RightExposure

Protecting Small Businesses from Cyber Threats and Strengthening Business Value in the United States and its Territories

May 8, 2019

Purpose: To provide an informal brief for interested parties on the progress made to protect small businesses from cyber threats in the United States and its territories including:

- Governments
- Small to mid-sized organizations
- Large organizations with smaller business partners and members of their business eco-system
- Product and service providers
- Supply chain members
- Standards organizations

A more formal detailed announcement is forthcoming from the Americas Small Business Development Center as market survey information to help both the public and private sectors understand how they can take advantage of the work being done as well as support and participate.

Charlie Tupitza 703 989-8777 ctupitza@rightexposure.com www.rightexposure.com 5/7/2019

RightExposure

7 May 2019

Interested Parties,

I am often asked the same questions about how small US businesses can protect themselves and our nation from the ever-increasing velocity and complexity of cyber threats.

- What is the responsibility/duty of US small businesses to protect themselves?
- What is the burden on small businesses to assess their readiness to protect themselves?
- How can we quantify this and reduce this burden?
- What resources are available to help small businesses provide consistent and effective assessments stored in a secure manner? Associated awareness and guidance?
- How can we help small businesses incorporate good practices as a normal course of business?
- Do cyber liability and data breach insurance play a role in helping small businesses?
- What is the balance between promoting a simple, available, clear path, and value?

I am encouraged by findings over the past year. The following will address some simple things happening now. Sometimes providing a simple, available, clear path is more effective than focusing all efforts to convince someone there is value.

We will declare the first round of victory when small businesses are compelled into informed business decisions made obvious through use of the NIST Cybersecurity Framework.

Will a bar be set because of these activities?

I am not a member of the Americas National Development Center but have been helpful in coordinating the activities in this letter and have been reaching out to the above interested parties for input.

We are very interested to hear your opinion or answer questions.

Charlie Tupitza
President
RightExposure

RightExposure

Federal and state governments, industry, regulators, and other parties need to do everything they can to help secure their business eco-systems. They often ask/demand contractors to perform assessments for compliance to standards. Until now many see these assessments as a burden too expensive to bear.

Progress is being made to remove a great deal of this burden/excuse while making the businesses case for organizations to protect themselves and others in their business eco-system including the nation's critical supply chain.

Secure, standard-based assessments help all stakeholders focus on effective approaches, continual monitoring, and training for small and mid-size businesses.

"America's small businesses benefit from utilizing consistent standard-based approaches to enhance their cyber security knowledge. This cannot be overstated. Businesses are safer, our nation more secure, and our economy stronger when efforts are coordinated to inform and train them."

Charles "Tee" Rowe – President/CEO of *Americas Small Business Development Centers*

MOVING FORWARD!

Americas Small Business Development Center (ASBDC) is supported by the Small Business Administration (SBA), state governments, colleges, universities, and local economic development organizations. The ASBDC acknowledges the value of having consistent approaches to address cyber and data breach exposures of small businesses. There are more than 4,000 business advisors located in more than 1,300 Small Business Development Center (SBDC) locations throughout the US and its territories. Numerous centers have technology-oriented programs that can support higher end cybersecurity for small technology firms and advanced manufacturing firms. Several SBDCs host Procurement Technical Assistance Centers (PTACs) for the Department of Defense which provide cybersecurity training to meet GSA/DOD contracting specifications.

The ASBDC CEO, Tee Rowe, recognized the risk of having the results of cyber assessments located on the very networks/systems being assessed by SBDC advisors as well as the computers of the advisors. This is akin to putting the keys to your house under the welcome mat. To protect this information, he submitted a request to the **SBA Chief Information Security Officer** (CISO) to have the Continuum GRC Inc. Software as a Service ITAM platform assessed by FedRAMP at a HIGH level. He chose "high" because many clients are contractors to the DoD and other organizations requiring this level of protection of confidential/nonpublic information. The CISO submitted the request to the FedRAMP Program Management Office and the assessment process has begun.

The University of Wisconsin-Whitewater (UWW) has created an assessment based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework 1.1 and associated awareness training specifically tailored for the small business community. They have also created a system which captures the amount of time Small Business Development Center advisors engage in the support of small businesses during an assessment. Measuring this effort is a valuable metric for many reasons.

Continuum GRC, a veteran-owned software company and creators of the ITAM software platform will host the University's assessment. The platform is in a **FedRAMP HIGH** cloud, providing the most secure location for the data obtained in the assessments to reside *(additional information about FedRAMP HIGH cloud provided in appendix A attached).* Using the Continuum GRC platform meets or exceeds the same cyber security requirements imposed on the largest companies contracted with the federal government. This platform ensures controlled access to confidential information associated with the assessment and the requirement to protect the integrity of the assessment process, itself. As organizations enter information in their Cybersecurity-Framework-based assessments, this information will, when necessary, cascade to other assessments which require more detail such as a more rigorous CSF assessment, a 800-171, 800-53, HIPPA, PCI, SOC or other.

