NFPPC NATIONAL FORUM FOR PUBLIC PRIVATE COLLABORATION

Global Forum to Advance Cyber Resilience llc 501(c) (6)

2 August 2017

Charlie Tupitza
Chief Executive Officer
National Forum for Public-Private Collaboration
resilience@nfppc.org

General Information

Our Forum leads public-private collaboration about, among other things, cyber resilience which is mission focused. We discuss the roles and responsibilities of all people in the organization to be aware, prepared, and authorized to act.

Our responses to the questions posed will substitute the word 'resilience' for 'security'. We will also address our responses from a high level within an organization of 'what' needs to be done without getting into how things get done. Our business focus addresses education in the marketplace which is required for organizations to be resilient and sustainable. We recognize the value of STEM and traditional cybersecurity technical training but will address the business side in this response.

We are currently leading collaboration around the workforce need to understand agility to face ever changing threats and opportunities. By focusing on the business aspect of cyber resilience we have a better chance for all stakeholders to understand cyber-resilience value before during and after design of services and products.

As we search for effective answers to the questions below we must know this is a team effort. We must support internal and public-private collaboration which includes a broad range of stakeholders.

We recognize the educational value of collaboration as it enables cyber-resilience which enables the mission and customer, or warfighter. Organizations of all sizes can benefit from:

- Understanding and managing risk across organizational boundaries throughout the life-cycle of a product or service, whether internal, external, or shared.
- Having a capability to exhibit trustworthiness between and across partners for a competitive edge.

Growing and Sustaining the Nation's Cybersecurity Workforce

Appropriate cyber-resilience policy:

We must establish the appropriate level of leadership and governance associated with cyber-resilience policy. With constantly changing threats and opportunities we must find ways to support dynamic policy.

Types of knowledge or skills do employers need or value as they build their cybersecurity workforce?

Overall considerations at the business level, understanding of:
Agility, Governance, Project Management, Lean, Prudence, Sustainability, Resilience, Reasonableness, Discipline, Value to Customer, Value to Organization, Understanding of Risks**:** Competitive, Opportunity, Cyber, Physical, other. We need to understand how each role impacts business value.

Knowledge and skills vary by role, industry, and sectors?

At a high level within an organization, which we address, there are more similarities then differences. Cyber-resilience enables business mission and customer value. We must take advantage to communicate at this level sharing use cases and lessons learned.

Most effective cyber-resilience education in the context of organizational resilience and agility:

Education making the connection to the business mission and therefore the customer is critical. There is value in utilizing a unified overall business approach to resilience. Organizations will benefit from understanding the value of cyber-resilience considerations as a core requirement to serve the mission.

Cyber-resilience enables the product or service so it needs to be considered from the beginning. Education must then provide the necessary support in terms of each role of stakeholders. We cannot expect leadership to know how to act or support the necessary governance without making this connection and educating them appropriately.

Greatest challenges and opportunities?

One of the greatest changes is to enable the mission and customer (or warfighter) side of the organization to communicate needs effectively with the risk management and resilience part of the organization. They must collaborate regularly internally, with customers, and with suppliers of products and services. Organizations will benefit from Agility and adaptability as core competencies.

Advances in Technology:

Understanding how to best automate our responses to threats and opportunities while being reasonable, prudent and without getting in the way of opportunities has great business value.

Agility accompanied by a proper level of governance for discipline without getting in the way of effectiveness and ingenuity is important.

Steps:

Federal: Public and Private collaboration leads to value to taxpayers. This can be done at many different levels to share lessons learned and develop referenceable use cases.

State and Local: Enable state and local governments to collaborate with the private sector to share lessons learned and best practices, identify available resources, lay the foundation for support within the local first responder community and foster mentoring relationships and the ability to share resources between large organizations and small ones in support of supply chain assurance. Participating in collaboration with the private sector will also help.

Public Private Sectors: Both public and private organizations benefit from providing meaningful internships to students to help them make the business connection between cyber and the business mission. It is helpful for organizations to engage in meaningful collaboration with others to help establish reasonable approaches to cyber-resilience**.**

Education and training providers: Traditional college and university programs have limited time and resources. They must encourage students to take intern positions during school and between sessions. Training companies must provide supplemental training unavailable at traditional education institutions as well as provide continual education beyond traditional education.

Technology partners: Must continue to add utility in their offerings and the training necessary to take advantage of it. They must clean up their own act and provide transparency to establish trust.