AUTOMATION FEDERATION
The Voice of Automation

August 1, 2017

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

The safety, security and prosperity of our Nation, and indeed the entire world we live in, depends on critical infrastructure whose systems are considered so vital that their incapacitation or destruction would have a debilitating effect on the economy, national security or public health and safety.

Over past decades, the systems underpinning the foundation of these critical infrastructures have remained for the most part to be based on obsolete computing technology, and even more disturbing – have become interconnected with business networks and the internet itself – exposing these mission critical systems to the myriad of cybersecurity threats from a wide swath of capable threat actors. One only needs to read the morning news to see daily accounts of nation state cyberattacks, ransomware or other forms of malware effecting these critical systems.

One of the leading contributors for these issues is the lack of a properly aware and trained cybersecurity workforce that recognizes the risks involved, and that take systematic steps to reduce this risk.

Our member organizations as well as other partner organizations such as the SANS Institute are highly concerned that there is a lack of cohesion or focus on ensuring that cybersecurity education is available at all skill levels in every step of the education system.

General Information

1. Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)?

Formed in 2006, the non-profit Automation Federation (AF) focuses on Workforce Development needs of our member organizations and the automation profession as a whole. The tremendous gap in cybersecurity knowledge at all skill levels in the workforce is a strong contributor to the vulnerability of our critical infrastructures, such as energy supply, water deliver, transportation, manufacturing.

The founding member of AF is the International Society of Automation (ISA). ISA created and manages the Control Systems Engineer (CSE) certification, and has content responsibility for the CSE Professional Engineering (PE) examination. This relationship brings a unique engineering perspective to the cybersecurity discussion which is often missed when cybersecurity is only discussed by computer scientists.

Automation Federation has multiple working groups focused on cybersecurity and workforce development. The core of what we do is engage in promotion and advocacy of these challenge areas through our extensive membership and partners. Through collaboration with training organizations such as ISA and SANS, thousands of automation professionals have been reached and have extended their understanding, knowledge, and capabilities to further mitigate cybersecurity risks to current and future industrial automation and control systems.

Through our partnerships with education groups such as the American Association of Community Colleges (AACC), Automation Federation has assisted in standing up the Automation Community College Consortium (ACCC), a partnership to bring colleges together with the Automation Competency Model (ACM). The ACM was developed by the Automation Federation and the Employment and Training Administration (ETA) of the U.S. Department of Labor – and is the tool that will assist the colleges in the development of automation educational curricula for future automation professionals.

Automation is moving into almost all areas of our lives as the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) promote ubiquitous connectivity of all manner of devices. In many cases, due to lack of knowledge, developers, inventors, manufacturers and consumers alike fail to build and install these devices in a cyber secure fashion. Significant improvements to workforce development efforts are required to address this national need.

Growing and Sustaining the Nation's Cybersecurity Workforce

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

Diverse sets of data exist on specific programs, but simply put – cybersecurity should not be considered an add on feature to any product or service, or even a curriculum or training syllabus. Cybersecurity needs to be incorporated into every facet of our lives including the education process. An example of a valuable metric would be how many standard engineering courses include cybersecurity as part of the curriculum? How many high school computer courses include cybersecurity as part of the course? We need to understand the true expanse of the gap we are dealing with – and counting how many cybersecurity specific programs exist isn’t going to do it. We need to determine why it isn’t included as a base fundamental skill in every part of our education system.

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

The answer to the question is “No”. Every skill level of worker in all categories of occupation require some cybersecurity understanding that is tailored to the job that they do. Currently it seems that we are targeting the two extremes of the spectrum – either the beginner / consumer level through programs such as “Stop. Think. Connect” or NSA sponsored “National Centers of Academic Excellence”. Little attention is paid to the millions of workers in the middle, who are most likely the ones who need the most knowledge on how to perform their day to day tasks in a cyber secure manner.