Arthur J. Gallagher, a major insurance broker, has a memorandum of understanding with the ASBDC agreeing to support the cyber initiatives of the ASBDC. Gallagher Affinity is a division specializing in supporting associations and trade groups representing small businesses and industry across the United States. They will be introducing and promoting the ASBDC cyber program to these associations, allowing significant access to a broad market of small businesses. They will also support webinars, conferences, mailings, and other outreach to raise the general awareness of SBDCs' advisors and their availability to aid small businesses; and will encourage these businesses to take the necessary steps to assess and address their cyber exposures. Additionally, they will provide an optional cyber and data breach insurance program, specifically designed for those businesses that conduct the risk assessment.

Continuum GRC Inc. issued two grants to help support small businesses in the US and its territories.

The University of Wisconsin Whitewater Grant will port their basic Cybersecurity Framework Assessment to the Continuum GRC ITAM platform on the FedRAMP High cloud. As part of this, they will help coordinate messaging around this and other assessments to ensure consistency. If approved by the small business being assessed, anonymized data will be shared with UWW to help understand effectiveness of approaches and identify readiness of communities.

An example: Wisconsin will be the new home for a massive computer monitor manufacturing plant. This company is asking the SBDCs to support awareness training for all members of the service community around them. As the SBDCs become successful, communities will be safer for themselves and be able to better attract new businesses to them.

The American Small Businesses Development Center's grant gives all state and local Small Business Development Centers and their advisors free access for their clients to utilize the assessment tool and awareness training program above. Advisors will assist the business in the assessment process and their interaction with the business will help coordinate messaging to ensure consistency and standardization.

The University of Wisconsin Whitewater is seeking a grant to support the entire inclusion of America's SBDC network. A full deployment throughout their large footprint will assist in creating a baseline understanding of America's small business' current state of cyber readiness. Additionally, America's SBDC business advisors will have the opportunity to work with clients and develop new relationships when assessment users seek further assistance per their charter of supporting book keeping, business plans, loan applications and others.

University of Texas in San Antonio Progress is being made for education and training associated with the NIST 800-171 through a joint effort with them. Stay tuned.

RightExposure

Example Target Organizations

It is easy to personalize the value of protecting 'confidential information' when we speak of lawyers. Thinking of government information is distant from many small businesses. We need to make this personal to progress.

Members of several bar associations are engaged in use cases and taking the assessment. They will provide feedback before engaging SBDC advisors to roll this out to the legal profession nationally. They already engage nationally to support lawyers with accounting, marketing, assistance with loans and other services.

Several other sectors such as federal civilian and defense contractors, health care, finance, manufacturing, and restaurants are part of the initial thrust of this effort.

Metrics:

Many organizations will be OK with a basic assessment. Identifying why organizations who utilize this “basic” Cybersecurity Framework based assessment progress to more comprehensive ones will be an important metric. Did they do this because they are required to or because they see the value outside the requirement?

Utilizing standards and best-practice-based approaches makes it easier for organizations to collaborate and share good practices with others. Measuring effectiveness is made easier. They have a better understanding of how they may transfer risk to others. Do they participate in collaborative events? Did they implement a best practice?

How many will engage with the insurance industry to share risk? What type of coverage is being purchased and for how much? Did they make the decision because the assessment brought informed clarity to them?

As organizations understand risks and opportunities revealed in assessments, they become qualified and informed customers for software, hardware, and service providers, making it easier for these providers to understand how to help. Did they purchase hardware or software? Did they engage with a consultant outside the SBDC?

Subcontractors are better positioned to ask their prime contractor for help. Did they ask their prime for help?

This knowledge will help them be informed participants in securing the nation’s supply chains.

HOW CAN YOU HELP

Stakeholders interested in small and mid-sized business can articulate sector-unique needs by utilizing the common lexicon created by the NIST Cybersecurity Framework to help with consistency. This assessment guidance will be necessary for Small Business Development Center Advisors to add value for specialized areas and ensure consistency which enables measurement of approaches.

Stakeholders can invest financially and provide resources to help this effort. The large footprint of the ASBDC makes this support available to any of the more than twenty-eight million small businesses who serve us daily.

Product and Service providers can help by articulating their values relative to the controls of the Cybersecurity Framework, 800-171, 800-53, HIPPA, PCI, FAIR and other standards and describe the rationale behind using your product and or service to address them.

A section on **workforce** is in progress which will address the National Initiative for Cybersecurity Education. Help!