infrastructure. The anticipated cost of moving to analog devices has been pegged at $10M and the process of identifying devices that could be replaced with analog versions would take nearly two years, hardly a worthwhile endeavor.

This is contrasted with most major utility companies which have, or are in the process of bringing security and specifically cybersecurity experts into their organizations. Traditionally, as

hackers-to-test-security-systems-us-government-slow-to-upgrade-cybersecurity-protections/ (last visited Sept., 8, 2016).

[9] Christopher W. Folk, *Cyber Round Up: DOE and MIT Sloan Partner up for Grid Security*, http://blog.cybersecuritylaw.us/2015/10/23/cyber-round-up-doe-and-mit-sloan-partner-up-for-grid-security-dod-needs-to-focus-its-hiring-efforts-uscg-rdml-thomas-on-port-security/ (last visited Sept. 8, 2016).

[10] *The Future of the Electric Grid*, Massachusetts Institute of Technology, http://blog.cybersecuritylaw.us/wp-content/uploads/2015/10/Electric_Grid_Full_Report.pdf (last visited Sept., 8, 2016).

[11] Christopher W. Folk, *Cybersecurity Law and Policy, Two Steps Forward – One Step Back*, http://blog.cybersecuritylaw.us/2016/06/21/two-steps-forward-one-step-back-the-reintroduction-of-retro-devices-to-improve-grid-security/ (Jun 21, 2016).

industries have increased their reliance on and use of technology those outside the core IT sector have paid scant attention to cybersecurity. However, as we continue to see cyber incidents that target critical infrastructure these organizations are quickly realizing that their reliance on technology necessitates cybersecurity and that is promising given the enormous exposure facing these industries as they transition from mere users of technology to experts in the implications of said use.

WHAT CAN OR SHOULD BE DONE NOW OR WITHIN THE NEXT 1-2 YEARS TO BETTER ADDRESS THE CHALLENGES.

Perhaps the most critical near-term initiative will involve a complete audit and assessment throughout our critical infrastructure entities to understand the following:

1) How do we define and characterize critical vs. standard infrastructure;
2) What vulnerabilities exist within the cyber context;
3) Within each sector, which agency(ies) have oversight authority;
4) Within each entity what has been done in terms of cybersecurity.

A comprehensive audit and assessment will provide a baseline within which a continuous improvement process should be initiated such that the assessment, feedback, and corrective action loop is repeated ad infinitum. Given that this is within the short-term timeframe, merely completing the initial assessment should be finished within the 1-2 year timeframe. This information though likely highly proprietary in nature should be shared with the agency that has regulatory oversight.

In addition to bringing in cybersecurity professionals and the addition of cyber experts within the C-Suite, those that provide critical infrastructure services are going to have to work together given the interconnected nature of infrastructure, such as the grid. Within this short-term the implementation of fail-safes and the ability to segregate grids should be undertaken. Where it is possible that an “event” could overload a portion of the grid and result in local outages that then proceed in a domino fashion to cause rolling blackouts throughout the grid, fail-safes should be developed to prevent such a scenario. This is somewhat analogous to controlled burns and firestops that allow or even facilitate the loss of certain areas in order to forestall even greater and more widespread damage. Here, an increased reliance on technology and smart devices could allow for more instantaneous information and the ability of integrated systems to develop a singular view of the entire grid infrastructure such that automated heuristic decisions could be implemented to shutdown interconnections and prevent a series of coordinated outages from overloading and disrupting the grid system.

Also, in the short-term, while the movement to an intelligent monitoring and management system is underway there will also need to be physical security to augment the virtual/cyber security. Here an educated workforce, as well as an actual security presence will be necessary to help ensure that neither a cyber nor a physical attack could result in the degradation of the entire grid with the enormous resulting impacts.

WHAT SHOULD BE DONE OVER THE NEXT DECADE TO BETTER ADDRESS THE CHALLENGES

As a long-term solution, the use of artificial intelligence may supplant and eventually replace heuristic-based systems to monitor and manage the grid infrastructure. The interfaces will have to be standardized so that all interconnections can be managed irrespective of the actual energy producer or the transmission medium.

As the autonomy and intelligence of the command and control systems increase, it may be possible to scale back the physical security presence. Where an event at one or more physical locations could be automatically managed without intervention, the use of a local response force may be sufficient to preclude the use of a preventative force.