A good analogy would be electrical safety awareness. Even small children are taught not to play with electrical outlets or devices – do we teach children just starting to use computers about the most basic cybersecurity, such as comparing passwords to keys? No

Apprenticeships are available to develop our workforce of electricians into the journeymen and women that build the infrastructure around us, and during their training they learn additional safety procedures that are applicable to their job. Do we teach them about cybersecurity best practices when installing electrical equipment? No

Our universities turn out advanced degrees in many different engineering disciplines. These are the men and women that are designing the fabric of the interconnected world around us. Does the chemical engineer receive training on the ramifications of connecting the new advanced chemical analyzer directly to the internet to update the software on it? No

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

In the context of Information Technology (IT) most companies and organizations have implemented and enforce basic cybersecurity policy.

In the Operational Technology (OT) domain, which comprises things such as Industrial Control Systems, Automation Systems, SCADA Systems, Internet of Things, and even embedded computing in automobiles, aircraft, railways, etc. there are often no cybersecurity training policies in place. Those entities that have policies in place are unlikely to be able to enforce them due to the vast number of devices that are simply 'unknown' – and have no person or persons that are responsible for their security posture. As stated in question 2, if all devices contain embedded computers and need some level of cybersecurity protection – then all workers require some level of cybersecurity awareness training.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

Some of the basic skills are common and fundamental regardless of role, industry and sector, like basic safety training required for every worker in every occupation. As workers go into more specialty careers, then cybersecurity training, just like safety training must be tailored and customized for the specific industry. Employers and hiring managers often do not understand cybersecurity themselves, and are at a disadvantage when it comes to measuring the cybersecurity skill levels of potential applicants. A lack of consistency in certification standards makes it difficult to compare individuals' actual skill levels, and many of the skills being taught are not applicable to their specific on-the-job needs.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

In the field of automation and operational technology (OT) systems, many of the workers are not degreed graduates of university programs. They have a mix of technical training and college education, but those training programs often lack basic cybersecurity content. Educators often cite that "the curriculum is full" and we must cut something out to add something in. The basic awareness of cybersecurity problems must be taught at this (and all) levels.

Organizations such as the International Society of Automation, and SANS ICS are developing and teaching both the fundamental cybersecurity skills needed by these workers, as well as some specialized "sector specific" training for those in specialty areas such as the electricity sector, which is subject to unique regulations. We can scale and teach the specialty areas, but it is not possible to scale to the level required to teach all workers in all occupations the most basic of awareness training – this must be done at the K-12 and college levels as part of the STEM curriculum. For example, Automation Federation has been working with the American Association of Community Colleges (AACC) in order to promote Operational Technology (OT) cybersecurity education at the college level.

We need to explore how to incorporate “the fundamentals” of cybersecurity training into all facets of our education system, so that industry specific training organizations can focus on teaching the specialized courseware that is unique (and sometimes costly) for those sectors that need it. The basics should be something that is standardized, ubiquitous and pervasive – so that when you apply for a job it is a given that you have that basic cybersecurity knowledge.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

The greatest challenge is that we don’t have enough trained personnel – period. The lack of attention and focus to STEM education has created a vast void in the pipeline that is feeding the hiring process in industry. We are seeing large numbers of retirees such as baby boomers, that are leaving with significant technical knowledge – and that knowledge is not being retained in the younger generation.

Cybersecurity is not immune to this. We must implement in parallel cybersecurity awareness training at all levels of the education system. We simply cannot afford to only implement it in the K-12 system and then wait for those youngsters to graduate and enter the workforce.

For a period of time this will be costly, but our future and prosperity depend on it.

7. How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

One of the significant challenges in cybersecurity education is the pace of change of the hardware, software, devices, systems and all things that are enabled by computing. Teaching basic electrical safety is greatly simplified by the fact that the physics of electricity do not change over time, thus the curriculum is relatively constant compared to that of cybersecurity or computer science.

Basic standards for cybersecurity conformance must be realized for the Cyber Physical Systems (CPS) in order to increase the likelihood that they will be deployed in a “secure out of the box” fashion. Much of this responsibility lies in the hands of the manufacturer or designer of a product. Just like an electrical device must have certain safety testing and certification performed by a recognized authority, and then must be installed by a qualified installer (electrician) – so should cyber enabled devices that connect to a network. Certain devices should be required to be installed by a qualified “cyber-installer” while others if they meet the conformance specifications can be considered to be “plug and play” such as an electrical appliance.

Keeping up with this pace of change is no small task, but if we can continue to innovate and drive new products into the marketplace at breakneck speed – then we as a nation are also capable of ensuring that those new products along with all their new features have the basic cybersecurity controls built-in.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?

Continue basic cybersecurity awareness at all levels. Harmonize the content and curriculum requirements so that educators can turn out graduates that consistently meet the needs of the workforce from a basic training perspective. Incentivize the development of industry and/or sector specific training, perhaps by utilizing the Sector Specific Agencies (SSA) for the critical infrastructure sectors.

Work on the global stage with other world governments to move towards global adoption of basic cybersecurity awareness training for the population as a whole, and for workers in all industries.

Recognize that we need to make significant investments in STEM, and that cybersecurity should be part of that effort at every level in the education system.

Lead through example in the hiring process and require cybersecurity skills and/or certifications for all manner of federal job categories.

ii. At the state or local level, including school systems?

Encourage educators to include basic cybersecurity concepts in all courseware throughout the K-12 system. Make available continuing education for the teachers and educators themselves to learn about cybersecurity concepts in order that they can incorporate these concepts into their classroom.

Lead through example in the hiring process and require cybersecurity skills and/or certifications for all manner of job categories for state or local employees.

iii. By the private sector, including employers?

Treat cybersecurity like you treat safety. Reward the "near miss". Document gaps and make plans to address them. Follow through with those plans and communicate them back to your workers.

Evaluate the cybersecurity risk in your company – at all levels and in all systems. Drill deep. Find the devices you didn't know about in the Operational Technology and Internet of Things categories. Find out who in your company is responsible for the safe operation of those devices. Ensure that they have the appropriate training that is pertinent to their job functions. Develop and enforce your cybersecurity policies.

Lead through example in the hiring process and require cybersecurity skills and/or certifications for all manner of job categories for your employees.

iv. By education and training providers?

Don't just treat cybersecurity as another independent course of study – incorporate cybersecurity concepts and best practices into every single category of curriculum and syllabus. It doesn't need to be much, but just enough to get the point across to the student "should I do this?" or "I should tell somebody about that"

Push governments and employers to support these efforts, and to make the funding and resources available for you to succeed in your endeavors.

Work with your peers to strive towards harmonization of cybersecurity content. We need to have graduates that no matter what institution they graduate from – they can talk the same cybersecurity language and understand the same basic cybersecurity concepts.

Lead through example in the hiring process and require cybersecurity skills and/or certifications for all manner of job categories for your employees.

v. By technology providers?

Ensure that every product, service or deliverable has a cybersecurity component. Devices should conform to basic cybersecurity best practices for the industry and/or application.

Make it easy for the research community to submit cybersecurity vulnerability information to you, and act on that information in a timely fashion by patching or mitigating the vulnerability. Don't punish the research community or threaten legal action, and treat this as "free quality control services"

Follow a secure development lifecycle, and ensure that all employees understand where they fit into this. Even the employee on the shipping dock can recognize when they are about to ship a product that has been sitting on the shelf and has an outdated revision code if the right procedures and training are put in place. Empower that employee to bring that forward to the right product group and get the updated firmware and/or software installed.

Educate your consumers on how to use your devices in a cyber secure manner. Be transparent about how your product works and how it doesn't work or areas that it shouldn't be applied due to cybersecurity risk.

Lead through example in the hiring process and require cybersecurity skills and/or certifications for all manner of job categories for your employees.

To learn more about Automation Federation, visit www.automationfederation.org

Respectfully Submitted,

--signed--

Marty Edwards
Managing Director
Automation Federation