Input to the Commission on Enhancing National Cybersecurity: Submissions by XAHIVE International LLC.

The following feedback has been prepared by XAHIVE International LLC, a cybersecurity company based in New York, for the Commission in Enhancing National cybersecurity. This document draws on XAHIVE's expertise and experience in the field of cybersecurity knowledge including references to research and suggestions from other experts in the field. XAHIVE believes that our input will enable policy decisions related to enhancing national cybersecurity.

Critical Infrastructure Cybersecurity

The status quo

- Statistical evidence demonstrates that there is an increase of cyber-attacks over the last few years on critical infrastructures and on Supervisory control and data acquisition (SCADA) systems – a 700% increase worldwide from 2012 to 2014. Often these attacks are political in nature (Dell 2015). This includes attacks on electricity generation systems, or water purification systems – attacks on the latter in particular can pose a major health risk for people.
- Data indicates that 83% of ICS/SCADA systems, do not have a sufficient cybersecurity framework in place. 67% of ICS/SCADA enabled companies surveyed in 2014 had a security breach. 78% of ICS/SCADA enabled companies expect to be cyber-breached within the next two years (Ponemon Institute 2014). The U.S. Department of Energy systems were reportedly breached over 150 times from 2010 to 2015 (SecurityWeek News 2016).
- A recent research survey demonstrates that from 2014 to 2015 82% of oil and gas industry respondents had seen an increase in cyber-attacks over the last year, and 69% were not confident that their organizations were equipped to detect all cyber-attacks (SecurityWeek News 2016).
- Since 2011, American utility companies have reported over 300 cyber-attacks on the electric grid. These attacks resulted in power disruptions. Former Secretary of Homeland Security Janet Napolitano believes that there will be further cyber-attacks on the U.S. electric grid (Krancer 2016).
- Lloyd's estimates that a major cyber-attack on the U.S. electric grid could potentially cause $1 trillion in economic loss, including $71.1 billion in insurance claims (Lloyd's 2015).

Progress being made

- Over the last 5 years $9.5 billion was spent on modernizing existing infrastructure into a "Smart Grid" (U.S. Department of Energy 2015). Legacy software and infrastructure can provide a backdoor through which cybercriminals are able to breach the system. The modernization initiative is a step forward to mitigating those risks.

XAHIVE Recommendations and Next Steps

- It is clear to us that more could be done to prevent cyber-attacks in the following ways:
  - Need more third party independent cybersecurity experts to validate and verify existing systems for vulnerabilities (see U.S. water company hack (Verizon 2016));
  - Need better backups so that in the event of an attack, it will be easier to restore normal working conditions;
  - Need better implementation of the NIST security framework in critical infrastructure organizations as this would help greatly in cybersecurity preparedness. This should be mandatory for all organizations that provide critical infrastructure as the threat and potential consequences are an ever present danger.

Cybersecurity Insurance

The status quo

- In today's world where cyber-attacks are ubiquitous, part of having recovery procedures includes having an adequate insurance policy in case of a cybersecurity issue. Especially in the U.S., cyber-attacks are proportionally higher than for any other country in the world – the U.S. accounts for about a quarter of global cyber-attacks. It has become increasingly important that corporations purchase cybersecurity insurance.
- Company boards of directors, c-suite, senior government officials and small medium enterprise owners may be unaware that traditional commercial insurance policies tend to not cover the damages incurred as a result of a breach of a company's data. Cyber insurance protects from Internet-based risk relating to information technology infrastructure and information assets if business data is destroyed, stolen, hacked, extorted, compromised, cyber insurance benefits kick in to minimize and indemnify companies for losses to others. Policy benefits often include security audits, post incident PR, customer credit monitoring services, investigative expenses and criminal reward funds (Basani 2015). These benefits of cybersecurity insurance must be included as part of the due diligence for each sector.
- Cyber risk insurance can provide some monetary relief for victims of cyber-attacks. By having adequate cybersecurity solutions, businesses can also take advantage of savings offered by insurance companies. All

of these facts illustrate the need for businesses to have an adequate cybersecurity plan.