The use of tabletop exercises which simulate ongoing and coordinated attacks on multiple critical infrastructure entities will help ensure that various scenarios are researched and simulated so all of the touch points are fully exercised in a variety of scenarios. It will not be sufficient for a single entity to operate in a vacuum given the interconnected nature of critical infrastructure, therefore, cooperation and coordination will be required in order to fully understand the potential impact that vulnerabilities pose in cases ranging from small-scale isolated incidents to large-scale, widespread intentional service disruptions.

FUTURE CHALLENGES THAT MAY ARISE AND RECOMMENDED ACTIONS THAT INDIVIDUALS, ORGANIZATIONS, AND GOVERNMENTS CAN TAKE TO BETTER POSITION THEMSELVES TO MEET THOSE CHALLENGES

This is another situation in which there is asymmetry between those countries or entities that have the greatest reliance on technology and the actors that could potentially prove disruptive. Where either a nation-state or a group operating in the middle of nowhere with a generator and a high-speed internet connection could potentially initiate a cyberattack against our critical infrastructure systems. Our ability to use offensive cyber weapons to disrupt their entire system and or their internet connection pales in comparison to the amount of damage that such an incident could inflict on US critical infrastructure.

Individuals: In terms of critical infrastructure, the individual's role is somewhat limited except in terms of those individuals that are in the workforce within said industries. Thus, workforce education presents a challenge, as was theorized in the Stuxnet attack, merely bringing a drive in and plugging it into an air-gapped systems resulted in a catastrophic failure. Education is vital so that individuals understand the vulnerabilities and work to mitigate those by practicing prudent and reasonable cybersecurity practices.

Organizations: these are essentially the "boots on the ground" they operate in the day-to-day operations and benefit from and incur the liability of their pervasive use of technology. These entities must continue to assess their vulnerabilities, their adoption of new and emerging technologies and their ability to continue to provide critical services in the presence of and in spite of ongoing attack scenarios.

Governments: ultimately, government oversight is likely to be necessary in order to encourage private entities to co-operate with one another and engage in information sharing. Here, as with CISA 2015, providing incentives to entities to share information and develop repositories can be done by providing incentives in the form of complete or qualified immunity from civil liability arising from cyber incidents when the entities are leveraging information-sharing. This may be a small price to pay in order to facilitate the open exchange of information between the players within the critical infrastructure area. This is also something that only the government is in a position to provide and should do so in support of the greater good.

CYBERSECURITY WORKFORCE

CURRENT AND FUTURE TRENDS AND CHALLENGES WITH THE CYBERSECURITY WORKFORCE

This is a significant issue both within the US and in the global context as well. Current estimates indicate that there are over 200K unfilled jobs in the cybersecurity sector within the US today and an expectation that 1.5M jobs in this sector will be unfilled globally by 2019.[12] While a number of institutions of higher learning have put together "cybersecurity" programs many of these merely include one or two courses in cybersecurity and are still primarily focused on general computer science principles. The real impetus needs to be with K-12 institutions that are able to help young minds develop a cybersecurity perspective that pervades their daily lives and provides them with the necessary skill sets to maintain personal "cyber-safety" or to join the cybersecurity workforce either immediately upon completion of secondary education or post-university or certificate programs. The challenges then are in getting traction within the K-12 institutions and in helping young students understand the rationale for gaining a better understanding of proper cyber-hygiene as well as the significant career possibilities that exist within this realm.

PROGRESS BEING MADE TO ADDRESS THE CHALLENGES

The advent of programs in post-secondary education is promising. So too, are various K-12 initiatives being promoted by the National Integrated Cyber Education Research Center (NICERC) as well as the National Security Agencies (NSA) Gen-Cyber summer camps. All of these are targeting educational opportunities to provide training and development both to generate interest in and ultimately consumption of cybersecurity training.

THE MOST PROMISING APPROACHES TO ADDRESSING THE CHALLENGES

The fact that institutions are moving to address the growing need for a cybersecurity workforce is encouraging. Attacking this from an educational perspective is a logical and reasonable approach to creating a cybersecurity workforce and offers both opportunities and outlets for individuals that have an interest within this discipline. Additionally, the fact that many K-12 institutions have formally adopted Science, Engineering, Technology, and Math (STEM) programs demonstrates that K-12 is dynamic and willing to adopt new curriculum models that it deems relevant to the education of our youth. Cybersecurity fits nicely within the STEM framework, the key will be to ensure that it receives equal footing with the STEM offerings and is not merely relegated to a subservient role within one of the existing STEM prongs. Perhaps C-

[12] Steve Morgan, *One Million Cybersecurity Job Opening in 2016*, Jan 2., 2016, http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#7a183f997d27.

STEM would provide the proper recognition due the new cyber prong within the existing STEM framework.

WHAT CAN OR SHOULD BE DONE NOW OR WITHIN THE NEXT 1-2 YEARS TO BETTER ADDRESS THE CHALLENGES

The continued expansion of intensive educational outlets such as the Gen-Cyber camps should be rapidly expanded both to provide exposure to and experience with cybersecurity but also should help target the immediate workforce needs by specifically targeting high school and college level juniors and seniors. Since there are a wide-variety of open cybersecurity positions, the ability to extend information outreach and help recruit individuals into these unfilled jobs could have an extremely positive impact. The immediate development of a workforce induction system that is roughly analogous to an apprenticeship program provides the ability to engage in on-the-job-training while evaluating and developing candidates for roles of increased responsibility. This is a shorter-term solution that could be used to engage students that have interests in cyber and could be slotted into positions to help fill the currently 200,000 open cyber positions.

WHAT SHOULD BE DONE OVER THE NEXT DECADE TO BETTER ADDRESS THE CHALLENGES

The continued use of the aforementioned apprenticeship-type program could be enhanced by providing core curriculum changes throughout the US educational system to ensure that cybersecurity is a core subject and is similarly situated with subjects such as biology, English, physics, etc. The addition of standardized testing developed with industry input would also help to develop a workforce-ready pool of high school graduates. While the traditional approach is to produce well-rounded individuals that are prepared to enter higher learning, the changing dynamics of the composition of US and worldwide job opportunities lends itself well to the adoption of industry involvement in determining which skills should be developed within the K-12 setting.[13]

[13] The presumption here is that industry involvement in the K-12 system is largely atypical while higher-education in its self-sustaining interest necessarily works to develop curriculum and training that is reflective of the current or anticipated workforce needs.

Within advanced education, cybersecurity should become a discipline wholly distinct from computer science. This would allow students to focus on cybersecurity and to then specialize in specific areas (for instance, a cybersecurity major could include minors in computer science, law, and policy, government administration, business management, etc.). The benefit here is that while cybersecurity is any many respects broad, the ability to develop a cyber workforce that is specifically tailored to certain areas would help reduce the transition period into the workforce and would also help organizations immediately leverage these newly minted cybersecurity experts within their specific industries (or in the public sector).

Additionally, displaced workers or mid-career persons should also be targeted as they could provide a rich pool of individuals that have broader life experiences and could provide a large pool of potential cyber workers. This is an area where the current industry and government-expertise could serve as the basis for continued workforce development where only core development is needed as these individuals are either current or former workforce professionals with the ability to operate in such a setting. With such enormous demand and a proper screening process, this targeted education could result in a near 100% placement rate which is far in excess of traditional workforce development programs that target displaced workers.

FUTURE CHALLENGES THAT MAY ARISE AND RECOMMENDED ACTIONS THAT INDIVIDUALS, ORGANIZATIONS, AND GOVERNMENTS CAN TAKE TO BETTER POSITION THEMSELVES TO MEET THOSE CHALLENGES

With the anticipated shortfall in the supply of cybersecurity professionals, the ability to meet this demand will continue to be an issue. The introduction of a cyber curriculum within the K-12 setting and also in higher learning will be a good step towards acknowledging and beginning to address this issue. This coupled with an attempt to target individuals that have either been displaced or merely decided to discontinue searching for employment could have an extremely beneficial impact. It could be possible to diminish the gap between the current supply of cyber professionals and the demand while simultaneously increasing the overall US workforce participation.

STATE AND LOCAL GOVERNMENT CYBERSECURITY

CURRENT AND FUTURE TRENDS AND CHALLENGES IN STATE AND LOCAL GOVERNMENT

As with nearly every other entity, State and Local governments (State_Local) find themselves embroiled in cybersecurity in spite of their general lack of knowledge or expertise in this area. While most States and many localities have adopted cybersecurity policies the truth is that the public sector is having, even more, difficulty obtaining cyber talent as the private sector generally offers better pay, greater visibility and often is able to incentivize the "best and brightest". One potential workaround is the possibility of increasing educational opportunities for a cyber workforce and also tying educational grants to public-sector service commitments following training.[14]

PROGRESS BEING MADE TO ADDRESS THE CHALLENGES

State_Local governments seem to minimally grasp the importance of cybersecurity knowledge. They are only just beginning to realize that all of the information they compile and store with respect to citizens could make them rich targets of opportunity. Since understanding and acknowledgement is an important first-step the fact that many State_Local entities have reached this point marks positive, albeit minimal progress.

THE MOST PROMISING APPROACHES TO ADDRESSING THE CHALLENGES

Since this is still very much in the nascent stage and even the Federal government has not really risen to the challenge, there seems to be an overall lack of promise within State_Local in rising to meet the cybersecurity challenges. However, as stated above, the very fact that media attention has focused on cybersecurity issues and several municipalities have had issues in this area has raised awareness and State_Local discussion is taking place in the area of cybersecurity.

[14] Bret Brasso, *How State and Local Governments Can Solve Their CyberSecurity Staffing Shortage*, Feb., 17, 2016, https://www.fireeye.com/blog/executive-perspective/2016/02/how_state_and_local.html.

WHAT CAN OR SHOULD BE DONE NOW OR WITHIN THE NEXT 1-2 YEARS TO BETTER ADDRESS THE CHALLENGES

A recurring theme: education and training. It will be important to develop a framework for State_Local governments so that they understand what cybersecurity means at a high level, and that they also realize the types of information they collect, retain, and use, and what their responsibilities and liabilities are with respect to the collection, retention, and safeguarding of this data. Additionally, it is impractical for local governments to procure and retain cybersecurity professionals, therefore State government should step in and identify and broker outsourcing using Virtual Chief Information Security Officers (CISO), and virtual Security Operations Centers (vSOC) that could be utilized by local governments. In outsourcing, they may be able to take advantage of economies-of-scale and municipalities will not be put in a position where they have to evaluate and retain cybersecurity professionals when it is likely that no single person at that level of government has either the expertise or general knowledge required to understand their needs let alone has the ability to properly vet and assess potential candidates.

WHAT SHOULD BE DONE OVER THE NEXT DECADE TO BETTER ADDRESS THE CHALLENGES

Once additional steps are taken to develop a cybersecurity workforce and so long as local governments are able to utilize vSOCs for their cybersecurity needs that piece of the equation should be satisfied. However, from a longer-term perspective, retaining local resources and the quest for autonomy may make a compelling argument for adding a CISO at the local level to maintain oversight of the vSOC. This is likely not feasible in the short-term and even in the next decade may be unrealistic for all but the largest local government entities.

Here too, a continuous improvement loop should be implemented that includes assessment, feedback, and corrective action. Training and education for local and state government employees and contractors will be essential for effective long-term management of cybersecurity issues. While insider risks are pervasive across the landscape and ordinarily represent the greatest cybersecurity risk, within a local or state government this can be exacerbated by the hierarchical nature of most government organizations which is public knowledge and freely available. Thus, social engineering or phishing campaigns can be augmented by open, and public organizational information that can be leveraged to identify relationships and would allow attackers to leverage valid employee credentials to gain unauthorized access.

FUTURE CHALLENGES THAT MAY ARISE AND RECOMMENDED ACTIONS THAT INDIVIDUALS, ORGANIZATIONS, AND GOVERNMENTS CAN TAKE TO BETTER POSITION THEMSELVES TO MEET THOSE CHALLENGES

We have seen a rise in the "hacktivist" who is more interested in social change and awareness than in personal financial gain or mere curiosity. Traditionally, hacktivists have targeted larger corporations or higher level government (e.g. federal), it is likely that hacktivism will extend its reach into State and Local governments as well. Consequently, it will be important for State and Local governments to be cognizant of the vulnerabilities that they face and the potential motivations. While organizations and individuals may face cyber-attacks that are focused on pecuniary gains, State and Local governments may be targets merely for their stance on certain issues, or as drivers for social change. Consider the power that social movements such as the "hippies" could have had in a cyber world where a virtual sit-in could be performed as a distributed denial-of-service attack that prevents authorized access to resources and disrupts standard operations. As protesters hold hands and unite to gain attention and direct others to their cause, so too could a cyber-attack against a State or Local government illicit empathy and give rise to coordinated incidents with more far-reaching implications.

OVERARCHING CHALLENGES

EMERGING TECHNOLOGY TRENDS AND INNOVATIONS: THEIR EFFECTS ON BOTH THE DIGITAL ECONOMY AS WELL AS CYBERSECURITY

The movement to a completely connected world is a testament to IoT and the vast amount of information flows within our daily lives. This coupled with increased research directed at artificial intelligence in areas such as self-driving vehicles further underscores the movement to a truly digital economy. An economy in which information is the universal currency and where the ability exists to extract and analyze data from across the globe, the vulnerabilities in a connected-world are quite staggering. Consider the use of IoT devices that lack proper cybersecurity and can be leveraged in a sort of bot attack that allows data hops between IoT devices so that even air-gapped systems could prove vulnerable if persons with insulin pumps or defibrillators are in the vicinity. As each of these IoT devices represents an active, open port through which traffic can be routed or information exfiltrated, the potential impacts are overwhelming. So too, in the context of a generation of people that have known no other world than the one in which we currently exist, a world with always-on instant communication. For these people, their connection to technology is persistent and pervasive and they will take advantage of hacks, tricks, and tips to circumvent cybersecurity protection merely to stay online and connected in such trivial aspects as social media for instance. Where these individuals lack a healthy respect for cyber hygiene we will continue to experience cybersecurity breaches.

ECONOMIC AND OTHER INCENTIVES FOR ENHANCING CYBERSECURITY

As we continue to rely on technology for nearly every aspect of our lives and as we move to a "cash-free" society, the potential for disruption abounds. Merely taking payment processing systems offline during the holiday season could result in significant issues for companies, suppliers, employees, local governments, all of which rely on instantaneous and continuous fund flows between institutions. If you were to couple an outage for the major payment processers with a coordinated DDOS aimed at ATM networks during the post-Thanksgiving shopping period stores would be overwhelmed, customers would have meltdowns and in many areas local pockets of rioters and potentially looters would arise when faced with an inability to complete transactions. This would overwhelm local law enforcement and would quickly reach critical mass with significantly far-reaching impacts. Therefore, there are enormous economic incentives for enhancing cybersecurity when a country such as ours becomes reliant upon technology any scenario where technology fails due to a cyberattack would include short-term impacts but also longer-term due to a loss of trust and faith in the system. This could have a ripple-effect within the economy.

There are of course myriad other incentives for enhancing cybersecurity. One is the mere fact that our citizens' information should be safeguarded and in a digital world more and more IP is also digital and a lack of cybersecurity could result in IP theft, and also PII on or citizens could be used to build dossiers in order for outside entities to exert internal influence within the US without ever having to physically enter our borders. Thus there are National Security concerns, Corporate concerns, a potential reduction in incentives for companies to invest in research and development, the touch points are numerous and widespread.

GOVERNMENT-PRIVATE SECTOR COORDINATION AND COOPERATION ON CYBERSECURITY

CISA 2015 begins to address this by encouraging and promoting cybersecurity information sharing. This should be further expanded to allow government-private sector collaboration on efforts to promote greater cybersecurity within the US. Increasing cyber-hygiene helps safeguard our data and our resources and leveraging expertise developed both in the government as well as the private sector is a sound approach towards improving our overall cybersecurity posture. This should be done by continuing to incentivize and by building close working relationships so that the government and private industry can engage in a symbiotic relationship where not only does each party benefit, but so too does the country as a whole.

THE ROLE OF THE GOVERNMENT IN ENHANCING CYBERSECURITY FOR THE PRIVATE SECTOR

Given our internal policies with respect to cybersecurity, there are many agencies within the executive branch and the DoD that have developed extensive expertise in cybersecurity. Thus, one could argue that the government should be responsible for disseminating this information to the private sector in order to provide them with the copious amounts of information related to cybersecurity. Certainly it makes economic sense to provide citizens and companies operating within the US with cybersecurity information and tools to allow them to take advantage of the taxpayer funded expertise that exists.