XAHIVE Recommendations and Next Steps

- XAHIVE recommends all industries purchase cybersecurity insurance and seeking certification for their organizations. There should be legislation requiring the purchase of cybersecurity insurance and regulations surrounding required certification.
- There should be tax incentives for those who do purchase cybersecurity insurance and seek certification in cybersecurity.
- The incentive program should be calculated based on the cascading savings to the government and industry organizations through the actual mitigation of cybercrime.

Cybersecurity Research and Development

The status quo

- In 2011, the National Coordinating Office for the Networking and Information Technology Research and Development (NITRD) published “Trustworthy Cyberspace: Strategic Plan for the Federal cybersecurity Research and Development Program,” a coordinated effort involving leading researchers, industry, and government.
- The cybersecurity Enhancement Act of 2014 further elaborated on the NITRD strategy. It recommended that designed-in security continue to be an area of emphasis in the 2015 plan and highlighted the importance of accessible, affordable, and understandable approaches to designing in security (Benzel 2015).

XAHIVE Recommendations and Next Steps

- Before developing economic incentives, metrics should be developed that can be used for evidence-based information on return on investment. These metrics are needed to make business decisions on designing and developing cybersecurity products. Recommendations for additional areas to include are the following:
  - Holistic approaches to securing systems;
  - System-of-systems security requirements;
  - Resiliency as a requirement;
  - Software assurance through languages and standard practices;
  - Virtual organizations as security containers;
  - Privacy-preserving data sharing;
  - Consensus algorithms as an approach to data;
  - Human behavior modeling; and
  - Experimental science as a research topic (Benzel 2015).

Cybersecurity Workforce

The status quo

- There is a huge need for cybersecurity professionals in the U.S. It was recently reported that there is a 90% year-over-year increase in cybersecurity jobs. According to a recent survey, it takes about three months to fill an entry-level security position and senior security leadership positions are often left unfilled for 12 to 18 months or longer (Martin 2015).

XAHIVE Recommendations and Next Steps

- The cybersecurity skills supply chain needs a reboot –
    - A good start would be increasing budgets available for cybersecurity professionals.
- Colleges and Universities need to include cybersecurity governance education as part of all professional training.
    - Get college students interested in cybersecurity careers
    - Increase the number of cybersecurity programs in educational institutions (this can be done through government incentives and increased corporate funding of cybersecurity programs with additional scholarships available for promising students
    - Primary and secondary education curricula should build in computing and information technology, emphasizing security as much as possible.
    - Security training and certifications should emphasize skills needed to address security risks and explain how to apply them on the job
    - Increase strategies such as the Delaware Cyber Initiative (DCI). This program seeks to create a collaborative learning and research network (Tittel 2014). The DCI proposes $3 million for a collaborative learning and research network dedicated to cyber innovation. The University of Delaware, Delaware State University, Delaware Technical Community College, and private institutions will develop the lab. These kinds of learning and research networks should be more commonplace. The initiative will cater to large employers but also to the state's banking and financial services sectors. It will also allow government agencies to recruit cybersecurity professionals from the same pool available to private firms (Homeland Security News Wire 2014).
- Need to educate the educators:
    - Cybersecurity champions need to develop a cyber-aware faculty through certification and training programs.
    - Business aspects need to be taught, for example, understanding why cybersecurity matters and what its value is to the business

- Students need to be taught that security extends well beyond the core of IT. Subjects such as legal, risk, communications and other nontechnical aspects of the business that organizations deal with day-in and day-out can all be connected to security.
- Expose the younger generation to the field of security much sooner

- Educate companies:
  - Companies may require a degree, a certification (e.g. Certified Information Systems Security Professional (CISSP)) or a certain number of years of experience in a particular role or position. Requirements should be stated so as not to squeeze the talent pool to a point such that drastically reduces the number of candidates.
  - Also, some job descriptions call for decades of experience with information technology contributing to the false belief that IT knowledge = cybersecurity knowledge. Cybersecurity is an evolving industry and requires the most recent knowledge rather than legacy education.
- Educate the employee:
  - Keep cybersecurity professionals inspired and motivated.
  - Include all employees in cybersecurity governance education activities.

Internet of Things

The status quo

- Recent projections estimate that the Internet of Things (IoT) represents $19 trillion USD global market. By 2020, it is predicted that 50 billion devices will be connected to the Internet. The U.S. is often seen as the leader in IoT with the iconic American firms of Intel, IBM, Microsoft, Google, Cisco, Hewlett Packard and Apple comprising the top 7 in order.
- Since 2015, the U.S. government has started to show increased interest in exploring IoT. In January, 2015, the Federal Trade Commission released a Staff Report on the Internet of Things which focused on the issues of privacy, security and on the need for legislation to regulate IoT.

XAHIVE Recommendations and Next Steps

- Recognize that innovation actually happens with startups as the big companies innovate by buying those startups. So funding and incentives for smaller companies doing R&D on IoT would fuel more effective innovation in this sector.
- XAHIVE recommends that companies practice “data minimization” which involves limiting the collection of data and the time that data is held for the period of time it needs to be used.
- XAHIVE also recommend that companies should prioritize the building of security into devices and that they should train employees adequately,

should ensure that contractors can maintain security, and should monitor devices and report to the consumer when security breaches are detected.

- XAHIVE recommends that IoT legislation be implemented in order to mitigate the risk of poorly envisioned solutions to critical industries such as healthcare and ICS/SCADA systems.

Public Awareness and Education

The status quo

- Data has shown that younger generations are more careless when it comes to cybersecurity (Akhtar 2015). Much of this is owing to lack of education on cybersecurity. Most breaches are caused by human error.
- Organizations maintain a “head in the sand” mentality
- People confuse IT experts as cybersecurity experts

What is being done

- Progress being made to address the challenges: the National Initiative for cybersecurity Education (NICE) provides a way for teachers to access a variety of available resources to help develop curricula and incorporate cybersecurity into their lesson plans.
- In October 2016, there is a National K-12 cybersecurity Education Conference taking place in Virginia to bring together educators, curriculum specialists, professionals, researchers, students, non-profit organizations, foundations, government, and industry to address the challenges and opportunities of cybersecurity education in elementary and secondary schools. The event includes workshops, keynote speakers, panel discussions, and exhibits designed to promote cybersecurity career awareness and support academic preparedness of K-12 students.

XAHIVE Recommendations and Next Steps

- Increase funding to cybersecurity education and training at all levels
- Require a standard of security for organizations dealing with personally identifiable information (PII) and personal health information (PHI).
- Require breach reporting with penalties, including criminal and civil charges for not reporting breaches to clients and channel partners.
- Create a specific framework for all U.S. organizations, not piecemeal
- More government outreach informing the public of the risks they are in. For example, many people may not know what a spear phishing email looks like, or what to do if they receive one.

State and Local Government Cybersecurity

The status quo

- One important development is the NIST cybersecurity framework which is fast becoming the standard for cybersecurity in U.S. government institutions.

XAHIVE Recommendations and Next Steps

- Cybercriminals, state and other threat actors in the cyber-crime space are very agile and constantly innovate in the area of cyber-attacks. This rapid development needs to be met by increased frequency of updates to the NIST cybersecurity framework which as of 2016, has only been updated every few years.
- Cyber breaches affect the entire value chain of an organization from supplier to client. As such, XAHIVE recommends that there be incentives for organizations to include the NIST CF as part of their ongoing audit activiities
  - In support of this, XAHIVE suggest that there be a way to receive NIST certification for organizations.
  - The NIST C&A process requires the management ‘sign off’ on the work that has been completed. It is known as the Authorization Stage of C&A. The Framework does not clearly define which documents and records are needed, and what is the minimum that must be implemented. And as such this is essentially attestation only and really should be replaced by a certification process as outlined above.
- Local and state government RFPs should clearly indicate and require that bidding parties have
  - Cybersecurity insurance in place
  - Some type of cybersecurity certification or recent successful audit evidence
- SMEs are the biggest threat in the value chain for cyber breaches as they do not practice adequate due diligence because of limited budgets. XAHIVE recommends that a cybersecurity governance hiring and training incentive program be established to facilitate the mitigation of cybercrime at the SME level.

References

Akhtar, Allana. 2015. "When It Comes to cybersecurity, Millennials Throw Caution to the Wind." *US News.* June 30. Accessed September 6, 2016. http://money.usnews.com/money/personal-finance/articles/2015/06/30/when-it-comes-to-cybersecurity-millennials-throw-caution-to-the-wind.

Basani, Vijay. 2015. "Opinion: cybersecurity insurance – weighing the costs and the risks." *Market Watch.* March 25. Accessed June 22, 2015. http://www.marketwatch.com/story/cybersecurity-insurance-weighing-the-costs-and-the-risks-2015-03-25.

Benzel, Terry. 2015. "A Strategic Plan for cybersecurity Research and Development." *IEEE Xplore.* July/August. Accessed September 2, 2016. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7180232.

Cohn, Carolyn. 2015. "Cyber attack on U.S. power grid could cost economy $1 trillion: report." *Reuters.* July 8. http://www.reuters.com/article/us-cyberattack-power-survey-idU.S.KCN0PI0XS20150708.

Dell. 2015. "2015 Dell Security Annual Threat Paper." *Dell.* https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf.

Insurance Information Institute. 2014. "Energy Infrastructure and Vulnerabilities ." *U.S. Department of Energy.* April 11. http://energy.gov/sites/prod/files/2014/04/f15/Remarksof_RobertHartwig_ppt_april11.pdf.Homeland Security News Wire. 2014. "Delaware launches cyber initiative." *Homeland Security News Wire.* March 27. Accessed September 2, 2016. http://www.homelandsecuritynewswire.com/dr20140327-delaware-launches-cyber-initiative.

Kovacs, Eduard. 2016. "Critical Infrastructure Incidents Increased in 2015: ICS-CERT." *Security Week.* January 20. http://www.securityweek.com/critical-infrastructure-incidents-increased-2015-ics-cert.

Krancer, Michael. 2016. "Did Big Energy Just Make Us Safer From Terrorism Or Cyber Attacks On The U.S. Electrical Grid?" *Forbes.* April 20. http://www.forbes.com/sites/michaelkrancer/2016/04/20/did-big-energy-just-make-us-safer-from-terrorism-or-cyber-attacks-on-the-u-s-electrical-grid/#1f014cc331b3.

Lloyd's. 2015. "Emerging Risk Report 2015: Business Blackout." *Lloyd's.* July 8. https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

Martin, Sean. 2015. "cybersecurity professionals: Five ways to increase the talent pool." *Techtarget.* December. Accessed September 2, 2016. http://searchsecurity.techtarget.com/feature/cybersecurity-professionals-Five-ways-to-increase-the-talent-pool.

Ponemon Institute. 2014. "Critical Infrastructure: Security Preparedness and Maturity ." *Ponemon Institute.* July. http://images.outreach.unisys.com/Web/UnisysCorporation/%7B3f7a3970-c2eb-4281-9e46-988f9048d4d1%7D_14-0316_Unisys_Ponemon_Study.pdf?elq=94ffd9e6a36b407b99378212c4327054&elqCampaignId=.

SecurityWeek News. 2016. "Oil and Gas Industry Increasingly Hit by Cyber-Attacks: Report." January 14. http://www.securityweek.com/oil-and-gas-industry-increasingly-hit-cyber-attacks-report.

Thompson, Kirsten, and Brandon Mattalo. 2015. "http://www.canadiancybersecuritylaw.com/2015/11/the-internet-of-things-guidance-regulation-and-the-canadian-approach/." *Cyberlex.* November 24. Accessed March 14, 2016. http://www.canadiancybersecuritylaw.com/2015/11/the-internet-of-things-guidance-regulation-and-the-canadian-approach/.

Tittel, Ed. 2014. "How to fix shortage of cybersecurity professionals?" *Search Networking.* May. Accessed September 2, 2016. http://searchnetworking.techtarget.com/answer/How-to-fix-shortage-of-cyber-security-professionals.

U.S. Department of Energy. 2015. "ARRA Grid Modernization Investment Highlights - Fact Sheet ." *Office of Electricity Delivery & Energy Reliability.* October. http://energy.gov/oe/downloads/arra-grid-modernization-investment-highlights-fact-sheet.

U.S. Department of Homeland Security. 2015. "The Future of Smart Cities: Cyber-Physical Infrastructure Risk." *Office of Cyber and Infrastructure Analysis, U.S. Department of Homeland Security.* August. https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf.

Verizon. 2016. "Data Breach Digest." February. http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf.