STRENGTHENING THE CYBERSECURITY POSTURE OF AMERICA'S SMALL BUSINESS COMMUNITY

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

HEARING HELD
JULY 20, 2021

Small Business Committee Document Number 117–026
Available via the GPO Website: www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
45–122 WASHINGTON : 2021

HOUSE COMMITTEE ON SMALL BUSINESS

NYDIA VELÁZQUEZ, New York, *Chairwoman*
JARED GOLDEN, Maine
JASON CROW, Colorado
SHARICE DAVIDS, Kansas
KWEISI MFUME, Maryland
DEAN PHILLIPS, Minnesota
MARIE NEWMAN, Illinois
CAROLYN BOURDEAUX, Georgia
TROY CARTER, Louisiana
JUDY CHU, California
DWIGHT EVANS, Pennsylvania
ANTONIO DELGADO, New York
CHRISSY HOULAHAN, Pennsylvania
ANDY KIM, New Jersey
ANGIE CRAIG, Minnesota
BLAINE LUETKEMEYER, Missouri, *Ranking Member*
ROGER WILLIAMS, Texas
JIM HAGEDORN, Minnesota
PETE STAUBER, Minnesota
DAN MEUSER, Pennsylvania
CLAUDIA TENNEY, New York
ANDREW GARBARINO, New York
YOUNG KIM, California
BETH VAN DUYNE, Texas
BYRON DONALDS, Florida
MARIA SALAZAR, Florida
SCOTT FITZGERALD, Wisconsin

MELISSA JUNG, *Majority Staff Director*
ELLEN HARRINGTON, *Majority Deputy Staff Director*
DAVID PLANNING, *Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

STRENGTHENING THE CYBERSECURITY POSTURE OF AMERICA'S SMALL BUSINESS COMMUNITY

TUESDAY, JULY 20, 2021

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Committee met, pursuant to call, at 10:01 a.m., in Room 2360 Rayburn House Office Building and via Zoom, Hon. Nydia Velázquez [chairwoman of the Committee] presiding.

Present: Representatives Velázquez, Crow, Davids, Mfume, Phillips, Newman, Carter, Bourdeaux, Delgado, Houlahan, Mr. Kim, Craig, Luetkemeyer, Williams, Hagedorn, Stauber, Meuser, Tenney, Garbarino, Ms. Young Kim, Van Duyne, Donalds, and Fitzgerald.

Chairwoman VELÁZQUEZ. Good morning. I call this hearing to order.

Without objection, the Chair is authorized to declare a recess at any time.

Let me begin by saying that standing House and Committee rules and practice will continue to apply during hybrid proceedings. All Members are reminded that they are expected to adhere to these standing rules including decorum.

House regulations require Members to be visible through a video connection throughout the proceeding, so please keep your cameras on. Also, please remember to remain muted until you are recognized to minimize background noise. If you have to participate in another proceeding, please exit this one and log back in later.

In the event a Member encounters technical issues that prevent them from being recognized for their questioning, I will move to the next available Member of the same party and I will recognize that Member at the next appropriate time slot provided they have returned to the proceeding.

For those Members and staff physically present in the Committee today, we will continue to follow the most recent OAP guidance. Masks are no longer required in our meeting space for Members and staff who have been fully vaccinated. All Members and staff who have not been fully vaccinated are still required to wear masks and socially distance.

As new technology has made America more dependent on digital tools, malicious actors have been launching more frequent and severe cyber attacks. In the early months of 2021, we have seen a wide array of headlines detailing attacks on institutions like large corporations and municipal governments.

Just yesterday, the Biden administration acknowledged that hackers affiliated with the Chinese government were responsible for hacking Microsoft email systems, compromising tens of thousands of computers worldwide and exposing reams of sensitive data. The fallout of the attack is still being evaluated, but it is estimated the hack could have affected hundreds of thousands of small businesses. Episodes like this exhibit the significant threat cyber attacks pose to small businesses.

This risk has increased in recent years as small businesses have begun to rely more heavily on digital technologies. According to the Connected Commerce Council, 72 percent of small firms increased use of digital tools during the pandemic.

Unfortunately, as digital adoption has increased, investment in security measures has not kept pace. Small businesses often do not have the resources to invest in an adequate cyber defense system or hire a dedicated specialist. Guarding against cyber attacks often comes with high implementation costs and substantial investments of time and resources. Many are already operating on thin margins and slim human resources.

Failing to prepare for a cyber attack can have disastrous impacts. Damage to information systems, regulatory fines, lost customer trust, decreased productivity, and lost income are all potential consequences of a cyber breach.

Because of their structural importance to the overall economy, attacks on small firms can have severe impacts on larger enterprises and governments connected to them through the supply chain. Given the greater risk cyber attacks pose to small employers and their limited capacity to protect against them, this Committee must find ways to help entrepreneurs strengthen their cybersecurity posture.

Today's hearing gives us the chance to examine how existing cyber resources can be enhanced and integrated into small business support mechanisms.

I also look forward to discussing new initiatives that can alleviate the financial burden of cybersecurity preparedness. Small businesses are the foundation of our economy, so their vulnerability is our nation's vulnerability. Investment in their security will make us all more secure.

I would now like to yield to the Ranking Member for his opening statement.

Mr. LUETKEMEYER. Thank you, Madam Chairwoman.

In preparing for today's hearing, I am reminded of how pervasive the use of the internet and information technology has become in our society in such a short period of time. We bank online, we work online, for the past year, we have held many congressional hearings online. Our growing dependency on constantly evolving information technology is fundamentally altering the way we live, and the way businesses of all size operate.

Although benefits springing from the utilization and adoption of new technologies are incalculable, we are forced to contend with a new threat, specifically, the explosive growth of a criminal industry seeking to steal valuable data and manipulate critical systems for financial gain.

As the world continues to embrace new technology, we increase the attack surfaces through which cybercriminals can infiltrate and wreak havoc to a devastating effect.

These attacks are not without consequence. The cost of cybercrime is absolutely overwhelming. Experts estimate global damages totaling $6 trillion this year alone, projected to reach a staggering $10.5 trillion annually by 2025.

Because small businesses are the intended targets of cybercriminals approximately half the time, the damage inflicted upon small businesses is catastrophic. These attacks push many to the brink with one in six businesses reporting the financial impact materially threatening the company's future. In addition to financial costs, many are unable to recovery from the loss of their intellectual property, resources, and reputation following a cyber-attack.

During my time with this Committee as a member and now as Ranking Member, I have had the privilege to speak with many small businesses in my district and beyond, and I say with certainty that many small businesses do not have the resources, knowledge, and awareness to properly defend against such attacks which is precisely what makes them attractive targets. Many lack insufficient inhouse expertise to deal with these breaches, leaving it up to the small business owners themselves to handle the matter with predictable results.

Make no mistake; this is asymmetrical warfare. Cybercriminals expend little effort targeting small businesses that often have fragile to nonexistent cybersecurity defenses, while small businesses must allocate valuable time and precious resources to defend against this faceless enemy. While attacks against large businesses consistently make frontpage news, small businesses must not be disregarded. The new reality is that large organizations are merely sprawling networks of interconnected business partners consisting of all sizes of companies including small businesses, each a viable vector for attack.

And one of the most effective means of shoring up cybersecurity defenses is knowledge. Knowledge is power and we need to empower small businesses with the tools they need to protect themselves, and by extension, the wider network of businesses and organizations they touch.

A critical component to knowledge is the need for information sharing among the public and private sectors. As fast as cybersecurity systems are established and patched, cybercriminals are already looking for and in many cases successfully finding new creative ways to infiltrate organizations' internal networks. Having a robust information sharing system is fundamental for a strong and effective cybersecurity defense not just for small businesses but for our country as a whole.

Unfortunately, small businesses experience significant resistance to participating in cybersecurity information sharing activities for a variety of reasons. They may be reluctant to risk exposure to potential legal liabilities resulting from the disclosure and they may harbor doubts regarding the government's ability to adequately protect reported data and privacy information.

The federal government recognizes these concerns and has made significant strides towards alleviating these fears. However, these effects must continue to improve in order to make the most impact on small businesses which derive the digital economy's growth, innovation, and job creation.

To that end, there are several pieces of bipartisan legislation introduced by my colleagues on this Committee which attempt to begin resolving some of the issues and reservations small businesses have. I hope we will engage in a fruitful dialogue with our witnesses about this legislation today. Combatting cyber threats is a vastly complicated issue that will require largescale coordination across the entire federal government and private sectors.

We must not let that complexity deter us from our goal. Rather, we must redouble our efforts towards strengthening the cybersecurity of our country starting with small businesses. I look forward to hearing the testimony of the witnesses.

And with that, Madam Chair, I yield back.

Chairwoman VELÁZQUEZ. Thank you, Mr. Luetkemeyer. The gentleman yields back.

I would like to take a moment to explain how this hearing will proceed. Each witness will have 5 minutes to provide a statement and each Committee Member will have 5 minutes for questions. Please ensure that your microphone is on when you begin speaking and that you return to mute when finished.

With that, I would like to introduce our witnesses.

Our first witness is Ms. Tasha Cornish, the Executive Director of the Cybersecurity Association of Maryland known as CAMI, located in Baltimore, Maryland. CAMI is dedicated to enhancing the local cybersecurity ecosystem by offering training, cyber career networking, and the Cyber SWAT team which is a free cybersecurity incident hotline. Ms. Cornish has nearly a decade of nonprofit leadership experience and she earned her master's degree at Johns Hopkins Bloomberg School of Public Health and holds a bachelor's degree in neuroscience from Cedar Crest College. Welcome, Ms. Cornish.

Our next witness is Ms. Sharon Nichols, the State Director for the Mississippi SBDC. The state's SBDC network provides business services at 15 centers and sites, including the Mississippi State University Center for Cyber Innovation. The MSU SBDC hosts a cybersecurity project to help small businesses with data protection in the wake of COVID-19. Before coming to Mississippi, Ms. Nichols spent 10 years working for the Oklahoma SBDC. Ms. Nichols has an MBA from the Northeastern State University and a bachelor's degree from the University of Central Oklahoma. The Mississippi SBDC was named Resource Partner of the Year for 2020. Congratulations, and welcome, Ms. Nichols.

Our third witness is Ms. Kiersten Todt, the Managing Director of the Cyber Readiness Institute known as CRI located in New York City. CRI provides prescriptive, accessible, and free content and tools to improve the resilience and readiness of small and medium-sized enterprises. Ms. Todt has a master's in public policy from the John F. Kennedy School of Government at Harvard University and earned her bachelor's degree at Princeton University. We appreciate your time and expertise, Ms. Todt.

Now I yield to the Ranking Member to introduce our final witness.

Mr. LUETKEMEYER. Thank you, Madam Chair.

I would like to welcome our final witness, Mr. Graham Dufault. Mr. Dufault is the Senior Director for Public Policy at ACT/The App Association, representing more than 5,000 app makers and connected device companies in the mobile economy. The app association gives voice to small technology companies and its mission is to help members promote an environment that inspires and rewards innovation while providing resources to help them raise capital, create jobs, and continue developing incredible technology. Mr. Dufault is no stranger to Capitol Hill having served as counsel for the House Energy and Commerce Committee. He now leads a number of critical public policy initiatives on behalf of The App Association members. He earned his JD with a concentration in communications law from George Mason University and a bachelor's degree in Economics from Emory University. Mr. Dufault, welcome back to the Hill. And thank you for your participation today. We look forward to your testimony. And you are parking at a very good spot along the street this morning by the way, right across from my apartment. So anyway, thank you, Mr. Dufault for being here. I yield back.

Chairwoman VELÁZQUEZ. The gentleman yields back.

Ms. Cornish, you are now recognized for 5 minutes.

STATEMENTS OF TASHA CORNISH, EXECUTIVE DIRECTOR, CYBERSECURITY ASSOCIATION OF MARYLAND, INC.; SHARON NICHOLS, STATE DIRECTOR, MISSISSIPPI SMALL BUSINESS DEVELOPMENT CENTER; KIERSTEN TODT, MANAGING DIRECTOR, CYBER READINESS INSTITUTE; GRAHAM DUFAULT, SENIOR DIRECTOR FOR PUBLIC POLICY, ACT/THE APP ASSOCIATION

STATEMENT OF TASHA CORNISH

Ms. CORNISH. Great. Thank you again for the invitation to be here.

So CAMI is an approximately 580-member association based in Maryland. We were founded in 2015 to grow the industry. About 80 percent of our members are cyber providers, providing products and services to small businesses and the government. The other 20 percent supports the industry through cyber liability, data privacy law, and other business building resources.

So one of our main roles is to provide business building resources to these cyber companies and the other is to educate small and medium-sized businesses about cyber hygiene and to provide solutions. So I am here specifically to talk about that. I am going to cover three of our programs today: our Cyber SWAT team; our variety of curated directories of products and services; and our advocacy work for financial incentives. Additionally, we do collaborative workshops with our business partners and chambers of erce and other trade associations, and we also do workforce development initiatives to build that critical pipeline of IT and other professionals in cyber.

So our Cyber SWAT team came out of this huge shift to work from home that happened last year. As mentioned before, it really expanded the threat surface that our small businesses experienced. Virtual machines, VPNs and remote access points are commonly high targets for threat actors. So we developed the Cyber SWAT team in partnership with the State of Maryland and it is a coordinated breach response with all components—technology providers, cyber providers, cyber insurance, legal and compliance, and communication and PR. So businesses who are either experiencing a breach or suspected breach can submit their request via email and online form or via the phone. So within 1 hour, they will receive a call from our triage team. We will triage their request to our best fit cyber companies based on their size, location, industry, and breach needs.

So there is no cost to connect with this information, resources, or referrals. They get that 1-hour free consultation. Of course, if they do choose the services, they enter a contract and then pay for those services. But this has helped greatly to assist companies in Maryland and beyond really with external threats such as phishing campaigns and ransomware. And also internal threats, including when terminated employees have unauthorized access to systems.

So moving further upline in the protect and defend section, we provide an online directory of all of our member companies with relevant designations, including minority-owned small businesses, women-owned small businesses, service-disabled veteran-owned small businesses, 8(a), et cetera.

So this is helpful for prime contractors and others looking for subs at government agencies, of course, but also private sector companies who prioritize diverse vendor pools. We also do publications with our local business guides and we are launching a program now with Exelon, a Fortune 100 company that works in every stage of the energy business. I do not need to tell you that there have been some pretty high profile breaches within that industry, and typically that is an industry that has not had a lot of regulations and compliance. So we are working Exelon to connect them through our new database with providers in our membership who can help their vendors build security programs and complete assessments to really secure that supply chain for the energy industry. It is a very highly specialized industry so many of these vendors are seeing this information for the first time so we are pleased to partner with them to do that.

Additionally, we will be doing something similar for our DOD contractors as CMMC or Cybersecurity Maturity Model Certifications come down the pipeline to again provide those resources to our small businesses who are doing government work.

Lastly, I want to touch on some of the financial incentives that we have advocated for. So in 2018, we actively advocated for the Buy Maryland Tax Credit which was approved by the Maryland General Assembly and signed by Governor Hogan. So it offers qualified Maryland businesses fewer than 50 employees to receive a tax credit, which is worth 50 percent of the purchase price when they buy it from qualified Maryland cyber providers of products and services. So qualified sellers are, again, small companies or companies owned by the specific designations. And this offers up to

$4 million worth of tax credits each year and has an active directory of about 50 companies.

Additionally, there are funds that come down from the federal government. So, for example, the Defense Cybersecurity Assistance program, which, again, being in Maryland, we have a lot of government contractors who do work with the DOD so there are specific funds that we help promote that those contractors can use for assessments and remediation. Thank you.

Chairwoman VELÁZQUEZ. Thank you, Ms. Cornish.

Now we recognize Ms. Nichols for 5 minutes.

Ms. Nichols, you need to unmute yourself, please.

STATEMENT OF SHARON NICHOLS

Ms. NICHOLS. It says that I am unstable. Can you hear me?

Chairwoman VELÁZQUEZ. Yes, we can hear you now. Thank you.

Ms. NICHOLS. Thank you. Good morning.

In order to survive the pandemic, many small businesses had to quickly pivot to online platforms to sell their product and shift to remote work. The small businesses of our nation are at high risk for hackers due to the inadequate cybersecurity protection for their data and intellectual property as was discussed before.

Why are they at an increased risk? Just like it was said, owners simply do not know how to protect their business or they lack the funds to do so. Most hackers want money but that is not all that is at risk here. No small business wants its customers or clients to know that they have been breached and it is a fear that they will lose the business or that hard-earned trust. And so many go unreported.

In 2016, it was estimated that 10 to 12 percent of all cybercrimes were reported. In Mississippi alone, in the last couple of weeks, there was a medical clinic in our small town that had to pay a ransom to get their data back. This was never reported in the news. Just 2 weeks ago, our own office was hit by an email phishing scam and I was given an email yesterday in regards to a heating and air company that lost a couple of weeks of work due to a scan.

My name is Sharon Nichols. I am the state director of the Mississippi SBDC where we offer connection, education and guidance for thousands of businesses across the state.

In response to the cybersecurity crisis, the MSBDC allocated a portion of the CARES Act funds we received to develop a cybersecurity center to help Mississippi small businesses become cyber aware and more prepared. This center that was developed offers training based on the CMM model and the CMMC, but we call it the CMM model because we do not do certification, offering actionable steps any business owner can take. Also, access to trained cybersecurity counselors for individual counseling, as well as on-demand cybersecurity workshops that are available on our website. Everything that we offer is for free.

The Cybersecurity Maturity Model that we have implemented is based on a program initiated by the U.S. Department of Defense in order to measure their defense contractors' capabilities, readiness, and sophistication in the area of cybersecurity. And we have adopted this model because it is a tool that can be personalized and expanded to meet each business's unique levels. Levels one through three, and there are five in the CMMC model, are considered attainable by small businesses and are designed to make securing a business affordable, yet very effective.

Please know, again, we do not offer the certification at the end of each level but business owners can pursue that on their own if they choose.

Collaboration and connection in all of our organizations is key and it is the future. The Mississippi Cyber Initiative we call MCI was created to offer a central location for the exchange of ideas and beneficial information about the cybersecurity. The Air Force Base on the Gulf Coast of Mississippi, Mississippi State University, and Mississippi Gulf Coast Community College are part of MCI. Our organization, the Mississippi SBDC has been invited to explore ways MCI resources can be shared with the business community. This is an example of collaboration and connection.

The Mississippi SBDC serves the small businesses of our state with connection, education, and guidance. And I would like to point out how we have applied these guiding principles in response to the cyber crisis. Through connection, we are connecting our business owners with valuable cybersecurity resources via the MSU Cybersecurity Center and MSI into MCI and other collaborations. We are acting as a conduit for the Federal, state, and local resources to the small businesses in our state.

In education, we are utilizing the Cybersecurity Center to educate business owners so that they can evaluate the threat that they have and their threat level and institute measures for protection. We will be employing a variety of marketing platforms reaching out through videos and PSAs and pushing awareness on all six of our social medial channels. We are working to dismantle the idea that small business owners are powerless to take charge of cybersecurity and make the process involved simple, yet effective.

Finally, through guidance, we actively supply support and guidance via our one-on-one counseling with cybersecurity counselors at no cost to business owners. By supplying one-on-one guidance, business owners can get answers to specific questions and solutions unique to their situations. There is no putting the genie back in the bottle. Our lives and livelihoods are connected via the cyberworld.

Small businesses play a huge part in the welfare of our communities and the nation. We must put cybersecurity and cyber safety of our businesses at the forefront of everything that we do and equip them with every tool to succeed and protect their businesses.

I very much appreciate the opportunity to be a voice for the small businesses of Mississippi, as well as the nation. Thank you for inviting me to testify.

Chairwoman VELÁZQUEZ. Thank you, Ms. Nichols.

Ms. Todt, now you are recognized for 5 minutes.

STATEMENT OF KIERSTEN TODT

Ms. TODT. Thank you, Chairwoman Velázquez, Ranking Member Luetkemeyer, and members of the Committee. Thank you for the opportunity to testify before you today.

I currently serve as managing director of the Cyber Readiness Institute, a nonprofit effort that convenes senior executives of global companies to share resources and best practices that inform the development of free cybersecurity tools for small businesses, including the Cyber Readiness Program, a five-step, self-guided program, several guides all based on human behavior.

In 2016, I served as executive director of President Obama's Commission on Cybersecurity, and after the conclusion of the Commission, several of the commissioners and myself came together to launch this effort. Relevant to the hearing today, I also served as a senior staff member on the Senate Homeland Security and Governmental Affairs Committee before, during, and after 9/11 and helped to draft the legislation to create DHS.

The assaults on our nation's digital infrastructure, particularly over the last 12 months, underscore the urgent need to close a critical gap in our nation's cyber defenses. When we think about cybersecurity, we tend to think at a macrolevel, about state actors and state secrets, hacks of millions of online identities, and direct threats to critical infrastructure. And when we think about remedies, we tend to focus on digital giants and on national or multinational policy making. These policy solutions are necessary and appropriate but they are not sufficient. The threats we face as a nation and as individual consumers and citizens are not restricted to the macro level.

Given that over two-thirds of large businesses outsource a portion of their functions and allow third-party access to their data, insufficient cyber protection among SMBs can be consequential for larger firms, too, as we saw with solar winds in Kaseya. SMBs, which are constrained by limited resources and unable to invest proportionately in cybersecurity expand our risk exposure significantly. Eighty percent of America's businesses have fewer than 10 employees, and 95 percent have fewer than 100.

SMBs are the backbone of our economy but they are inherently fragile. During the pandemic, according to the SBA administrator at the time, a small business was closing every hour. These small enterprises lacked the resilience to withstand a barrage of cyber attacks. Small businesses do not have the safety nets that large businesses do. An attack of any size can challenge their viability.

At the end of 2020 and earlier this year, we experienced the impact of several high-profile attacks, with impacts across multiple supply chains and critical infrastructure. We have been forced to now understand that in addition to physical supply chains, all businesses, especially small businesses, must pay attention to their IT supply chains.

These events have brought us to another so-called inflection point. So-called because we use this term frequently when it comes to cybersecurity, yet we continue to fail to do what is necessary to improve America's cyber defenses. These events and attacks are symptoms of the challenges we face. Policies are not enough, nor can we simply shrink tools and techniques employed by major corporations into compact versions for SMBs.

Small businesses need access to cybersecurity resources and support from the federal government. They need prescriptive, easy to adopt programs that strengthen their everyday operations while not pinching their budget. Because a small business may not have a department or even a single employee solely focused on cybersecurity, approaches grounded in creating cultural change through human behavior and education are critical to helping small businesses become more resilient.

Human behavior can be a force multiplier for cybersecurity in small businesses and larger ones as well. Small businesses must be educated on the threats and the fundamental actions that they need to be resilient.

The federal government can play a critical role. Earlier this year, the Cyber Readiness Institute released a white paper, The Urgent Need to Strengthen the Cyber Readiness of Small and Medium Sized Businesses: A Proposal for the Biden Administration, outlining actions to help small businesses. Here are five steps from the white paper that the federal government can take to improve small business cybersecurity defenses.

My prepared testimony goes into greater detail and I am happy to elaborate during our Q&A.

1. Create a Small Business Cybersecurity Center. Today, no single government agency curates cybersecurity resources from multiple vetted sources for SMBs. Given the ongoing work to support SMBs by the Cybersecurity and Infrastructure Security Agency and the recent allocation of additional resources to the agency. CISA is a recommended agency to perform this function.

2.Establish cybersecurity incentives. Tax credits to SMBs that invest in cybersecurity can incentivize cybersecurity efforts.

3.Set cybersecurity standards. We need minimum standards for cybersecurity that all organizations must follow, including small businesses.

4.Launch national cyber squads. We should amplify the existing cyber corps with government-funded cyber squads of student interns to help minority-owned SMBs and to fill a desperately needed talent pipeline.

5.Roll out a national cyber readiness education campaign. Awareness is critical for small businesses in the entire population. We need an effective public service campaign that would focus on a single, basic cybersecurity issue, such as using multifactor authentication which experts assert would reduce cyber attacks significantly.

Our nation's cybersecurity challenges are diverse. One foundational way we can improve our defenses is by supporting and investing in the cyber readiness of small businesses. America's hundreds of thousands of small businesses can be mobilized, educated, and supported to be our resilient frontline of cyber defense and to become a great strength for our country. This critical investment in building that strong defense will pay major dividends for our nation. Thank you.

Chairwoman VELÁZQUEZ. Thank you, Ms. Todt.

We recognize Mr. Dufault for 5 minutes.

STATEMENT OF GRAHAM DUFAULT

Mr. DUFAULT. Thank you, Chairwoman Velázquez, Ranking Member Luetkemeyer, members of the Committee. My name is Graham Dufault, and I am senior director for Public Policy at ACT/The App Association. The App Association is the leading trade group representing small, connected device and mobile software companies in the app economy which is about a $1.7 trillion sector globally that supports about 5.9 million jobs in the U.S., including in your districts.

I am here to ask for your help to improve the cybersecurity resources for small businesses that are the backbone of your districts.

In Brooklyn, Ali Iberraken founded Chaperone, an app to help teachers organize and manage fieldtrips. Jason Oesterly, a former IBM and MasterCard developer created WASHMO Media in Washington, Missouri. So app economy innovators like Chaperone and WASHMO deal with cyber threats all the time. Small companies, even in industries associated with a higher level of technical expertise, like our members, our favorite target is cybercriminals. In fact, about 71 percent of companies reporting cyber attacks are small firms. And around 80 percent of small firms say they are not prepared for a cyber attack. Most of them are reticent to tell anyone about the fact that they are victims as you have heard from other testimony today.

We want to highlight four main things for this hearing.

1. While recent high-profile ransomware attacks are grabbing headlines, it is difficult for small companies to share information about threats, incidents, and defensive measures they use. Legislation like H.R. 1649 and 1649 from last Congress would help create better conditions for information sharing and readiness. So we appreciate the Committee's work on those pieces of legislation and we are pleased to see that at least one of them is being reintroduced this week.

2.Cybersecurity is a team sport in many ways. Small companies, especially app makers, leverage the cybersecurity capabilities of software platforms such as app stores, operating systems, and Cloud services to protect their clients and customers. Federal policy should enable these platforms to take protective measures and to avoid undue interference with them on antitrust and other grounds.

3.Cybersecurity begins with good defenses. Small companies rely on technical protection measures like encryption of data in transit and at rest and on devices, so where is the Committee to push back on proposals that would weaken encryption?

And a bonus,

4.I would be remiss if I did not mention the number one daily issue my industry faces and that is finding and hiring enough qualified people. With about 3.5 million unfilled cybersecurity jobs globally, Federal investment in this area is necessary. So we support programs like the Master Teacher Corps and legislation like the Computer Science for All Act, H.R. 3602.

App Association members and our customers have everything to lose when it comes to cyber threats. The onslaught of recent attacks comes amid a global talent shortage so we cannot simply hire our way out of the problem. Therefore, we need your help.

Cybersecurity for mobile devices is important for everyone. For example, Black and Hispanic Americans rely disproportionately on mobile devices as opposed to desktop computers to access online services. These devices now contain our most sensitive personal data, including financial real-time location and health information. Therefore, app makers in particular must leverage the security features of software platforms and Cloud services. Unfortunately, in some proposals in Congress and in some states that prohibit these gating functions ostensibly to help my member companies and your constituents but in truth they would do much more harm than good. So we urge you to reject those ideas as the make smart devices much less secure and much more attractive targets. Why? Because cybercrime is a business after all. And cybercriminals benefit also from the silence of their victims.

If Congress's goal is to make it harder for cybercriminals to do business, information sharing plays a key role. We need to make it too costly for cybercriminals to target small companies with $15,000 ransoms. The attacks we see on small firms from real estate investment to neighborhood bike shops are often well-designed to ensnare specific kinds of victims. The attackers learn the lingo of the sector they target and study everyday practices to disguise phishing attempts so that they look legitimate. Understanding these shifting forms of camouflage requires rapid intelligence sharing and we need to counterbalance the potential legal exposure and reputational harm of disclosure.

While small companies often rely on outside support and expertise for cybersecurity, it is impossible to contact away risk or accountability for security. It is incumbent on small companies to develop a level of independent working knowledge of cyber threats to their business and information sharing best practices.

The Committee is well-positioned to help improve cybersecurity, literacy for small firms, and the conditions for information sharing, and we look forward to assisting with those efforts.

Thank you for the opportunity to share our views, and I look forward to your questions.

Chairwoman VELÁZQUEZ. Thank you, Mr. Dufault. I will begin by recognizing myself for 5 minutes. I just want to say that it is kind of scary listening to your stories and your expertise regarding the threat of cybersecurity. I would like to ask Ms. Todt, based on your own experience having worked for the federal government, and now as the CEO of this institution, do you think that there is an ongoing education throughout the federal government in terms of different agencies as to the threat that they are exposed to? How does that trickle down to those most vulnerable—in this case, small businesses?

Ms. TODT. Thank you, Madam Chairwoman.

There is absolutely an education challenge. And when we talked to small businesses, and I think this holds true certainly for large businesses, the issue is not that they do not know, they do not want to do anything, the issue is that they often do not know what they should be doing and where the threat is.

There was a survey done by Apple recently that said that many small businesses asked, well, is this not part of my software package, the security piece? And so we have to be more prescriptive. So when we are looking at the Federal agencies, and this is where I think the increase in resources to CISA is going to play a significant role as well as the new leadership working in collaboration across agencies to create a synchronized effort that educates the agencies on the priorities and also creates a unified government approach so that you do not have agencies looking to others to understand what is happening but that there is leadership both within the White House and within CISA that helps to streamline what needs to happen because the threats are certainly consistent across all of our agencies and I think as Chris Inglis, the new national cyber director said in the context of the international arena but it certainly is in the domestic arena as well, in order to get one of us you have to get all of us and I think that approach for government needs to hold true.

Chairwoman VELÁZQUEZ. Thank you.

Ms. Nichols, what were the most common services requested by small business owners in the transition to telework because of COVID-19?

Ms. NICHOLS. You know, I would like to say it was cybersecurity but that was not it. It was mostly sources of capital because they were concerned about how they were going to keep their doors open. And confidence to survive, trying to find out how to handle their financial projections as well as the logistics of employees, Internet connections, suppliers, and commitments. Cyber was not that one thing that they contacted us about. And so while it was the greatest need, it was not what they contacted us about.

Chairwoman VELÁZQUEZ. Ms. Nichols, the SBA rolled out several COVID-19 programs in 2020. Did any of these programs provide cybersecurity specific guidance?

Ms. NICHOLS. To my memory, neither the EIDL nor the PPP programs provided cybersecurity specific guidance. The PPP was primarily for payroll followed by other items, such as rent and utilities and the EIDL had an allowance for accounts payable and other bills but not specific to cyber unless it was already a related expense.

Chairwoman VELÁZQUEZ. Thank you.

Ms. Cornish, with respect to commerce directly, what is the importance of including the designations or certifications small businesses may have as part of the company information?

Ms. CORNISH. Sure. So part of it is for, you know, subcontractors and prime contractors and even government agencies to better diversify the government contracting workforce. Additionally, when our companies are looking at their own DEI plans, many of them want to incorporate diverse vendors in that pool as well. So we are excited to help support those efforts through our designations.

Chairwoman VELÁZQUEZ. Thank you. Do you think that including such designations can promote diversity and cybersecurity contracting?

Ms. CORNISH. Absolutely.

Chairwoman VELÁZQUEZ. Mr. Dufault, recent security breaches have heightened the importance of continuously monitoring against outside threats but the necessary technologies and practices are too expensive for small firms. How much on average is the cost to secure networks?

Mr. DUFAULT. That is a great question. It is one of the main areas of focus that a lot of our member companies have to pay a lot of attention to. I am not sure exactly what the cost is per small company. It probably varies as to what kinds of tools you want to adopt. One of the observations of one of our member companies is that for a lot of really specific cybersecurity focused tools that help you manage your threats across your supply chain, the number of licenses that you have to buy is really high. And so it is kind of you have to buy in bulk, and this particular member company just signed up as a reseller so they could get access to a smaller number of licenses. And so that is potentially a problem and a potential area of focus here to provide more Federal resources so that companies can buy smaller and not necessarily in bulk access.

Chairwoman VELÁZQUEZ. What can SBA and its resource partners do to remove barriers for small firms that want better protection?

Mr. DUFAULT. That is a great question, Chairwoman. There are a few things that you guys can do. We were really happy to see Congress introduce H.R. 1648 and 1649 last Congress. These are bipartisan bills that would help ensure that there are liability protections for information sharing with the government, but also to provide more resources for small companies through the federal government through the SBA to have access to cybersecurity counselors. And so that was H.R. 1649 which has a certification program for SBA employees. So access to that through the SBDCs is something that we feel would be a great improvement and would help them.

Chairwoman VELÁZQUEZ. Thank you. My time has expired.

Now we recognize the Ranking Member, Mr. Luetkemeyer.

Mr. LUETKEMEYER. Thank you, Madam Chair.

Mr. Dufault, you know, one of the things that is concerning to me is the cost to be able to protect the small businesses out there. And so it is a two-part question. The first part of it is what would be the average cost that a small business would have to anticipate occurring to be able to protect themselves? And then the problem becomes, well, you have got to protect it today but there are a lot of smart guys out there that are going to figure out how out how to break into the security you have got right now so you are going to have to continue to update your security and you are always behind the curve, so to speak here in trying to protect yourself. And so these ongoing costs are sometimes things that I think deter small business from even, they throw their hands up and say, well, I probably cannot afford the first set of security measures. I sure cannot continue to pay money out the door when I think my exposure is small. How would you answer that question?

Mr. DUFAULT. So it is a great question, Congressman. I think, you know, one of the member companies described the cost of just trying to get penetration testing, which is kind of an entry level set of services where an outside firm comes in and tests your network. Tests the integrity of the security systems that you are using. And that can cost between $10,000 and $30,000 according to the member company. And that is just the one-time cost. And that is just for that service. So if you want to buy the full suite of services it goes up from there.

Now, we also have member companies that have worked with other customers that have had trouble putting together $200 to pay for antivirus software which is the lowest, sort of the lowest level tool that you can invest in. So it ranges quite a bit, I think, depending on the kind of company you have and your focus and whether or not you are seeing these threats.

Another thing I will point to is the IT sector coordinating council. So DHS has various sector coordinating councils where they focus on cybersecurity in different sectors. The IT sector coordinating council did a survey of small businesses, and about 38 percent said they do not expect to see a cyber incident in the next 2 to 3 years which is a little bit of overconfidence I think. And so there is a baseline level of sort of an appreciation that you have to have in addition to the amount of money that comes along with the basis for spending that kind of money on these protective measures. So on an ongoing basis as you pointed out, it is even harder.

Mr. LUETKEMEYER. Thank you.

Ms. Cornish, you talked about a tax credit that was put together by I think the State of Maryland I think you indicated, which is intriguing to me. But I was curious, what kind of participation rate was there among the small businesses? And what was the average cost that they actually were able to get a credit for? Or do you know that information off the top of your head?

Ms. CORNISH. Sure. I can speak a little bit to that.

So it certainly is not utilized to its full potential by our small business community. So we know that there is work to do on our end to help promote that as well. I think to Graham's point, many of the costs range between $5,000 to about $30,000. There are ways to do continuous monitoring that is a little bit less expensive on the defensive side. So then it only cost about $6,000 to $10,000 a year.

Mr. LUETKEMEYER. One of the things I think, Mr. Dufault, I think back to you again. I think somebody else mentioned, talked about the number of folks within the industry worth 3.5 million jobs, people short to be able to fill the number of folks. What is the problem here? We just do not have enough people interested in the field? The wages are too small to attract people into it? Nobody likes to do that kind of work? What do you think?

Mr. DUFAULT. There are a number of different factors. Some of it is cultural. There is a lack of, I think, awareness of the available jobs. When you are going into college and when I was going into college there was not a whole lot of emphasis on sort of STEM fields at that time. So there is sort of an outreach campaign that can be done to make sure the folks know that this is where high-paying jobs are. It is $89,000 median salary for this kind of work here in the U.S. across the country.

Mr. LUETKEMEYER. Let me interrupt. My time is about up here.

Is this something that Small Business Administration could do? They could entice or enhance or send out information to the high schools and folks, colleges, to let them know that there is availability of all this? I mean, we have to get the SBA engaged in this somehow because this is a small business issue.

Mr. DUFAULT. I think that is a great idea. I think that there is definitely a role for the Small Business Administration there. There are other Federal agencies that ought to be involved but the Small Business Administration in particular because small companies do have trouble finding access to qualified folks.

Mr. LUETKEMEYER. My time is expired. Thank you. I yield back.

Ms. HOULAHAN. The gentleman's time is expired and the gentleman yields back.

The gentleman from Colorado is now recognized for 5 minutes.

Mr. CROW. Thank you, Madam Chair.

For more than 20 years, the SBA Office of the Inspector General has listed IT security as one of the most serious management and performance challenges facing the SBA. So this is not obviously a new thing but it is more acute and becoming more of a problem as particularly nation state actors and others weaponize the ability to go after our small businesses.

Recently, I reintroduced the bipartisan SBA Cyber Awareness Act which would direct the agency to issue an annual report assessing its cybersecurity infrastructure. It also requires the SBA to report cyber threats, breaches, and cyber attacks to the respective House and Senate Small Business Committees. And then to notify affected individuals within 30 days because we know that notification is one of the biggest issues, is the required notification.

So that is part of it. But even after the notification then there is the issue of what happens next? And in all of your testimonies you referenced the challenges particularly facing small businesses that just do not have the resources.

So Ms. Cornish, starting with you, can you describe, flush out for me a little bit more what resources are available, could have the biggest impact on providing resources or support to small businesses particularly in high tech sectors? Like, I have a lot of defense, aviation, and aerospace within my district and a lot of those are small businesses and they are prime targets of hacking and intellectual property theft. What is out there and what could make the biggest impact that is not out there?

Ms. CORNISH. Sure. So in the defense industry, specifically, there is the Defense Cybersecurity Assistance Program which provides funding for assessments, and honestly, you know, investing in the assessment and the protection phase is really where you are going to get the largest ROI for the SBA and others. So I would certainly encourage investment there. When companies are breached, you know, definitely it varies by the situation, but certainly shoring up interventions to improve your chances moving forward are critically important there.

So I would love to see that the DCAP comes down from DOD. I would love to see other agencies also do something similar through their Office of Small Business work.

Mr. CROW. Thank you.

Ms. Todt? Mr. Dufault?

Ms. TODT. Thank you. One of the key issues that we focus on at the Cyber Readiness Institute is human behavior because it recognizes that regardless of the sector that you are in or the resources that you have you have got to start by creating these cultures of behavior. And if we make the analogy to safety, creating cultures of safety that we did with businesses particularly following 9/11, it helps us to understand that while this is all new to us and it is somewhat foreign and uncomfortable, we often say security is not convenient, we can create those cultures. And by doing so, you have force multipliers in your companies when every individual recognizes that he or she can be an access point to the network, that he or she can be the strength that actually prevents an attack or can be the opportunity. And I think that is one of the pieces in the education that we have got to be focusing on to help employees have that accessibility to those resources and the knowledge.

Mr. DUFAULT. Yeah, Congressman. And I agree 100 percent with the comments of Ms. Todt because all it takes is one weak point in a company or an organization and that is why you saw with some of the recent cyber attacks they used the password spray where they try really common passwords on a large number of accounts because chances are in an organization of a couple hundred people or a couple thousand people somebody will use password123. And so creating that culture that Ms. Todt described is extremely important. And also understanding which kinds of threats are being directed to your specific industry because they are kind of, as I said in the oral statement just a minute ago, the attackers are studying the everyday habits and trying to mimic those and they do a pretty good job of that based on specific sectors. So, info sharing within sectors is extremely important.

Mr. CROW. Thank you.

And Ms. Nichols, to you, and I guess to that last point since you are with an SBDC, on the training piece, training of employees and others, how can we better do that or assist small businesses in conducting the training?

Ms. NICHOLS. So we are basing our model on the DOD cybersecurity model, the CMMC, but just using the CMM portion of it. And I liken it to the Maslow's Hierarchy of Needs. Basically, on level one through three is basic cyber hygiene, and it is all about education and awareness, where also I think it is very imperative that we look at what is our consistent voice and what is that consistent messaging because there are a lot of resources out there and a lot of organizations, and I believe that the consistent messaging and education and training is very key not only just for employees but for potential employees because there needs to be that standard base and education.

Mr. CROW. Thank you. My time is expired. I yield back.

Ms. HOULAHAN. Thank you. The gentleman's time is expired and the gentleman yields back.

The gentleman from Texas, Representative Roger Williams, the Vice Ranking Member of the Committee is now recognized for 5 minutes.

Mr. WILLIAMS. Thank you, Madam Chair.

A 2021 Cybersecurity Trend Report shows that phishing is the top cyber threat for small businesses as we have talked today. In this type of attack, simply clicking on a link or opening an attachment can compromise an entire company's network. Rather than target a vulnerability within the cyber network, this tactic targets unknowing employees. Regardless of what additional resources or best practices are shared to the industry, we must ensure that we are not leaving out the socially engineered attacks that can occur on untrained employees.

So Ms. Nichols, first of all, Mississippi State has a great baseball program.

Ms. NICHOLS. Yes, they do.

Mr. WILLIAMS. That is good.

Secondly, can you discuss the training that SBDCs, and we have talked about this a little this morning, have to ensure employees are aware that they could be targets of these phishing attacks?

Ms. NICHOLS. Specifically attacking employees, is that what you are asking?

Mr. WILLIAMS. Yes.

Ms. NICHOLS. Yes. And it is just a matter of awareness. Just like I said in my presentation, our organization had been phished. And it is raising awareness of that basic, what to be ready for and, you know, what are the very basic minimal things that you have to look for. And that is what we want to show our small businesses is how to prepare their employees to work remotely but also keep their intellectual property and their information safe. So the social engineering is really the focus of most training that is going on right now. And while it is at a higher level and you hear about the big ones like the pipeline and different things that have happened, it is the smaller phishing that is really affecting the smaller businesses. So education is key.

Mr. WILLIAMS. Thank you.

When small businesses are targeted with cyber attacks, it may not make the news like some of the more high-profile cases we have seen lately such as the Colonial Pipeline or Microsoft attacks. Unfortunately, since many of these smaller companies operate on tighter budgets, they are often easier targets and then the intruders can go undetected for long periods of time than some of the more established businesses.

So Mr. Dufault, you mentioned in your testimony that smaller firms could leverage the cybersecurity capabilities of Cloud services. Can you elaborate on the advantages of using this service and why it may be a more attractive option for smaller firms who do not have as large of a budget to dedicate to cyber defense?

Mr. DUFAULT. Absolutely, Congressman. It is a great question.

As there was testimony earlier this year in the Homeland Security Committee where witnesses sort of elaborated on the capabilities that Cloud providers have in contradistinction to where you are using on-premises hosted servers. Right? Where if you have your own servers there at the small business, it is incumbent upon you, the small business, to install updates that could have security patches. It is also incumbent on you to sort of on your own go out and find threat indicators and indicators of compromise whereas all that stuff sort of happens quickly and efficiently if you are using Cloud-hosted servers where the updates are sent automatically, that patch potential vulnerabilities, and you also sort of benefit in real time and quickly from indicators of compromise that other folks are seeing that are using the same Cloud services. And so that is sort of what I am referring to when I say the ability to leverage those capabilities.

Mr. WILLIAMS. Very good.

Cybersecurity breaches are only going to become more common as we know and technology continues to advance and criminals get more sophisticated. While small businesses do what they can to protect themselves from attacks that never happened in the first place, it is ultimately the government's responsibility to track down and hold these bad actors accountable. If we use every tool at our disposal to hold these criminals accountable, it will deter these attacks in the future.

Ms. Cornish, are there any roadblocks that are preventing the federal government from more aggressively prosecuting cybercrimes?

Ms. CORNISH. To my understanding, no. But I do——

Mr. WILLIAMS. You believe that?

Ms. CORNISH. I am encouraged by the partnership, the public-private partnership that we are continuing to discuss because I do also believe that that is part of it. But I do not feel like I can speak to the roadblocks specifically at the Federal level blocking that.

Mr. WILLIAMS. Well, public-private partnerships only work better. No question.

I yield my time back, Madam Chair. Thank you.

Ms. HOULAHAN. Thank you. The gentleman's time is expired and the gentleman yields back.

The gentleman from Maryland, Representative Mfume, the Chairman of the Subcommittee on Contracting and Infrastructure is now recognized for 5 minutes.

Mr. MFUME. Thank you very much, Madam Chair. Good morning, everyone.

I have got a question for any of you or either of you who may know the answer should feel free to address. With respect to cyber attacks, what do you estimate the average loss to be as a percentage of overall revenues to small businesses regardless of their size?

Ms. TODT. So based on research and studies that we have conducted with some of our member partners and the larger global companies, we estimate that a cyber breach can cost about $4 million per small business. So when you think about the revenue that small businesses have, sometimes that does not even cover their revenue. And the number of employees, whether it is 2, 20, or 200, the significance of that piece. And I think the challenge for small businesses is their awareness that they are an access point to larger companies but that they also hold data. And data a couple years ago surpassed oil as the most valuable global commodity. And I think these issues for small businesses require the education so that they are not in a position where they are paying $4 million to respond because the recovery takes quite a long time.

Mr. MFUME. And so how many small businesses does that wipe out on an average per year?

Ms. TODT. So there are different statistics around this but what we saw with the pandemic is that over 65 percent of small businesses that suffered a breach did not go back online 6 months later. So that given a 6 month recovery time, those small businesses did not recover.

And I think one of the things that we have learned again, a lot from our large member companies is that the recovery piece to this, it is like a hurricane. We get very involved in the crisis response. It is on the front page of the paper. We are looking to see how everybody is doing. But when you go back 6 months later into the community, or 12 months later, you are seeing long-term and devastating impact. The same is true for businesses, particularly with ransomware attacks because of the impact it has.

Mr. MFUME. And what about 5 years ago. What would you have said that same dollar amount would have been?

Ms. TODT. So I would say it would have been a lot less. I cannot estimate but I think, you know, and I do not even believe that small businesses were the target that they are today. What has happened with IOD and the interdependencies of the digital economy is that small businesses are such critical parts of global supply chains that now to the point that we have all discussed, they are a target because they are the weakest link.

Mr. MFUME. And because of that, do any of you know or are aware of the number of states that offer the kind of tax credit that Ms. Cornish referenced earlier?

Ms. TODT. I am not aware of others. I do not know if——

Ms. CORNISH. I am not either.

Ms. TODT. I do think it is something the federal government could look at.

Mr. MFUME. So let's talk about Maryland since we know about that, Ms. Cornish. You said that that tax credit is being underutilized.

Ms. CORNISH. It is.

Mr. MFUME. Why do you think that is?

Ms. CORNISH. I think partially there is an under awareness among users as well as cybersecurity companies. So we certainly have a cybersecurity audience, so we will continue to promote among our membership and also among our strategic partners and other trade associations and such.

Mr. MFUME. I think it would have to be an aggressive sort of promotion. If you have been around offering a tax credit and people are not taking advantage of it and yet they are being hit by these attacks that we just heard could just completely wipe them out. How are you going to do that over the next few months?

Ms. CORNISH. Yeah. I can certainly reach out to our close partners at the Department of Commerce because I do believe it is a state-driven approach as well.

Mr. MFUME. And I do not know how much time I have left but what, if any of you think the SBA should be doing to lower the threat level? Have you got some concrete suggestions for us?

Mr. DUFAULT. I will take that one, Congressman. That is a great question.

I think the SBA could, number one, provide personnel and a certification program for SBA personnel to get up to speed on the latest cyber threats and be in a position to counsel companies from SBDCs and then provide some funding for those programs on an ongoing basis. That is a great way to do it because SBDCs are a great resource that folks use quite a lot. And then the SBA could also create sort of a hub for information sharing, a little bit like what CISA does through NCCIC at the Department of Homeland Security. And so those are two ways that small businesses could be better supported and help them on a more cost-effective basis deal with——

Mr. MFUME. Mr. Dufault, I get the sense that you have more than two ways to suggest. So could you write those down and transmit those to the Committee? I want to specifically try to follow up with the SBA to make sure that those sort of suggestions get heard outside of this Committee room.

Mr. DUFAULT. That is excellent. Absolutely. We will do that.

Mr. MFUME. Thank you. I yield back, Madam Chair.

Ms. HOULAHAN. Thank you. The gentleman's time is expired. The gentleman yields back.

The gentleman from Minnesota, Representative Hagedorn and the Ranking Member of the Subcommittee on Underserved, Agricultural, and Rural Business Development is now recognized for 5 minutes.

Mr. HAGEDORN. I thank the Chair and the Ranking Member for holding this Committee. Thanks to the witnesses. And Mr. Dufault, one of your members is in our district in Rochester, Minnesota, Southern Minnesota, Advantage Software, and it sounds like they have had a great business for going on 40, 50 years providing farmers with real-time data and inventory and doing all sorts of things that production agriculture really makes a big difference in that type of thing. So we appreciate that work and all the other members that you have going quite something. It seems to me this might be one of these areas again where big government, some politicians think let's impose standards. Let's force the small businesses to do all these things to comply in order to do business with the government and it becomes unreasonable, the mandates. And then they turn around and say, well, let's subsidize it. That is kind of a typical pattern that we see.

But one of the things that bothers me is I am concerned that the agencies sometimes require the contractors, the smaller businesses to comply and do things that they themselves do not do. I mean, I am one of 21 million Americans who had their records stolen from OPM. The Communist Chinese, I guess, know whatever they want to know about me and yet nobody could be sued. There was no liability. The government has a different standard than they impose to others. Do you think small businesses who work in good faith with the government provide the information, do what they can in order to protect themselves and the business operations? Do you think they should have a liability standard similar to the government where they are not sued?

Mr. DUFAULT. Congressman, it is a great question. I think it points to two things. One, Federal agencies need to probably do a better job when it comes to securing their networks. And I think that points then to whether or not my member companies and other businesses across the nation are willing to share threat data and share sensitive, potentially sensitive information that shows what the threats might be with Federal agencies. They do not want that information to be breached.

And then secondly, the other point that you made, whether or not there ought to be some sort of liability protection for information sharing and other measures that my member companies and other companies like them take to make sure that other companies are ready and that other folks in the sector are ready. Absolutely. I think CISA is a great start. I think that other legislation that was introduced last Congress and I think hopefully will be introduced again this Congress would ensure that there is additional liability protections for small businesses because we have to over-come the reputational damage, not just as my fellow witnesses pointed out, the initial problems.

Mr. HAGEDORN. I think most businesses have real incentive to make sure that they can protect their customers and do work. They do not want to lose business. They do not want to go broke. They like to be able to continue to build their business. So your industry is quite fascinating. You said something like $1.7 trillion, all these millions of employees, and that there is all these open jobs—3, 4 million open jobs, some of which are paying $50,000, $60,000, $70,000, $80,000 just to get going.

Can you walk us through what the average person in your industry would do in order to be trained up or get education? And how are some of the small businesses, are they working with them to try to bring them in and pay for some of that?

Mr. DUFAULT. That is a great question, Congressman.

Some of our member companies have just developed their own training programs because they need access to more folks that will write software. And so one of our member companies in Denver created a coding academy and they sort of focus on cybersecurity measures and secure coding. I think that is one of the things that training programs are trying to emphasize right now but write software that is secure at the beginning. It is sort of like what the Federal Trade Commission says about privacy by design. If you are designing a software product, build security into it. And so they have developed training program that have specific focuses like that. We also have a member company, Bit Source in Kentucky that sort of specialized in training former coal miners to code so that they would have a bigger workforce base.

Mr. HAGEDORN. So one bill that we have introduced, I have introduced, is the American Workforce Empowerment Act which would enable people who have 529 education savings accounts to use that for an array of different purposes, not just to go to a 4-year college or whatever. It seems like there could be areas here where folks could utilize those types of money in order to get into your industry. So I would encourage folks to cosponsor that bill and try to get things moving for you. Thanks very much.

Mr. DUFAULT. Thank you.

Chairwoman VELÁZQUEZ. The gentleman yields back.

Now we recognize the gentleman, Mr. Phillips from Minnesota, Chairman of the Subcommittee on Oversight, Investigations, and Regulations for 5 minutes.

Mr. PHILLIPS. Thank you, Madam Chair.

Ms. Cornish, you mentioned the DOD program that makes funding available to contractors to perform assessments and take steps to defend against cyber threats, of course. And we all know that large firms like Intel and Google engage in what are called bug bounty programs that provide rewards for identifying security threats and vulnerabilities on their own platforms. And just last month, CISA had launched the first Federal Civilian Security Vulnerability Disclosure program—boy, that needs an acronym, I think—to work with the hacker community to secure its networks. So would you support the establishment of a fund at SBA or NIST or CISA to support small businesses that want to partner with bug bounty programs and identify and repair weaknesses in their cyber defenses?

Ms. CORNISH. Certainly. That is a wonderful idea.

Mr. PHILLIPS. I like those easy answers. Thank you.

Ms. Todt, how do you feel about that notion?

Ms. TODT. I can continue to make it easy for you. Absolutely, because I think small businesses need to be told not only what to do but what is going on and the reasons behind that. And I think the bug bounty programs help to demonstrate where the threats are coming from. And as Graham said earlier, if they can understand that approach, then they have a better education for their employees, as well as for the businesses themselves.

Mr. PHILLIPS. Wonderful. I appreciate that and happen to feel the same.

Ms. Nichols, I want to thank you for your services that you are providing to your community. You are bridging the gap for a lot of businesses who need guidance about how to protect themselves and their customers from malicious attacks.

Not long ago I Chaired an Oversight and Investigations Subcommittee hearing that examined the challenges facing small businesses seeking to adopt a CMMC certification and enter into Defense Department contracts. At that hearing, we learned that when the initiative is fully implemented, it has the potential, the likelihood to shut out small firms who lack the expertise or resources to navigate that certification process. So if this Committee considers legislation empowering SBDCs to lead cybersecurity outreach to small businesses, how would you recommend that we instruct SBDCs to incorporate guidance about CMMC into their outreach and training?

Ms. NICHOLS. Thank you for the question.

So last year, our association embraced the CMM model and we recognize that we would not ever provide the certification piece of that but we felt that their levels one through three is something that we could embrace on the education piece. And so we have worked with our association to develop a training model to prepare the small businesses so that they will be prepared, maybe not just for the DOD or defense contracts or contracts with the federal government, but also just the general small businesses.

So to prepare the SBDCs, I think that we are already on that pathway because we did recognize that this would be a good partnership and I hope that answered that question.

Mr. PHILLIPS. No, it did. Absolutely.

And I just want to thank our Chairwoman and Ranking Member for holding this hearing. I cannot help but think that this issue is going to grow in importance and it is our responsibility to ensure that small businesses can defend themselves and, of course, their customers.

So with that, I yield back.

Chairwoman VELÁZQUEZ. The gentleman yields back.

Now we recognize the gentleman from Pennsylvania, Mr. Meuser, Ranking Member of the Subcommittee on Economic Growth, Tax, and Capital Access for 5 minutes.

Mr. MEUSER. Thank you, Madam Chairman. And thank you to our Ranking Member.

So, certainly an interesting conversation. Interesting hearing. In 2020, I think it is no surprise to any of us that ransomware attacks were up double, over 102 percent. So let me ask, let me start with Mr. Dufault, if I can.

The cyber attack, cybersecurity insurance I understand is through the roof as far as expense goes. So is there any group plan that any of your organizations perhaps work to try to bring down that cost and create that as an opportunity for businesses?

Mr. DUFAULT. I think, absolutely, thank you for the question, Congressman. Cybersecurity insurance is very expensive. I think Ms. Todt might have a good handle on this as well. But for our member companies, they are looking for affordable options here and they are looking for—and also as Ms. Todt pointed out, $4 million is what it costs a small company to have a cyber incident. So the level of investment and the frequency with which our member companies are targeted kind of leads us to believe that we are going to have to invest a little bit more, even though we are small companies. And so I will just say that, you know, they are willing to invest a lot in cybersecurity insurance and in other measures but we are definitely looking for those plans that will be group plans or other ways of making the risk pool a little more affordable.

Ms. TODT. If I may add to that. So I think cyber insurance, it is a challenging sector right now. The Cyber Readiness Institute has focused a lot on it this year. The challenge is that if you are a small business and you do not have cyber insurance you are often seen as being negligent. But if you are truly evaluating on an ROI perspective, it does not always make financial sense.

There is a great opportunity for the insurance industry to step up to say you have to do these basics in order to be covered. That will both help the premiums stay down and it will also create a momentum shift in doing the basic cyber standards without having to talk about regulation or anything like that. It is the choice. It is like a good driver discount. If you do well by these standards then we will cover you. And I think that is where the insurance industry really has an opportunity to improve what it is doing.

Mr. MEUSER. I imagine the IT companies as well would find some protection measures by charging for added security. And I know that is certainly occurring as well.

In my district it is not like any other. I have many small businesses, medium sized businesses, large businesses getting hit, some more than once. Some pay, some do not. And they work their ways around it but usually at quite a cost. Sometimes just being shut down for 6, 7, 8 days. So it is a serious issue.

I want to just backtrack for a moment. We had a hearing with the Department of Defense, Cybersecurity Maturity Model a few weeks back and we saw that small businesses that made for the defense industry, it was very difficult to get the type of levels of security that they wanted. In fact, I have one business in my business that spent over $100,000 and they are not even exactly sure what level that they are. They think they are at level three. So it is discussed in the Mississippi SBDC how small businesses would, or I guess my question is, are your models helping gain compliance for the DOD?

Ms. NICHOLS. So ours is through education and training because we cannot, and we can also provide guidance so that we can say, you know, here is our situation. We can give them some information. Again, we cannot provide that certification but the education piece, and we have really outlined it so that it is very clear. We have created training specifically right now. All it is posted is for level one because we believe that is basic hygiene. And it is raising that awareness. And to reiterate, it is important that they have that basic understanding so that they can get that certification. A lot of people do not think it is attainable because they do not understand. And if you can educate them that it can be very simple but yet very effective to get them to that level one through level three.

Mr. MEUSER. Okay. All right. Thanks, Ms. Nichols.

Ms. TODT. Congressman, if I may just add a quick point to that because we are actually working with Cyber Hawaii and the Department of Defense to create a primer to help small businesses get ready for CMMC. And it is taking that point where most small businesses are, which is with no understanding, and getting them ready for CMMC. And it is a model that we hope to be able to replicate across the country because it addresses the points that you are calling out which it can be very costly and take a lot of time without the right preparation.

Mr. MEUSER. Last quick question. I am out of time.

Does cryptocurrency affect this whole situation?

Ms. TODT. I think an unregulated monetary currency that is being used for a malicious and criminal act cannot be expected to be a positive force. If we are using cryptocurrency, it should be regulated along other international monetary sources.

Mr. MEUSER. Thank you, Madam Chairwoman, I yield back.

Chairwoman VELÁZQUEZ. The gentleman yields back.

The gentlelady from Illinois, Ms. Newman, is recognized for 5 minutes.

Ms. NEWMAN. Thank you, Madam Chair, and thank you Ranking Member for putting this discussion together. Very helpful. And thank you to our guests, illuminating and really helping us understand the gravity and depth and width of this problem.

So mine is pretty simple, my line of questioning, and I think it is likely for Mr. Dufault or Ms. Todt. So we are looking at all these things to help small businesses. I think all the suggestions today have been fantastic and we should look at it as a Committee for sure to see if there is legislation there to support small business.

My question is the other lane. So deterrence. Right? So how is the SBA and all of these organizations represented here working with law enforcement, whether it is FBI or CIA, once these attacks occur, are they following them? Are they tracking them? Are they investigating? What is happening there? And then do you have any suggestions around deterrents? And what would that model look like?

I will ask Mr. Dufault first.

Mr. DUFAULT. Thank you for the question, Congresswoman.

I think when it comes to the deterrents, one idea that we talked about here and some of the witnesses mentioned was sort of creating a clearinghouse for information sharing through SBA but perhaps co-locating it with Department of Homeland Security so that it is rapid intelligence sharing and that the Federal agencies are on the same page. With that kind of apparatus that kind of says to cybercriminals, well, I guess there is a good mechanism in place for folks to learn about what I am trying to do to deceive my intended targets. And that, in and of itself, can be a little bit of a deterrent because suddenly you are talking, back to cybercrime as a business, you are increasing the cost of the attack because you might have to do a little bit more to try and trick that one person that you need to fool to get into the network. So that can go towards deterrence. And sort of co-locating the SBA center with DHS can help advance threat sharing and SBA's role as just sort of a facilitator of information getting to law enforcement agencies is maybe the appropriate role for SBA as well.

Ms. NEWMAN. And then Ms. Todt?

Ms. TODT. Yes. Building off of that, I think when we can share the techniques, tactics, and procedures, the TTPs with other businesses then they are aware of what needs to happen. And I think that is one of the challenges that we have had, and we saw this with Colonial Pipeline when Colonial did not share what was going on the government was not able to then distribute that TTP that was being used. And, oftentimes, what we learn from large businesses we can apply to small businesses. And so to Mr. Dufault's point, sharing the TTPs.

Also, when we talk about deterrence, we have to prosecute criminals. The biggest challenge we have right now is that ransomware is going to continue to be a very lucrative business because you can do it without getting prosecuted and having any repercussions. And so particularly for small businesses, this is one of the challenges. And this is also why reporting incidents and also when there is ransomware that particularly small businesses have to pay to stay viable, being able to share that with the government so that you can help to prosecute the criminals, this gets us to a better place. Obviously, we have talked about all the liability protections that come with that but we are only going to be better if we have better exchange of the attacks that are being used and the tactics and the techniques.

Ms. NEWMAN. So if I may follow up, and either of you can answer, is it that companies, small businesses are not reporting these? Or is it that when reported they cannot be investigated for whatever reason or are not being investigated? Is it both or is it either?

Ms. TODT. You go first.

Mr. DUFAULT. Yeah, Congresswoman, I think it is both. There is a real reluctance I think among small companies to notify authorities and to notify maybe others of either an unsuccessful or a successful attack, especially the successful attacks because they are sort of an automatic conclusion that folks draw fairly or unfairly that the company that is subject to a successful breach was not taking the proper measures to secure their networks. And so there is a lot of underreporting I think.

Ms. NEWMAN. I think that needs to be a part of any communication or kit that any of your organizations put out, SBA puts out, and we can follow up. And if you can include those recommendations in the recommendations that Congressman Mfume talked about, I think that that would be great for the Committee to take up as a whole. So I do appreciate your work and thank you for sharing today. And I yield back.

Chairwoman VELÁZQUEZ. The gentlelady yields back.

Now we recognize the gentlelady from New York, Ms. Tenney, for 5 minutes.

Ms. TENNEY. Thank you, Chair Velázquez and Ranking Member Luetkemeyer for this, and to our witnesses. I really appreciate you being here.

I have a couple of questions. First, Ms. Cornish, in your testimony you described your newest initiative surrounds the critical lack of skill diverse cybersecurity professionals to protect critical infrastructure and essential services. Do you find that this shortage is in urban and rural communities? And how can we meet those needs? And I am particularly curious because we are looking at rural broadband in our communities and trying not do, based on a municipal level, just like we have municipal electricity and others, and that is going to be particularly interesting to us as we move into that realm. And how is that going to be something your taskforce is going to be looking into?

Ms. CORNISH. Certainly. I think that is a huge challenge, the lack of broadband, especially in rural communities, especially when you are thinking about small and medium-sized businesses. And really, how the workforce is distributed; right? You want to make sure that your rural areas are still competitive for that.

So our main task in the workforce initiatives is really to connect the dots. We have 17 centers of excellence in Maryland alone for cybersecurity, yet we have 19,000 unfilled positions. So for us, it is really creating comprehensive and wraparound services and connecting those who are doing the training with those who really need the work. And to the point made already, in small businesses it can be really challenging to take on that training yourself. It can be challenging to have the manpower to do that training and to support that. So we are really looking to see how we as an association can take away and kind of pool together all of our resources to put less onus on the small businesses who really need that workforce.

Ms. TENNEY. More and more small businesses are going to be depending on this rural broadband that we are trying to explore, and actually, we have a test site in my own community of Sherburne, New York, where we are going to be having municipal broadband opportunities which we are trying to do anything to minimize the risk of cyber attacks which is my concern, and also on this, and I would like to address it to the other witnesses. I know that SBA is going to be designated as the single Federal entity for the small business cybersecurity information sharing.

I have a concern though. I come from New York State and there was a point in time where we consolidated all of our services, including all banking and insurance into the New York State Department of Financial Services and we felt that that could put us at great risk for cyber hacks because the government typically does not have, and the taxpayers are paying for maintenance of this when banks were spending billions of dollars to protect their customers. Because of the liability and insurance was referenced before, how can we make sure that SBA is going to be able to handle this kind of burden and making sure that our small businesses are going to be protected when you are consolidating this type of issue? I do not know if you want to address it, either Mr. Dufault or——

Mr. DUFAULT. Sure, Congresswoman. It is a great question. That is one of the reasons that you see some hesitancy among the member companies and other small companies that are being asked to share data with Federal agencies. The question is, well, we have seen the recent headlines where other Federal agencies and maybe SBA have been the victims of compromise. So they want to be assured, basically, that these Federal agencies are taking the steps that they need to take to ensure that that data is protected adequately and that all of the personnel that work at these agencies are observing the proper protocols because as we have discussed throughout this hearing, all it takes is just the one employee that has the weak password or that otherwise makes the wrong move to compromise the network. And so, anything that the Committee can do to ensure that there are greater resources, more accountability and other levers that would ensure that the agency is taking the proper precautions, those would help our cause quite a lot.

Ms. TENNEY. Yeah. Thank you. Because I have concern as a small business owner. We obviously spend a lot of money in making sure we do not get hacked. We have a lot of heavy data downloads in our business. And so to be hacked at some point and finding out that it is SBA without any duplication of protections or redundant storage areas, where are we going to be? And that concerns me.

I do not know if anyone else wanted to weigh in on it.

Ms. TODT. If I may, Congresswoman. Yes.

Ms. TENNEY. I have got 30 seconds left.

Ms. TODT. Yes. Absolutely. I think certainly when we talk about a single point of success, it is also a single point of failure. But that is really what the new money and the new authorities for CISA are supposed to address. And I believe if we look at agencies, SBA is not going to be the only agency that has this type of responsibility and this type of challenge. And so what we should expect and you are seeing some of the beginnings of this happen already, which is looking at how CISA will work with the agencies to ensure that there is that redundancy and that resilience built in. Because, as we know, small businesses cannot afford to not have that safety net. But again, with those additional authorities, this is not going to be SBA on its own. It will be SBA in collaboration with the other cybersecurity infrastructure and the federal government.

Ms. TENNEY. Thank you. I appreciate it. Great testimony. Thank you.

Chairwoman VELÁZQUEZ. The gentlelady yields back.

Now we will recognize the gentlelady from Pennsylvania, Ms. Houlahan, for 5 minutes.

Ms. HOULAHAN. Thank you, Madam Chair. And thank you to everybody for joining us today. And I think I would like to follow up on many of the different lines of questions that we have heard today. They all seem to have a real common thread. One is to try to understand how much of all of this has to do with just changing culture and changing the ways that people perceive their responsibility and their role in cybersecurity for their companies. I am trying to cess out, you know, that seems to be a very large part of the problem. And then kind of the other 20 percent of the problem seems to be what kind of software and hardware that you should have and you should invest in the types of teams that you should have to be able to protect from the rest of the 100 percent of the universe. My understanding is that is in the thousands of dollars of range in cost. My understanding is that the consequences is in the millions of dollars of range in cost. My other understanding having run and owned and operated a lot of businesses and been responsible for IT is that there is a need for seats or logins for some subset of software that people do not have the ability to afford. Is there any sort of universe where, imagine a cloud, imagine, you know, certified or approved vendors that are part of that cloud that the Small Business Administration can administer or some other organization can administer that would allow you to pick up logins rather than seats so to speak, you know, to be able to defray the costs that small businesses are experiencing in their cybersecurity? Is that something that already exists and I just do not know about it? Is that something that could be useful to design is sort of a clearinghouse of software that would defray the costs for smaller businesses?

And I guess, Mr. Dufault, you seem to be doing most of the conversation on that. And we will start there.

Mr. DUFAULT. Thanks, Congresswoman.

It is a good idea. And I think there could be a role for SBA there, whether it is providing just a grant program or funding or something more hands-on where the agency is sort of designing a fulsome sort of program. So I think it is worth discussing. It is a good idea and I think we would want to just continue to engage on this because it is a need that was identified sort of by a couple of our member companies and that, you know, I think it is worth further discussion probably at this point. Yeah.

Ms. HOULAHAN. Okay. Thank you.

Ms. Todt?

Ms. TODT. Thank you. It is actually something that we are hearing from small businesses at the Cyber Readiness Institute because we do not advocate for vendors but we are hearing we need to have a clearinghouse to know which ones to turn to or at least the general categories. And it is something that we are looking at this year because we want to be prescriptive and not leave everybody in the dark and recognize that when you outsource the function as a small business, you still have a responsibility and you do not outsource the responsibility.

If I may address your question about culture. I do think this is the 80 percent component of cybersecurity, particularly for small businesses. And cultural change takes a lot of time. If we think about, we have all heard the analogies, seatbelts. It was inconvenient for a long time and then you saw the safety requirements. Or if you even make the analogy to physical hygiene and health, we are not doctors, but we have learned over time from doctors that we should have certain tests taken on a regular basis. And so you do not need to be an ID specialist to know that these are the basics that need to happen.

And we have talked a lot about workforce training. And to your point about culture, I think it is important when we see all these cybersecurity positions that people out there recognize it is not just about math and science. Cybersecurity is interdisciplinary and we need capabilities and qualifications in sociology, history, politics, psychology, that those all play into this so that the workforce that we are talking about for cybersecurity is much larger than I think we conceptualize because it is not just math and science.

Ms. HOULAHAN. Ms. Cornish, anything?

Ms. CORNISH. Certainly. We have experience curating these lists by business protocols and also specific needs. So if you would like to speak further about building this clearinghouse, I would be happy to answer that more specifically.

Ms. HOULAHAN. Thank you. I appreciate that.

And with what is left of my time, I want to focus on a piece of legislation that I am a co-sponsor of, the Small Business Development Center Cyber Training Act of 2021, which would certify 5 or 10 percent of the number of employees of a small business development center to provide cybersecurity assistance to small businesses. If enacted into law, this program would provide expertise to small business owners on the proper steps towards cybersecurity.

With my last remaining seconds, what are some of the best practices that SBA could showcase their cybersecurity efforts on? Do you know also similarly of best practices that the DOD has had? How can we encourage interagency best practice sharing?

Ms. TODT. If I may, this is what the Cyber Readiness Program is. We focus on four issues. Strong authentication, which is a pass phrase of 15 characters or more. Phishing training. Not using USBs but instead looking at the cloud. And software updates. Helping individuals understand that every 24 hours they should actually download the patch. Those are our foundation and I am certainly happy to talk to you more about that because this is the core of how we can help small businesses and I commend the act and the legislation.

Ms. HOULAHAN. Thank you.

And with that, I yield back, Madam Chair.

Chairwoman VELÁZQUEZ. The gentlelady yields back.

Now we recognize the gentlelady from California, Ms. Young Kim, Ranking Member of the Subcommittee on Innovation, Entrepreneurship, and Workforce Development.

Ms. KIM of California. Thank you, Chairwoman Velázquez and Ranking Member Luetkemeyer for holding this important hearing. And I want to thank the witnesses for being with us today to discuss the ways of strengthening our cybersecurity for small businesses.

I am very troubled by the increase of cyber attacks. They just seem to be designed not only for monetary purposes but also to instill distrust in our economic system and our institutions. Just between 2019 and 2020, our country saw 400 percent in cyber intrusions. Successful cyber attacks on our small businesses also discourage future entrepreneurs from establishing a small business and creating jobs. Some estimate that 60 percent of small businesses go out of business within 6 months of a cyber incident.

So let's think about that. Cyber attacks are putting 6 out of 10 of our entrepreneurs out of business. So given this urgency of the moment, I was happy to join my colleague, Representative Crow, to introduce the SBA Cyber Awareness Act to find ways to improve the SBA's cybersecurity infrastructure and share information with Congress if there is a reasonable basis to believe that a cybersecurity incident occurred at the administration.

Let me pose the question to all witnesses. Let me start with Mr. Dufault.

In your testimony, you indicated that threat-sharing for small companies is complicated because usually they lack the resources to join and participate in information sharing at analysis centers. Can you elaborate on what can Congress do to incentivize higher participation of small businesses in NCCICs?

Mr. DUFAULT. Thank you, Congresswoman. It is a difficult task to create an incentive that would really cause small companies to participate in a robust way in these information sharing enterprises. One of the ways that we can at least start on that task is to provide potentially additional liability protections at least, right, because the couple of issues that small companies face when they are being asked to share information about the threats that they receive or even incidents that they are victims of is that, number one, the reputational fallout will cost quite a lot of money, over and above the cost of actually remediating the breach, and then number two, it is just a matter of am I going to be liable for anything associated with sharing this information? Whether it is a privacy cause of action or just simply that they did not take the precautions necessary to protect their networks. And therefore, they run afoul of data security laws in the states or at the Federal level, the Federal Trade Commission Act. So it is the liability and the reputation. And so a good start is to help them defray some of that potential liability.

Ms. YOUNG KIM. Ms. Todt, could you briefly elaborate on that, too?

Ms. TODT. Thank you.

I think the other piece is that when we look at the supply chains that small businesses are a part of, there is a responsibility on the larger companies to work with them to incentivize because those large companies, as we saw with solar winds in Kaseya, can be taken down if the small businesses are vulnerable. And there is a better infrastructure of support that can happen within supply chains. And I think as we have seen the interdependencies grow with the digital economy, this is another opportunity to incentivize that engagement, that threat sharing. We work with large manufacturing companies and one of them has put out very specific efforts and information to their small businesses to help them understand where the threats are but also to facilitate that sharing because they know that as a large company, if their small businesses get taken down that will affect them. So there is more responsibility and collaboration that can happen across supply chains than we have seen before.

Ms. YOUNG KIM. Thank you very much.

You know, I am a big proponent of advancing STEM education, especially with underrepresented communities to increase our 21st Century talent pipeline and our economic competitiveness. So I am sure you understand the importance of STEM education and computer science in training and expending our cybersecurity workforce.

How could our small businesses and our economy benefit from increasing the cyber workforce?

Mr. DUFAULT. Thank you, Congresswoman.

One of the most significant problems my member companies face is access to folks that are trained in software development or computer science more generally. And so my member companies would benefit quite a bit I think from investments in K-12 education, but also in workforce development programs.

I mentioned earlier that some of our member companies developed these training programs on their own but there is a role for Federal investment as well and that is why we support the Computer Science for All Act and also the Master Teacher Corps, which is a training program for K-12 educators to provide computer science education.

Ms. YOUNG KIM. Thank you. I see that my time is up. I yield back.

Chairwoman VELÁZQUEZ. The gentlelady yields back.

Now we recognize the gentleman from Louisiana, Mr. Carter, for 5 minutes.

Mr. Carter, you need to unmute.

Mr. CARTER. Yes, thank you.

Madam Chair and Ranking Member, thank you very much for giving us this opportunity for this hearing. Much has been said and many questions have been answered. But Ms. Cornish, if you could perhaps touch on this and any other member, maybe Ms. Todt can as well.

We know that we obviously are concerned about small businesses and making sure that they have the security to operate their businesses via Internet, and cybersecurity is certainly an issue that touches us all. I know my credit card has been breached several times with large companies. I will not say what the company is but I will say that it has been breached. And I know that they have all of the algorithms, all of the security known to man to secure them. I know that cities have had their systems breached. The City of New Orleans has had ransomware. What have we learned from what the large companies are doing that we can pass on to our smaller businesses, best practices, if you will. Even at their highest level of security they have still been caught in ransomware and cybersecurity threats.

Ms. CORNISH. So I would reiterate the importance of human behavior and training of our staff and our employers because in addition to being our largest threat, they are also our largest defenders. So we can empower them to treat data care instead of cybersecurity and empower them to protect the data they are entrusted with.

Additionally, I think the thing that has not been belabored here a lot but as documented policies and procedures, there are many holes that we are missing simply because there are not checklists or we do not really understand all of our assets that we are managing. So I think documentation and training is key in this.

Mr. CARTER. But could you elaborate? If we talk about the larger companies that have a robust security system where they are empowered with significant tools to counteract these threats, yet they are still caught in the lurch, if you will, what can we as Congress, what can SBA, what suggestions would you give us that we can aid in this battle? Because obviously, on many fronts we are losing.

Ms. CORNISH. Sure. I think Ms. Todt's outline of the Cyber Readiness Institute does a great job of how we can empower our employees because, again, that is really our biggest threat.

Mr. CARTER. Ms. Todd, can you weigh in, please?

Ms. TODT. Sure. I think, you know, the good news and the bad news is that these large companies are getting breached by very basic attacks. So when we look at Colonial Pipeline, they were breached because they were not using multi-factor authentication, and they actually did not need to shut down the pipeline. They were just worried about getting paid because their payment system shut down. And so that showed the interdependency of the systems and the importance of separating IT technology with your operations. And so those lessons, the sophisticated attack of a nation state adversary is separate and distinct, but when we have seen the other issues with solar winds and others, those are getting breached through authentication. Through network access. And so what we are talking about for small businesses, obviously at a smaller level, really holds true for the large businesses as well. And that is where I think we have learned the most from these breaches over the last 6 to 12 months is that we have got to create those basic standards in helping businesses do all of those. And this is, again, we talked earlier about where I think insurance companies can play a role and others to have those incentives so that those basics become a requirement for further resilience.

Mr. CARTER. And real quickly before my time expires. As a member of Congress with tons of small businesses throughout my congressional district, what can we do in the way of Town Hall meetings or ways of better educating our small businesses in our communities to utilize these resources? Are there leave behinds? Are there handouts? Are there things that we can do? We often do Town Hall meetings for various issues. This could be one that certainly can benefit our small businesses. What suggestions would either of you have as to how we could better serve and provide resources? You have about 43 seconds.

Ms. TODT. What we have seen, what we are hoping to see with CISA and with SBA is this collaboration of resources focused on human behavior. So taking the work of the nonprofits and making those available to you so that when you go to these town meetings there is a simple, accessible, basic protocol. These are the things you need to be doing on your personal devices as well as your professional devices, an education campaign that does this.

One of the points in my testimony talks about an awareness campaign. If we get every business to use multifactor authentication, the decrease in cyber attacks would be exponential.

Chairwoman VELÁZQUEZ. The gentleman's time has expired.

Mr. CARTER. Fantastic. Thank you very much.

Chairwoman VELÁZQUEZ. Now we recognize the gentleman from New York, Mr. Garbarino, for 5 minutes.

Mr. GARBARINO. Thank you, Madam Chair and Mr. Ranker for holding this hearing.

As the Ranking Member on the Cybersecurity Subcommittee, Department of Homeland Security Committee, I have learned a lot over the last 6 months about cyber attacks and ransomware, which is why I have worked on several pieces of legislation.

Ms. Nichols, this question is for you. Yesterday, I introduced H.R. 4515, the Small Business Development Center Cyber Training Act. I am honored to have the support of my fellow colleagues on the Committee here, Mr. Evans and Ms. Houlahan, and I encourage others on the Committee to co-sponsor this bipartisan piece of legislation.

Small businesses often lack the resources or technical knowledge to prevent cyber attacks, and with the high cost of hiring specialized employees and cybersecurity experts, it can be difficult to bridge the sizeable education gap. My bill would help small businesses get the information they need to implement their own cyber strategy and take appropriate steps in the event of a cyber attack against their business.

Ms. Nichols, given your position as the state director of the Mississippi SBDC, would you share your thoughts and provide feedback on the bill, the Small Business Development Center Training Act, please?

Ms. NICHOLS. Thank you. I have not reviewed the whole bill. I was given a little bit of information this morning in regards to that. However, just like Ms. Todt and several of the other people said, communication and education and the consistent messaging is very key. And I think that raising the awareness to be able to be that voice for the small businesses and given that information, I think we are at this time where we need to create those base standards and create an information—I do not want to say an overload—but be very consistent in how we provide the information to our small businesses.

And as an SBDC, we have to serve all 82 counties of Mississippi and so it is not just rural. It is every aspect. And it does not matter if it is a small business, medium-size business, or large business, they are still at risk. And I think it is very important and we appreciate that the government is passing this legislation or is attempting to in proposing these bills because it is so imperative that our companies are prepared for cyber.

Mr. GARBARINO. And we feel that since you already have the employees and have been coming up with this program where your employees, or at least a number of them are trained to address these cyber issues with small businesses, especially ones that you are helping develop and create and get started up, that this would be very helpful.

I want to move to Ms. Cornish and Ms. Todt. You talked about, in your testimony, Ms. Todt, you talk about doing a tax Credit. Ms. Cornish, you run an agency that deals with tax credits. One thing I have seen is major corporations and governments can spend a lot of money on cybersecurity. Small businesses, they cannot. They cannot hire a dedicated person. And it is not just about best practices. You know, okay, making sure that you change your password. That is one thing that we have to do and CISA has been great with that in coming up with best practices and what businesses and small governments should do, local governments should do. But there is also a cost of keeping your system upgraded. You cannot just buy a good piece, the best piece of equipment today because 6 months from now or 3 weeks from now it is going to be outdated. That is a heavy cost especially for small businesses. Is a tax credit the best way to help offset that cost? What is the best way to do this? And Mr. Dufault, you can jump in, too, if you have an answer.

Ms. CORNISH. For us, it was a great place to start, but certainly, I think there needs to be more incentive, financial incentive, perhaps I heard some mention of grants, projects to get that off the road because, as you mentioned, it does take money to maintain it but there is certainly a lot of startup costs that that could help defray as well.

Ms. TODT. Tax incentives are certainly not the only answer. One of the things that we were looking at particularly with the pandemic was could you use some portion of the PPP loans that could turn into a grant if it were used towards cybersecurity. And so looking at the tools available to small businesses for money to incentivize them to allocate a percentage towards cybersecurity. And I think it is a piece of the pie in all of this and we have just got to find those tools that together can help incentivize small businesses to be motivated to invest and to understand why they need to be, the role that they have and their vulnerabilities.

Mr. DUFAULT. I will mention, Congressman, it is a great question and we are supportive of H.R. 4515. When we were preparing it did not have an H.R. number yet but happy to see that. And we are supportive. We were supportive last Congress, too, of substantially similar legislation. So tax credit is a great idea. I also do not want to underappreciate what our member companies rely on when it comes to a software platform. So app stores and operating systems and the ways in which they harden those systems and ensure that unvetted software is not accessing personal data, not accessing device features and things like that, these are baseline practices that software platforms use and that our member companies sort of rely on at this point to ensure that there is protection from threats in the mobile space in particular. And so that is a piece that I think we want to make sure is on the record here. And so to ensure that the Committee is sort of on the lookout for proposals that would make it harder for companies to use those measures.

Chairwoman VELÁZQUEZ. The gentleman's time has expired.

Now we recognize the gentlelady from Georgia, Ms. Bourdeaux, for 5 minutes.

Ms. BOURDEAUX. Thank you so much. And thank you to our witnesses for joining us to discuss an issue that really is top of mine for many small business owners, and large business owners, which is cybersecurity.

In my home state of Georgia, we saw what happens when critical infrastructure is not secured from cyber attacks when the Colonial Pipeline attack left many of my constituents high and dry at the gas pump for several days. But the Colonial Pipeline is just one rather extreme result of cyber vulnerability. The Department of Homeland Security, Secretary Mayorkas said at a recent event that 50 to 70 percent of cyber attacks are aimed at small to medium-sized companies, costing an estimated $350 million in 2020. And this threat is not going anywhere anytime soon. Ransomware attacks against smaller businesses have increased 300 percent over the past year.

Listening to some of the testimony and discussions today, it occurs to me that there are several ways that you can approach this. And there are a lot of great ideas out there about how to change the behaviors of small businesses, training, you know, all of that kind of outreach. And that is very, very important. But one other way to approach all of this is to require the software that is sold to small businesses or the products that are sold to them to be more conscious of security and ways to protect from breaches.

Ands o I just wanted to check in with I guess Ms. Todt might be a good person to talk on this, are there recommended practices for software developers or for people who are selling to small businesses to help protect them from cyber attack?

Ms. TODT. It is an important question and it is something that we have spent a lot of time looking at. So to your point, right now, the market does not incentivize security. It prioritizes first to market, convenience, ease of use, before security. As a result, we are seeing software go to market that has holes and bugs in it that is not being secure. When you look at the research that has been done, it is absolutely possible to build secure software but the economic incentives are not there.

So I commend what the Biden administration has done in the executive order, which is to look at software transparency, a software bill of materials to understand what goes into it, but as a nation and as a government, we have to create. This is where I do think regulations and standards around building secure software need to be discussed because right now if you look at where the vulnerabilities are coming from, often it is because of holes in the software. The Kaseya attack most recently was a result of that. And we have an opportunity to—we call it secure by design, choose your phrase—but the idea is building that safety and security. Again, if we use the car analogy, we would not think about building a car without an airbag anymore. And we have got to be thinking about safety and security when it comes to software and hardware development.

Ms. BOURDEAUX. Thank you. It is very, very difficult to change individual behavior at massive scale to deal with security. It is much quicker if we could catch it early on through the product itself.

Just kind of on that vein, and I do not know, Ms. Todt, maybe you would have an answer on this or Ms. Cornish, what has been done in terms of the policing side of things? So one of the things we see an awful lot of is we have these attacks and then, you know, we get out from under it somehow, we deal with the ransomware situation, and then what kind of policing capacity do we have or do we need to build up in order to bring people who do this to justice?

Ms. TODT. This is a huge gap in our defense right now because criminal actors are getting away with a lot of attacks. And whether it is a simple lone wolf in the United States or it is a nation state, but we have to be able to prosecute criminals who are committing these types of actions. If you think about Colonial Pipeline again, if someone had put a bomb in that pipeline to prevent the gas and jet fuel from going to the East Coast, we would have no qualms about what to do with that individual. Essentially by shutting down—I live in Virginia so I had a similar—we saw the lines a few blocks down the road. There was an impact and it was a psychological impact because people were afraid. And when we look at that type of impact, we have to think about what are the repercussions for these types of actions? And I think this is something that the United States just should not do by itself. This is where we would look to cooperate with our likeminded economic partners, our allies, to understand what are the boundaries and the lines that are being crossed for criminal actors, and what are the consequences for this type of activity? Because even though we are not seeing the immediate devastating effect if we look at solar winds, the repercussions continue to cascade. And this is why we have to create those boundaries and the definitions around what is a criminal act and what are the consequences for that act?

Ms. BOURDEAUX. Thank you so much.

I yield back the balance of my time.

Chairwoman VELÁZQUEZ. The gentlelady yields back.

Now we recognize the gentleman from Minnesota, Mr. Stauber.

Mr. STAUBER. Thank you, Madam Chair and Ranking Member Luetkemeyer for holding this. And to the panelists who spoke with us today. Very informative.

As we have seen over the last few years, cybercrime is becoming more and more common. The cyber attacks affect our small businesses both directly and indirectly. Most recently as we talked about, the Colonial Pipeline was hacked by the Russians and created a huge gas shortage in the nation. Small businesses that relied on any sort of transportation or travel for daily operations were adversely impacted. While big businesses have the capital to proactively protect themselves from cyber attacks, as well as recover from them, small businesses do not have that same luxury.

And so to the panelists, what can the federal government do to help small businesses protect themselves from and/or recover from cyber attacks? And does this assistance need to look different for small businesses with 10 employees versus 100 employees and so on?

Mr. Dufault, go ahead.

Mr. DUFAULT. Congressman, that is a great question. Congressman Garbarino and Congresswoman Houlahan mentioned a bill that they just introduced which urged folks to support H.R. 4515, which would require the Small Business Administration to develop a certification program for SBA employees and then to deploy them to SBDCs (small business development centers), and to provide cybersecurity expertise and counseling for small companies in the area that they cover.

That is one thing that the federal government can do, and a little can go a long way in that respect because a lot of small companies use SBDCs as sort of a clearinghouse for help in a number of different ways. Now, if you had personnel there that could help with cyber readiness but also, as you said, remediating after a breach, that would be very helpful and that is something that the federal government can do specifically for small companies.

Mr. STAUBER. And I think that it is important to get that small business back up and running as soon as practicable because the days, I mean, you are losing a lot of money each day.

If the other two witnesses would like to comment on that question, please?

Ms. TODT. Sure. In addition to the piece of legislation that was introduced, which just to reiterate, I think really calls upon the resources of the Small Business Administration by using SBDCs and the effectiveness of that. One of the things that we recommend in a white paper at the Cyber Readiness Institute earlier this year was an opportunity to curate the resources that are out there. There are a lot of nonprofits, a lot of organizations that are looking to help small businesses. But if you are a small business, and this goes to another question, that has been attacked, you often do not even now who the first call should be. Is it an IT provider? Is it the local police? And just being able to provide a prescriptive roadmap for small businesses on incident response plans as well as what to do when attacked, I think that this is something that CISA, in coordination with the SBA, could just provide a resource and curate those tools to help small businesses.

Mr. STAUBER. Well said.

Ma' am?

Ms. CORNISH. I would just add to that, having a documented incident plan as mentioned is not often enough. People are in panic. They are not taking the proper channels. So supporting something or exploring something like we have in Maryland as a Federal Cyber SWAT team or, you know, even organizing it maybe at the SBDC level to have a response line to support small businesses when they are going through a breach, to connect them to the different types of resources they need.

Mr. STAUBER. Yeah.

And my last question, and this is specific to cybersecurity, specific. What would you caution the government from doing?

Mr. Dufault?

Mr. DUFAULT. One thing that comes to mind for us is, I mentioned this a minute ago where a lot of our member companies are specifically concerned with security in the mobile space. So what measures are we taking to harden our devices and to prevent unwanted software on our mobile devices? Because these mobile devices now have very sensitive personal information on them. Health care information, financial information, and then real-time location data. So all of the measures that software platforms take, (software platforms like the app stores and the operating systems) to ensure that unvetted software and software that has not been reviewed for security flaws is not inadvertently downloaded via clickbait or some other vector. Those are really important measures to be able to take. So I would caution the federal government not to overreach on antitrust, for example, because these are companies that are larger firms that have a lot of customers and they are sort of in the crosshairs right now when it comes to antitrust. There are proposals in House Judiciary that would make it illegal to take those measures to prevent access to personal data on antitrust grounds. And we are very concerned with those.

Mr. STAUBER. Thank you. My time is up. And thank you very much, and I appreciate this opportunity.

Madam Chair, I yield back.

Chairwoman VELÁZQUEZ. The gentleman yields back.

The gentlelady from Texas, Ms. Van Duyne, Ranking Member of the Subcommittee on Oversight, Investigations, and Regulations, is recognized for 5 minutes.

Ms. VAN DUYNE. Thank you. Thank you much, very much, Chairwoman Velázquez and Ranking Member Luetkemeyer.

Yesterday, the Biden administration announced China was to blame for the sweeping cyber attack on Microsoft earlier this year that left hundreds of thousands of small businesses vulnerable to cyber intrusion. And then just a month ago Russian hackers were able to cripple operations at both the world's largest meat supplier and one of the largest pipelines in the United States. In 2021 alone, cybercrimes could cost $6 trillion, which would make it the third largest global economy.

Cybersecurity, for a number of reasons, is very, very important for small businesses, both real and rapidly intensifying as we have heard today. It is a new way for our adversaries to wage war. Companies need to be ready and we must determine the appropriate role for the federal government in prepping the businesses that we serve as the engine of our economy. And while the need for improved cybersecurity is clear, adding too many requirements can be overly complicated and counterproductive. And one example is the DOD's new cybersecurity assessment framework (CMC). Last month, the Oversight Committee, which I serve as the Ranking Member, we held a hearing to review this program. And one image that just stuck in my mind is the sheer amount of paperwork that was needed for a small business to complete just be certified. One of the witnesses held up this three-ring binder that I swear took him two hands to hold up because it was just so intense. And pretty much most of their guidance was coming from LinkedIn because DOD and SBA simply were not helpful.

So moving forward, we have to make sure that we have simple framework, which is easy to understand, but also , companies need to know how they can be secure, who they can turn to for help and how to respond when they are attacked.

I want to thank the witnesses all for being here today, but I also want to reiterate my concern that we are discussing such a significant small business issue without a representative from SBA present. And if we are going to have a collaborative solution to address this matter, it is crucial that SBA is here to at least demonstrate their willingness to discuss their plans. And I hope they can join us in the future.

Ms. Nichols, in your experience working with small businesses, when they have an issue regarding cybersecurity or they get breached, who do they typically turn to for help? Is it the SBA or a private partner? And who do you believe they should turn to?

Ms. NICHOLS. That is a good question.

When they get to us, they are really not sure who to talk to. They do try to reach to a private industry and to have help with that. Because they do not initially think to refer to the government, specifically SBA, because they do not know the resources that are there and we would like to change that.

Ms. VAN DUYNE. Okay. That makes a lot of sense.

In your testimony, you said the average time—and this will still be for Ms. Nichols—you said the average time to identify and contain breaches is around 120 days. I am sorry, 280 days. Can you explain why it takes this long and how Congress can help to shorten that period?

Ms. NICHOLS. Well, it has to do with they have to find it and they may not be prepared to figure out how to do that so they have to hire and it is very expensive. And it is just like any other IT issue. You have to rule out everything that is going on. And again, I am going to default to this. I am a state director. I do not run the department. And it is very challenging because when you deal with a small business who knows nothing and they have a data breach, that was not what their initial concern is because they are delivering a service. They are trying to make money. And so they are trying to still stay in business and mitigate that data breach and get past that. So that is just going alongside the business. And I am looking at this as a business approach. It does take a long time because they are not going to shut down while they try to deal with this. They are going to try to keep it as far under the table as possible and just keep moving forward. And it does take time. So it does take time for any other type of disaster.

Ms. VAN DUYNE. So, no, I was not being critical that it took so long. I am asking how can Congress help to shorten that period?

Ms. NICHOLS. Oh, I do not know. I do not know. Any other suggestions?

Ms. VAN DUYNE. Yeah. I was not being critical. This is just how long it takes so what can we do to help?

Mr. Dufault, overall small businesses are unprepared when it comes to cybersecurity. A recent report said that 70 percent of small businesses are unprepared for a cyber attack and only about half are allocating any money towards cybersecurity. With small businesses running on such tight margins, especially after a pandemic, how can we make it easier for small businesses to be prepared without breaking the bank?

Mr. DUFAULT. It is a great question, Congresswoman. And again, I go back to H.R. 4515, which would provide some expertise via the Small Business Development Centers for cybersecurity. And by creating a certification program inhouse at the SBA, you are creating a Federal resource that can be, sort of that can reach a lot of small companies via on-the-ground folks that are at the SBDCs. And so that would go some distance toward helping ensure that folks are aware of the current cyber threats but also the best practices that Ms. Todt has referred to on authentication, software updates, and just training around social engineering and phishing scams. So that is what I would point to.

Chairwoman VELÁZQUEZ. The gentlelady's time has expired.

Now we recognize the gentleman from Wisconsin, Mr. Fitzgerald.

Mr. FITZGERALD. Thank you, Madam Chair. Thank you very much.

I do not want to rehash some of the earlier questions and kind of discussions but let me go back to the idea of the cloud and the applications associated with it. So maybe, Mr. Dufault, you could comment.

Obviously, when COVID-19 struck, many of the businesses moved to remote work and it seemed like the only way for them to kind of survive what was going on. But they did switch up kind of their cloud applications at the time. And you know, in some instances that may have helped them streamline kind of their business practices and they may adopt those permanently now; right? But it also increased the security risk is the assumption that is being made by some, not all, who think maybe that is not the case. But you know, do you share those concerns? And you know, I think it is something that small business specifically struggles with because of not necessarily having the resources and the personnel and the ability to kind of track this on a regular basis. So I just wanted you to maybe comment on that.

Mr. DUFAULT. Well, thank you for the question, Congressman. And it is something that we are concerned about. As more work is being done, more education is happening remotely, certainly during the pandemic, and as you said, going forward, more commerce I think, in general is going to be transacted in the cloud and on smart devices. And so it does point to the need as I mentioned earlier for us to allow software platforms, like the app stores and the operating systems to take measures to remove and keep out sideloaded software. That is where you click a link accidentally and it downloads something onto your devices. Those measures in place to keep that software off of the device are really important.

I would also point to the fact that, for example, we have got a member company in the Minneapolis area, Vemos, that provides remote services for restaurants. So you can split a check just with one click on your handheld device. I think there is an assumption that if more of that is happening online and over the Internet, that there are more potential attack surfaces, and so I think that observation is correct and that that should cause us and your Committee to look closely at what the opportunities are to ensure that the threats are adequately being dealt with and that small businesses are taking precautions.

Mr. FITZGERALD. And some of these managed service providers, you know, they are going to have to adapt kind of new, standard operating procedures when it comes to cyber hygiene; right? So I am just wondering, you know, how far behind the 8-ball are we on this stuff? Because it came at us so quickly and now trying to adapt to it, it is probably going to take a while; right? I mean, we just do not have the ability to make this kind of do a 180 like small business is being asked to do.

Mr. DUFAULT. Well, one thing that came up earlier in the discussion was, you know, are people at greater risk if they are using on-premises servers? And that is not necessarily true. And to your point that folks are using the Cloud a little bit more, one of the aspects I pointed to in my written testimony was the fact that if you are using off-premises Cloud services, then you do have access to a faster patches and updates, software updates that can address the newest threats and the newest vulnerabilities. Whereas, if you have on-premises servers, you are manually installing those updates and you are trying to keep up with those threats manually and on your own. And you also do not have access to sort of the real-time updates for indicators of compromise that others are experiencing that are using the same Cloud service.

And so from that perspective, we may be in a little bit better of a position to the extent that we are relying more on Cloud services because we have better access to real-time threat sharing and we have better access to real-time updates to software. So that is one dynamic that sort of cuts the other way that I wanted to point out.

Mr. FITZGERALD. Very good. Thanks for being here today. I yield back, Madam Chair.

Chairwoman VELÁZQUEZ. The gentleman yields back.

Well, thank you again to our witnesses for being here today to testify on this critical topic. Your words have highlighted the significant risks that small businesses face without adequate cybersecurity measures. With more entrepreneurs online and more bad actors looking for targets, cyber preparedness has never been more important. Today's hearing has made it clear that Congress must take an aggressive approach to shield small businesses from cyber attacks. It is also vital that federal agencies and the private sector continue to collaborate on resources, training, and technical assistance to understand and reduce small businesses' cyber vulnerabilities.

I look forward to working with my colleagues on both sides of the aisle to make this happen as we consider three cybersecurity bills at our markup next week.

I would ask unanimous consent that Members have 5 legislative days to submit statements and supporting materials for the record.

Without objection, so ordered.

If there is no further business to come before the Committee, we are adjourned. Thank you.

[Whereupon, at 12:11 p.m., the committee was adjourned.]

APPENDIX

Thank you for the opportunity to provide testimony for the July 20, 2021 hearing entitled "Strengthening the Cybersecurity Posture of America's Small Business Community." The Cybersecurity Association of Maryland, Inc. has 580 member companies and was created in 2016 to grow the cybersecurity industry in Maryland. Approximately 80% of member companies are cybersecurity product and services companies, and 20% are academic institutions, workforce programs, and companies that support the cybersecurity industry (legal, accounting, human resources, banking, etc.).

CAMI is committed to strengthening the cybersecurity posture of small businesses through a variety of programs: the Cyber SWAT team; curated directories of products and services; advocating for financial incentives for cybersecurity investment; collaborative educational workshops; and workforce development initiatives.

In 2020, as companies shifted to remote work, the threat surface for small and medium sized businesses also grew. Virtual machines, virtual personal networks (VPNs), and other remote access technologies regularly top the list for cybersecurity incidents. In response to the growing threat surface and in partnership with the State of Maryland, we provide a coordinated breach response effort that includes all components of a response team -- technology providers, cybersecurity providers, cyber insurance, legal and compliance, and communications and PR. Businesses can submit a request via email, online form, or phone. Businesses will then receive a call from a cybersecurity professional within one hour who will gather additional information and triage their hotline request to the best fit cybersecurity firm based on their size, location, industry and breach needs. There is no cost for this hotline service connecting businesses with information, resources and referrals. Our SWAT team has assisted teams in responding to external threats, including phishing campaigns and ransomware, and internal threats, including terminated employees who compromised systems through unauthorized access.

Our website includes a directory of all members, including any relevant designations (MOSB, WOSB,SDVOSB, 8(a), etc.). Small businesses can filter the list by needed service (policy development, system scan, awareness training, etc.) or industry (finance, healthcare, manufacturing, etc.). Additionally, we produce curated directories in response to the needs of small and medium sized businesses. Annually, we partner with the Baltimore Business Journal to produce the Maryland Cybersecurity Buyer's Guide. This guide includes a subset of our member companies, and includes companies that specialize in working with companies <50 employees. Most recently, CAMI is partnering with Exelon, a Fortune 100 company that works in every stage of the energy business, as they take on a new and bold effort to assist the critical infrastructure vendor community. Specifically, CAMI is connecting Exelon to qualified providers to build a network of business coaches and advisors who can help vendors build their security programs and successfully complete the required assessments. The vendor community supporting utilities is highly specialized and typically does not manufacture or support other business verticals. Therefore, the introduction of risk assessments and "trust but verify" audits is new to this population of vendors. Lastly, in response to the need for 300,000+ DoD contractors to be Cybersecurity Maturity Model Certification (CMMC) compliant, we will be organizing our member companies, and producing a Maryland specific marketplace to facilitate compliance.

CAMI continues to advocate for financial incentives for small businesses investing in cybersecurity services and products. In 2018, Governor Hogan signed the Buy Maryland Tax Credit legislation, which permits businesses with fewer than 50 employees to a tax deduction worth 50% of the purchase price of products/services when they buy from a qualified seller. Additionally, there are funds from the DoD that are available to contractors to perform the necessary assessments and employ remediations for cybersecurity solutions, and we support our partners in MD MEP in promoting this program.

A key factor of our mission is education to our partners. It is very important to socialize the idea of cybersecurity in a way that is relatable to small and medium sized businesses. Through our partnerships with business leagues, Chambers of Commerce, and trade associations, our memberships present educational workshops on highly relevant cybersecurity practices and principles that are vertical-specific or critical for small and medium sized businesses. These workshops are not sales opportunities, and provide baseline knowledge through organizations who already have the trust of small and medium sized businesses.

Our newest initiative surrounds the critical lack of skilled, diverse cybersecurity professionals to protect our critical infrastructure and essential services. Maryland has many training and educational resources, but there is often a disconnect between training and industry needs. With our wide network of partners, we are promoting industry-forward conversations that both inform our training partners of industry best practices and needs, and connect our member companies with existing resources and innovative programming, including apprenticeships.

AMERICA'S
SBDC
MISSISSIPPI

Congressional Testimony

Strengthening the Cybersecurity Posture of America's Small Business Community

Testimony before

Committee on Small Business
United States House of Representatives

July 20, 2021

Sharon Nichols
State Director
Mississippi Small Business Development Center

Chairwoman Velazquez,

Thank you for inviting me to testify today on behalf of not only the Mississippi Small Business Development Center (SBDC) but also America's SBDC. I am the State Director of the Mississippi SBDC. We serve Mississippi through 22 physical locations and soon-to-be added virtual access locations, called Huddle Centers.

We have had the privilege of serving the small businesses and aspiring entrepreneurs of Mississippi for 40 years. Our host for the SBDC program is the University of Mississippi and we work diligently to connect resources of UM, other higher education institutions and state agencies. We serve Mississippi by:

- **Connection** to resources;
- **Education** through training and information dissemination; and
- **Guidance** with one-on-one business counseling and technical assistance.

Brief introduction to MS-SBDC & U.S. SBDC programs

The 62 SBDC networks across the U.S. operate out of host institutions, primarily colleges and universities, and they operate (with some exceptions) statewide. California and Texas are the exceptions having five and four regional networks respectively. Some SBDCs (CO, IL, WV, IN, OH, MT) are hosted by their state departments of commerce or economic development. The host institution manages the operations of its SBDC network through its sub-centers and many of those are at other colleges, community colleges and chambers of commerce. Those host institutions and their partners contribute matching funds that exceed the federal funding. Federal funding for SBDCs is allocated based on population census figures with a minimum funding level established for smaller states (VT, NH, SD, etc.)

Just like many other SBDC networks, Mississippi SBDC is based at the business school of the University of Mississippi and we leverage the skills and knowledge of the professors and students with the practical experience of our business counselors. However, while Mississippi SBDC is headquartered at the University of Mississippi our centers are all over the state's communities. We strive to develop partnerships with local groups to ensure that our services are reaching as many small businesses as possible in all areas of society.

For example, we have recently opened our first Business Resource Center (BRC) located in Gulfport, MS. The Gulf Coast BRC is a physical space, donated by a regional financial institution, to serve the entire Gulf Coast; it serves as a connection to resources for small businesses and aspiring entrepreneurs. The Mississippi SBDC is the hub of this Center with other federal, state and local entities having space and representations. Resources that have space at the Gulf Coast BRC include, but are not limited to: the state

Procurement Technical Assistance Center (PTAC), Veteran's Business Opportunity Center (VBOC), Secretary of State, Mississippi Development Authority (MDA), and a local minority networking group providing training and networking opportunities specifically for minorities and women.

The Mississippi SBDC provides services to small businesses at all stages of development. Over 50% of our clients report that they are in a minority group, roughly 12% are veterans, and 50% are women.

In 2020 we tripled the number of clients we typically serve in a year. That number continues to rise, and we believe several factors contribute to this increase of clients:

- COVID-19 pandemic,
- increased awareness of services, and
- increased collaboration and partnership with other resource organizations.

Cybersecurity and Small Businesses

As the Mississippi SBDC continues to serve the small businesses of the state, Cybersecurity education and guidance have become an essential part of the services we offer. Similar to requests for disaster assistance, we are striving to educate and guide our clients to prepare their businesses in case of a targeted cyber situation. In order to assist in strengthening the cybersecurity posture of Mississippi's small businesses, we have had to clearly define the issue, determine how the Mississippi SBDC can be aligned with other statewide and national efforts, and then formulate our response in providing education and guidance.

THE ISSUE:

Most cyber hacking incidents affecting small businesses are underreported because of fear of lost reputation and reduced trust from the community service areas.

In a report generated by *Verizon*[i], extensive research been conducted to identify common traits of data breaches. Root causes were grouped into three categories:

- **System glitches**, including both IT and businesses process failures;
- **Human error**, including negligent employees or contractors who unintentionally cause a data breach; and
- **Malicious attacks**, which can be caused by hackers or criminal insiders.

This report stated that over 44.24% of all attacks are initiated by out-of-nation attackers.

Root causes of a Data Breach are:

- 52% caused by malicious attack;
- 80% with customers' personally identifiable information (PII) was the most frequently compromised type of record, and the costliest, in the data breaches studied.

This report also stated that the average cost per lost or stolen record is $150 per Customer PII record and $146 across all data breaches. Many small business owners do not have the funds to hire an IT person full time, especially now, coming out of the pandemic. For many small business owners, time is also in short supply. They don't have a lot of extra hours to learn about cybersecurity.

The average time to identify and contain data breaches is estimated to be 280 days.

Examples:

- Local doctor's clinic was hacked, they paid the ransom and it was kept quiet as to not affect their business.
- MS-SBDC email phishing scam (money and time spent on the situation)

MS-SBDC RESPONSE TO THE CRISIS:

America's Small Business Development Centers (ASBDC), including the Mississippi SBDC, are adopting and promoting the Cybersecurity Maturity Model (CMM) as a best practice for small businesses. This North Star CMM is based on Department of the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) with a focus on protecting critical confidential information. We use the CMM (the model), for awareness and direction.

The CMM is composed of best practices from several cybersecurity standards and will act as the roadmap for businesses to use to help organizations implement quality cybersecurity practices and procedures. With this well-constructed roadmap, businesses can write policies that address the practices written in the CMM and train employees accordingly.

Mississippi SBDC allocated a portion of the CARES Act Funds received to create the MS-SBDC Cyber Security Center, a collaboration with Mississippi State University's (MSU) Center for Cyber Innovation (CCI). CCI is led by Dr. Drew Hamilton, a leader in Cyber solutions, to develop solutions for defense, homeland security and the intelligence community. The primary focus of the CCI is to research, prototype and deliver cutting-edge cyber solutions that support global national security, homeland security and peacekeeping operations. While small business support was not part of CCI's mission, the opportunity to align the principles used with the National Institute of Standards and Technology (NIST), and other entities such as Department of

Defense, Department of Homeland Security and the U.S> Intelligence Community, has proven timely and the precursor to innovative discussions on alignment.

CCI's staff, alongside business counselors from Mississippi SBDC and Washington SBDC and with input from America's SBDC, created a framework of education and information that small businesses can use to evaluate their business for the potential of cyber risk. Educating and providing guidance to small businesses in order to mitigate risk is at the core of the Mississippi SBDC cybersecurity initiative.

To date, we have produced CMM Level 1 content in the form of a guidebook, policy workbook, along with three online workshops as On-Demand trainings. To help teach the principles associated with CMM, our workshops center on an *Introduction to Basic Cyber Hygiene* as well as *Cybersecurity and Data Protection.* During these workshops, we stress that regardless of size, small businesses could be in danger to cyber-attacks that can negatively impact their mission.

In addition, we cover the following specific practices in CMM Level 1:

- Access Control
- Identification and Authentication
- Media Protection
- Physical Protection
- Systems and Communications
- Systems and Information Integrity

These have been developed to educate small businesses in Cybersecurity, focusing on mitigation of risk. The development of all materials and training was a collective effort with members of the Washington and Mississippi SBDCs as well as representation from America's SBDC.

Our Mississippi SBDC cybersecurity initiative is not a certifying body and has not affiliation with the CMMC accreditation board (CMMC-AB). As the CMM is discussed, we provide broad guidance on how to protect a business's confidential information.

WHY THE SBDCs

The MS-SBDC is strategically placed to help small businesses assess their cyber security threat level. Due to our unique position, we are a natural link between cyber resources (federal, state and university) and the small business community.

We are the boots on the ground; counselors and directors hear from small business owners every day. We hear first-hand their worries and concerns so we can tailor our services and programs to meet their specific needs.

We have access to the technical information that the business owners need, and can translate it into every-day language that makes it easier and quicker for busy business owners to understand and implement.

GOING FORWARD/NEXT STEPS

Collaboration is the Future! MS-SBDC has been invited to be a part of the ***Mississippi Cyber Initiative (MCI)*** with other state entities such as Mississippi State University, Mississippi Gulf Coast Community College and Kessler Air Force Base to potentially align programming and work with small business needs. The MCI will offer a central location for the exchange of ideas and beneficial information.

The Mississippi SBDC also is developing and deploying video shorts that promote easy ways for businesses to test their cyber security proficiency. Public Service Announcements (PSAs) are also being developed and released across the state that will feature cyber security advice for small business owners distilled into small bites of easy-to-understand and implementable information. In addition, we are connecting with stakeholders to increase awareness for business, industry and municipal sectors.

Cybersecurity impacts businesses and communities. The SBDC national network is poised to serve by providing **Connection, Education** and **Guidance** to meet the needs of small businesses not only for cybersecurity risk mitigation but through many other small business topics the SBDC has offered over the years.

By *Strengthening the Cybersecurity Posture of America's Small Business Community*, we are striving to meet the needs of business owners, at their level of understanding, so that they can focus on the customer and the health of the business knowing they have a cybersecurity plan to protect their reputation as well as loss of trust and funds.

We will continue to keep the lines of communication open with our clients! This and every other plan will pivot to meet their needs – we are at their service.

[i] Verizon, "Expert Cybersecurity Tips for Business" [Online]. Available: https://enterprise.verizon.com/solutions/protect-your-enterprise-from-threats/business-security-tips/ [Accessed: 16-Dec-2020].

CYBER READINESS
INSTITUTE

"Strengthening the Cybersecurity Posture of America's Small Business Community"

Testimony of
Kiersten E. Todt
Managing Director, The Cyber Readiness Institute

United States House of Representatives
Committee on Small Business

July 20, 2021

CYBER READINESS
INSTITUTE

Chairwoman Velázquez, Ranking Member Luetkemeyer, Vice Chair Mfume, and Vice Ranking Member Williams, thank you for the opportunity to testify before you. I currently serve as Managing Director of the Cyber Readiness Institute, a non-profit effort that convenes senior executives of global companies to share resources and best practices that inform the development of free cybersecurity tools for small and medium-sized businesses (SMBs).

The assaults on our nation's digital infrastructure, particularly over the last twelve months, through the compromise of small and medium-sized businesses (SMBs), underscore the urgent need to close a critical gap in our nation's cyber defenses.

When we think about cybersecurity, we tend to think at a macro level – about state actors, and state secrets; about hacks of millions of online identities; about direct threats to critical infrastructure. And when we think about remedies, we tend to focus on digital giants and on national or multinational policymaking. Those policy solutions are necessary and appropriate, but they are not sufficient. The threats we face – as a nation, and as individual consumers and citizens – are not restricted to the macro level. As the saying goes, a chain is only as strong as its weakest link. Today, that chain is our economy's supply chain, and our small and medium-sized businesses (SMBs) are a weak link.

SMBs, which are constrained by limited resources and unable to invest proportionately in cybersecurity, expand our risk exposure, significantly. Eighty percent of America's businesses have fewer than 10 employees, and 95% have fewer than 100. SMBs are the backbone of our economy, but they are inherently fragile. During the pandemic, according to the SBA Administrator, a small business was closing every hour. These small enterprises lack the resilience to withstand a barrage of cyber attacks. Small businesses don't have the safety nets that large businesses do – and an attack of any size can challenge the viability of SMBs.

At the end of 2020 and earlier this year, we experienced the impact of the SolarWinds and Microsoft Exchange attacks. Earlier this year, we have also witnessed the impact of supply chain disruption demonstrated through attacks against Colonial Pipeline and JBS. More recently, we have been forced to understand that, in addition to physical supply chains, all businesses – including SMBs – must pay attention to their IT supply chain. These events have brought us to another so-called "inflection point" – "so-called" because we use this term frequently when it comes to cybersecurity, yet we continue to fail to do what is necessary to improve America's cyber defenses. These events and attacks are symptoms of the challenges we face. Policies are not enough. Nor can we simply shrink tools and techniques employed by major corporations into compact versions for SMBs. Many SMBs are doing what the experts tell them to do – updating and patching software, changing passwords, removing malicious code—but neither they nor we can be lulled into believing that they are doing enough.

SMBs need access to cybersecurity resources and support from the federal government and need prescriptive and easy-to-adopt programs and approaches that strengthen their everyday operations. Because a small business may not have a department or even a single employee solely focused on cybersecurity, approaches grounded in creating cultural change through human behavior and education are critical to helping SMBs become more resilient. Human behavior can be a force multiplier for cybersecurity in SMBs (and larger companies, as well). SMBs must be educated on the threats and the fundamental actions they must take to be resilient.

There are multiple threats to SMBs, but ransomware, phishing, and credential-stealing (password theft) are among the most serious. These threats are only expected to grow as industries continue to take more operations online because of the changing nature of work, post-pandemic. This rapid change has led to gaps in cyber resiliency, as firms, especially those with fewer resources, struggle to keep up. These increasing vulnerabilities are being readily and frequently exploited by malicious actors.

The consequences of a cybersecurity compromise are not only relevant for the company in question but expose other businesses in their supply chain, as well. Given that over two-thirds of large businesses outsource a portion of their functions and allow third-party access to their data, insufficient cyber protection among SMBs can be consequential for larger firms, too – as we saw with SolarWinds and Kaseya. A 2020 report compiled by Accenture found that up to 40% of cyber breaches are indirect, meaning they target weak links in supply chains or business ecosystems.

Our nation's cybersecurity challenges are diverse. One foundational way we can improve our defenses is by supporting and investing in the cyber readiness of small and medium-sized businesses. America's hundreds of thousands of SMBs, mobilized, educated, and supported to be our resilient frontline of cyber defense can become a great strength for our country. The critical investment in building that strong defense will pay major dividends.

The federal government can play a critical role. Earlier this year, the Cyber Readiness Institute released a white paper, “The Urgent Need to Strengthen the Cyber Readiness of Small and Medium-Sized Businesses: A Proposal for the Biden Administration,” outlining actions to help small businesses. Here are five steps, from the white paper, that the federal government can take today that will have expedient and measurable impacts on SMB cybersecurity defenses.

#1: Roll Out a National Cyber Readiness Education Campaign. Awareness is critical. For SMBs and the entire population, we need an aggressive, accessible and easy-to-understand nationwide awareness campaign.

As a nation, we have a long history of using public awareness campaigns to save lives and change behaviors – from forest fires to seatbelt safety, to the post-9/11 “See Something, Say Something” advertisements. Now is the time for a national awareness campaign that focuses on the role of human behavior in cybersecurity and educates everyone about the actions that will make us all secure. There is public support for a government campaign: More than 60% of the U.S. and global SMBs, in a 2021 CRI survey, believe the government should create a national public awareness campaign to promote cyber readiness.

Cybersecurity is a complex area, not easily reduced to a simple message. An effective public service campaign should focus on a single, basic cybersecurity issue – such as using multi-factor authentication, which experts assert would reduce cyber attacks, significantly. Focusing on a single topic with a simple recurring message will help protect SMBs from commonly used methods favored by hackers.

#2: Create an SMB Cybersecurity Center. A national awareness campaign focused on cyber readiness will naturally direct SMBs to a list of available public and private resources. Today, those resources are scattered across several government agencies, sometimes with advice that is too technical for many business owners who do not have an internal IT staff or who outsource cybersecurity. Given the ongoing work for SMBs by the Cybersecurity and Infrastructure Security Agency (CISA), we recommend that CISA is the agency best positioned to be tasked with the curation of cybersecurity resources for SMBs. The agency commissioned to curate resources must also have as its core mission the task of simplifying concepts surrounding cybersecurity to make them understandable and accessible to business owners.

#3: Establish Cybersecurity Incentives. To spur SMB investments in cybersecurity, the federal government should provide an incentive in the form of tax credits. The Treasury Department, in collaboration with the Small Business Administration (SBA) and CISA, should establish guidelines for SMB investment in cybersecurity to qualify for tax credits. While tax credits will reduce the amount of taxable income the government collects, improved cybersecurity will reduce the economic damage done by cyber attackers and have a net positive impact on the security, strength, and resilience of the digital economy.

Working with other agencies and soliciting industry input, Treasury can establish requirements for companies to indicate that they have taken steps to become cyber ready before receiving any tax credit. These standards should require cybersecurity training and education for employees to qualify for the credit. Education should underscore the need to create a culture of cybersecurity in the workplace. Awareness of the risks that come with cyber breaches, and behaviors that mitigate these risks, should be embedded in everyone's actions, from employees to firm leadership so that employees understand their responsibilities, and actions are taken to ensure the organization is cyber ready.

#4: Set Cybersecurity Standards. We can no longer rely on market forces or voluntary actions to improve the cybersecurity of our public and private institutions. Currently, "first-to-market" trumps "secure-to-market." Market forces prioritize profit over security – and enable vulnerabilities, which our adversaries easily expose. This structure is unacceptable and must change. We must create standards that prioritize security in the market. Aligned with an effective education and awareness campaign, market standards for security will help consumers prioritize security, as well.

Establishing standards through industry and government collaboration is vital to securing supply chains. We have successfully established regulations that improve the safety of our roads, health care, and financial systems. We should establish minimum standards for cybersecurity.

There is no one-size-fits-all solution to preparing organizations to be cyber ready. The number of employees, industry, technical knowledge, and financial capabilities are just a few factors that vary by company. But industry and government can work together to establish standards, focused on a risk management approach, that take those factors into account.

#5: Launch National Cyber Squads. A government program funded through grants awarded by the National Science Foundation already exists – CyberCorps: Scholarship for Service. That program, however, is designed to recruit and train IT professionals and cybersecurity managers for positions with federal, state, and local agencies. A new Cyber Squad program would expand the pipeline of talent available to SMBs and will also facilitate engaging different disciplines and expertise in creating cultures of cyber readiness across SMBs.

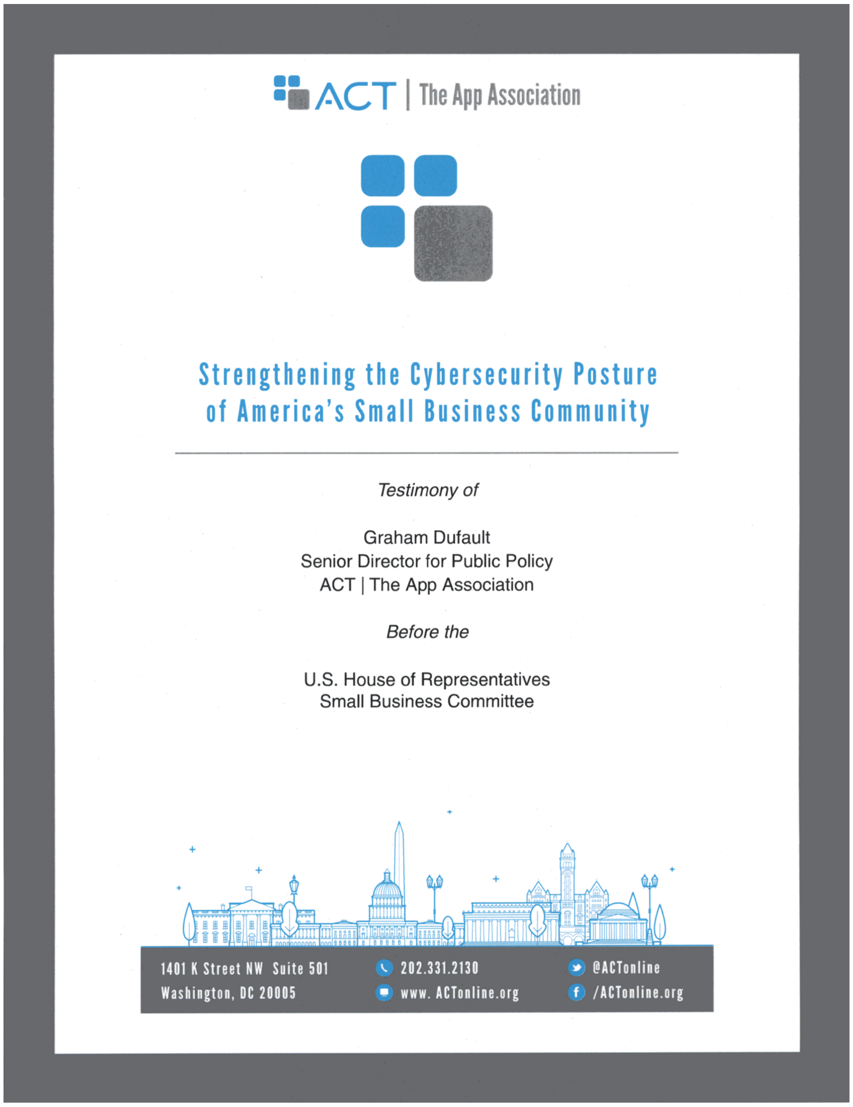
Cyber Squads can address several issues that hinder SMB efforts to become cyber ready – including a talent shortage and a lack of financial resources. A Cyber Squad program modeled after the Peace Corps or a campaign similar to the Science, Technology, Engineering, and Mathematics (S.T.E.M.) education initiative will allow students to explore an interest in pursuing cybersecurity as a career path while providing a connection with their local communities.
In cooperation with community colleges and universities, student interns with expertise in various disciplines would receive additional training in the role human behavior plays in making SMBs secure – issues such as password management, updating software, and phishing awareness – that are not addressed in many cybersecurity programs. Cyber Squads would be sent into the community to help local SMBs improve their cyber readiness. Initially, the program would focus on helping underfunded minority-owned businesses.

CONCLUSION

These recommendations and actions highlight the need for urgent public/private collaboration to address the serious vulnerabilities that put our national security and economic well-being at risk.

The cyber events of the last year demonstrate how our cyber adversaries are increasingly sophisticated in identifying our vulnerabilities and weaknesses and exploiting them. We must bolster our cyber defensive capabilities while continuing to invest in our offense.

SMBs need access to cybersecurity resources that are prescriptive and accessible. Resources, tools, and techniques for SMBs require a different approach from what larger enterprises need. The goal is the same, to create a healthy, protected company, but the path to get there is different. We cannot simply shrink the tools and techniques employed by major corporations into smaller versions for SMBs. We must be proactive in supporting SMBs to become a strength in our ecosystem, not a weakness. They must become more resilient and cyber ready to ensure our nation has a strong foundation and a culture of security.



ACT | The App Association

Strengthening the Cybersecurity Posture of America's Small Business Community

Testimony of

Graham Dufault
Senior Director for Public Policy
ACT | The App Association

Before the

U.S. House of Representatives
Small Business Committee

1401 K Street NW Suite 501
Washington, DC 20005

☎ 202.331.2130
www. ACTonline.org

@ACTonline
/ACTonline.org

Executive Summary

ACT | The App Association (the App Association) is the leading trade group representing small mobile software and connected device companies in the app economy, a $1.7 trillion ecosystem led by U.S. companies and employing 301,030 people in New York and 88,190 people in Missouri.[1] Our member companies create the software that brings your smart devices to life. They also make the connected devices that are revolutionizing healthcare, education, public safety, and virtually all industry verticals. They propel the data-driven evolution of these industries and compete with each other and larger firms in a variety of ways, including on privacy and security protections.

We applaud this Committee for examining the impacts of cyber threats and what Congress can do to ameliorate the cybersecurity posture of small businesses. In recent months, the United States has faced serious cyber incidents targeting a range of victims and through a variety of attack vectors. We can learn much from these incidents, and they should inform the Committee's work in the 117th Congress to equip small businesses with the tools they need to keep Americans safe from cyberattacks. Our message to the Committee is simple and has four components:

- Recent attacks highlight the importance of timely and appropriate disclosure of a cyber incident as well as a strong infrastructure for threat and defensive measure sharing to investigate bad actors. Congress can do more to promote information sharing of threats and defenses—especially for small businesses.
    - For example, we supported previous efforts by this Committee (H.R. 1648 and 1649, 116th)[2] to provide Small Business Administration (SBA) cyber expertise and establish an information sharing channel especially for small businesses.
- Software platforms (app store / operating system combinations) and cloud services play a key role in our cybersecurity posture in the mobile and desktop space; app makers leverage the security features and controls they provide.
- Federal policies should continue to promote the use of technical protection measures (TPMs) like end-to-end and device encryption.
- App Association members suffer from a lack of available software personnel, with about 3.5 million unfilled cybersecurity jobs globally, according to one estimate.[3] We support significant federal investments in workforce development to produce

[1] ACT | THE APP ASSOCIATION, STATE OF THE U.S. APP ECONOMY: 2020 (7th Ed.), *available at* https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf.

[2] Small Business Advanced Cybersecurity Enhancements Act of 2019 (H.R. 1648, 116th); Small Business Development Center Cyber Training Act of 2019 (H.R. 1649, 116th).

[3] 2019/2020 OFFICIAL ANNUAL CYBERSECURITY JOBS REPORT, CYBERSECURITY VENTURES (2021), *available at* https://cybersecurityventures.com/jobs/.

software developers and cybersecurity experts who can meet and exceed today's cybersecurity challenges.

I. Recent Attacks Underscore the Need for Federal Assistance on Cybersecurity

Recent successful ransomware attacks have underscored the need for this Committee to review its role in bolstering cybersecurity for small businesses. For example, on July 2, 2021, hackers associated with REvil exploited a vulnerability in Kaseya's IT management system, Virtual System Administrator (VSA), to perpetrate a massive ransomware heist snaring about 1,500 businesses. Interestingly, Kaseya had almost prevented the incident. On April 1, Dutch Institute for Vulnerability Disclosure identified seven vulnerabilities in VSA, and Kaseya successfully patched four of them before hackers took advantage of one of the remaining three. Although the attack mainly targeted a large firm with lots of clients, many of the impacted businesses are small companies that are either partners that resell Kaseya offerings and provide services around them or are clients of Kaseya.

Small companies have a built-in incentive to protect themselves from cyberattacks like those involving ransomware. Even if a small business can afford to pay the ransom itself, the cost of remediating after an attack can be crippling.[4] And if the financial fallout directly resulting from an attack does not kill a small company, the reputational damage could. Customers went back to Target after its breach, but the same perhaps could not be said for customers of little-known app makers. For small companies, the consequences of an attack can be dire, and they present ample motivation not to be the weak link in any digital supply chain.

a. Information Sharing Challenges

Enhancing information sharing by small businesses is especially important because smaller companies are a favorite target of cyber criminals. Reports suggest that up to 71 percent of cyberattack targets are small companies.[5] Several of our member companies have shared stories about phishing scams and similar attacks, and the App Association itself is an occasional target of social engineering. The fact that a business is small should not prevent it from sharing key information about the attack with those who can make use of it. If they fail to do so, we could be missing a substantial piece of the investigative puzzle. Cyber threats evolve quickly and developing a robust understanding about how cyber criminals design their attacks for various kinds of targets in real-time is a key component to a successful national cyber policy. As Joe Bonnell, founder and CEO of our member company Alchemy Security in Denver, CO,

[4] INST. FOR SECURITY AND TECH., RANSOMWARE TASK FORCE, COMBATING RANSOMWARE (Jun. 2021), *available at* https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.

[5] BEAZLEY, 2019 BREACH BRIEFING 8 (2019), *available at* https://www.beazley.com/documents/2019/beazley-breach-briefing-2019.pdf.

tells us: if anyone in the cybersecurity business took a three-month hiatus, they would have to relearn everything they knew completely. Information sharing and the advanced tools to make it useful are necessary to match the speed of the enemy.

As former Cybersecurity and Infrastructure Security Agency (CISA) Director Chris Krebs recently pointed out, ransomware (like many forms of cybercrime) is a business.[6] Federal policy should therefore focus on prioritizing enforcement to deter ransomware attacks, increasing costs for cybercriminals, while also lowering their expected returns on investment by better preparing government and private sector actors to respond. One key aspect of deterrence and enforcement is empowering all relevant stakeholders to share what they believe to be threat information in a format that works for investigators and in a manner that does not expose sharing entities to undue liability. Threat sharing for smaller companies is complicated, however.

The Department of Homeland Security (DHS) has shared and facilitated cyber threat data sharing for years. But the structure and mechanics of information sharing are complicated. The main private sector information sharing hub, United States Computer Emergency Readiness Team (US-CERT) is a 2003 outgrowth of DHS' Office of Cybersecurity and Communications (CS&C). Now US-CERT is the triage and information sharing branch of CS&C's National Cybersecurity and Communications Integration Center (NCCIC), which is now, as of 2018, a subdivision of the Cybersecurity and Infrastructure Security Administration (CISA). But it is DHS' Office of Intelligence and Analysis (I&A) that deploys field personnel to support the National Network of Fusion Centers (National Network), which accepts and shares threat data at the local level. The portals for private sector entities to receive and share threat data are often private sector-led information sharing and analysis centers (ISACs). However, small and medium enterprises (SMEs) usually lack the resources and wherewithal to join and participate regularly in ISACs. Moreover, most ISACs serve critical infrastructure industries, and most of our members fall outside the definition of critical infrastructure.

So, which arbitrary arrangement of alphabet soup is most important to a small business? When an App Association member company is hit with a cyberattack, whom do they share it with? Somebody at NCCIC? Somebody at their local Fusion Center or an ISAC? Where are these entities, and how should our companies share threat information with them? As with specialized legal and accounting functions, small businesses cannot be expected to maintain in-house cybersecurity expertise. But as Sebastian Holst, chief operating officer of our member company vFortified, points out, while small companies may be able to contract with IT firms to outsource cybersecurity services, they cannot transfer away cybersecurity risks from their business or outsource their own accountability. Sebastian also notes that we cannot expect small businesses to be able to effectively select and leverage outside cybersecurity firms without first

[6] Hearing on "Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis," before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation (May 5, 2021), 117th Cong., 1st Sess. (Statement of Christopher C. Krebs 3-4), *available at* https://homeland.house.gov/imo/media/doc/2021-05-05-CIPI-HRG-Testimony-Krebs.pdf.

having their own independent, working knowledge of cyber threats and information sharing best practices. Small companies will always have ultimate responsibility for the fallout from cybersecurity attacks and, as such, will always suffer the inevitable financial and reputational consequences that follow. And yet, about 83 percent of small companies report that they do not have the capabilities to manage cyber risks. Organizations like the Cyber Readiness Institute provide meaningful materials for small businesses and there is a role for government as well. If federal outreach can help simplify and streamline the learning curve for non-expert small companies, they will be in a better position to secure their businesses, their partners, and of course their customers. Improving small company awareness brings us further down the road to improving information sharing overall to better protect our local economies from threats both here and abroad.

b. Legislative Proposals to Address the Challenges

We commend this Committee for moving legislation in past Congresses to address these issues. Specifically, the Committee unanimously approved H.R. 1648 and H.R. 1649 last Congress. We appreciate that H.R. 1648 designates a single federal entity, the Small Business Administration (SBA), as the information sharing hub for small businesses based in the United States that are not otherwise under a separate information sharing framework. The legislation also appropriately collocates the central Small Business Cybersecurity Assistance Unit (SBCAU) with the existing National Cybersecurity and Communications Integration Center (NCCIC), enabling the agencies to work closely together on the common goal of facilitating threat indicator and defensive measure sharing. The bill also builds on the Cybersecurity Information Sharing Act of 2015's liability protections, clarifying that small businesses sharing covered information with SBCAU are not liable for causes of action arising from actions or inactions associated with sharing such information. If a hacker tries to use a novel behavioral engineering attack on one of our member companies—for example, a specific type of phishing email or communication—the bill would provide an incentive for them to share the relevant information with SBCAU. Investigators could match the attempt with others like it, and it may be the missing piece to prosecute the perpetrators or take other measures to stop them.

Beyond information sharing, H.R. 1648 also bolsters cybersecurity resource materials for small business concerns, including by requiring SBA to coordinate with National Institute for Standards and Technology (NIST) to identify and disseminate information on the most cost-effective methods of implementing the NIST cybersecurity framework; and requiring SBA's Office of Advocacy to ensure that other agencies avoid compromising the cybersecurity posture of small business concerns. The NIST Cybersecurity Framework provides a useful guide for companies to operationalize the management of cyber risk. But Version 1.0 of the Framework is 41 pages, and Version 1.1 is longer, at 55 pages. Small businesses, even in tech-driven sectors like our members, have precious little time and resources to get through dense documents that recommend consultation of more resources—such as "COBIT 5 BAI09.01, BAI09.02,"[7]

[7] Nat'l Inst. Of Standards and Tech, Framework for Improving Critical Infrastructure Cybersecurity 24 (Apr. 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

which provides a system for the inventory of physical devices and systems. Although the Framework is intended to be scalable for SMEs, its complexity is daunting, and the provisions of H.R. 1649 tailoring NIST's and similar materials for small companies is a welcome proposal.

The Committee also took a positive step with H.R. 1649, which would require SBA to create a certification program to certify some of its own employees as cyber counselors. The bill would house the counselors in regional Small Business Development Centers (SBDCs) and require SBDCs to maintain a minimum threshold percentage of staff with cyber counselor certification. Rob Pope, the co-founder and chief technology officer of App Association member Dogtown Media, supports this concept, noting that the majority of small businesses he has worked with recently have no full-time IT staff. He also points out that they are generally confused by available cybersecurity guidance, including the NIST framework. As this Committee and others take steps to enhance federal protections and resources for companies to improve their cybersecurity capabilities, spreading the word about these enhancements is another challenge, and certifying SBA employees in SBDCs can go some distance toward addressing the problem. The bill is a good complement to H.R. 1648 because having cyber experts in the SBDCs can help ensure that small companies across the nation are actually making use of the incentives and information sharing structure in H.R. 1648.

II. Software Platforms and Cloud Services Play a Key Role in Small Business' Cybersecurity Posture

As app makers, our member companies benefit from leveraging the security features in mobile devices and their operating systems, as well as through app store vetting. Our member companies purchase a bundle of services from software platforms—the app store / operating system combination—and that bundle includes security features. For example, app stores currently vet apps for security flaws and facilitate the general distribution of software updates to apps' users. The vetting function is a worthwhile hurdle our member companies clear because it creates an environment in which consumers trust the apps in the store, even when they come from app makers they have never heard of—the common profile of our member companies. Similarly, mobile operating systems generally reject "sideloaded" software that an app store has not vetted and which may contain malware or other defects. Android allows consumers to install unapproved apps, but only if the consumer expressly authorizes installation from a specific source in the device's settings, while Apple's iOS completely disallows unapproved software on the operating system.[8] These are important measures to

[8] Dallas Thomas, "How to Sideload Apps by Enabling 'Unknown Sources' or 'Install Unknown Apps,'" GADGET HACKS (Jan. 24, 2020), *available at* https://android.gadgethacks.com/how-to/android-101-sideload-apps-by-enabling-unknown-sources-install-unknown-apps-0161947/.

protect consumers and enhance App Association member prospects by bringing consumers to the marketplace.

The measures software platforms take to prevent cyber incidents are not based on theoretical risks. Ransomware has migrated to mobile platforms in the form of locker ransomware, which locks a mobile device's user interface and only unlocks upon payment of the ransom. The typical attack involves clickbait or another kind of link that, if clicked, downloads the ransomware onto an Android device.[9] Another observed method is for bad actors to create fake versions of popular apps like Netflix and Candy Crush, entice consumers to sideload them, and use them to circumvent operating system permissions to spy on their targets. These copycat apps have been known to take control of microphones, take screen shots, log keystrokes to steal credentials, and even access messages, contacts, and location.[10] If the device is running a recent version of Android, the attack vectors are limited to sources (e.g., the Chrome browser) the consumer expressly authorized to download software that Google Play has not approved. In the case of iOS, these attack vectors are mainly limited to trying to sneak malicious code by app reviewers because the option to allow sideloading from a specific source is not available.

The ability for software platforms to narrow or close these kinds of attack vectors is crucial to a strong cybersecurity posture for small companies doing business in the mobile space. This is especially true because the worst threats are overseas and outside United States jurisdiction, where they are beyond the reach of federal penalties. Since Congress cannot legislate away this downside risk, it is even more important to empower private sector actors to employ gating practices to protect consumers on smart devices from foreign threats. Therefore, we oppose proposals like the American Choice and Innovation Online Act (H.R. 3816), which would prohibit some of the measures software platforms take to limit attacks on consumers because they could be said to advantage the platform's own offerings over others by limiting free access to consumer data and device and operating system features to all comers. One of the consequences of legislation removing the gating function software platforms provide is to put the onus on consumers to figure out whether they should trust software makers. This result would be highly disruptive to App Association member prospects; in general, consumers are not familiar with small app makers, which do not have the built-in consumer trust large, established brands have. If consumers can trust the app stores and operating systems to prevent malware, consumers are much more likely to download software from a company they've never encountered. Conversely, consumers may generally stop downloading software from unknown companies if they are unable to rely on the app stores and operating systems to prevent and remove malware. We urge the members of this Committee to view proposals like H.R. 3816 with skepticism

[9] Jaime-Heather Schwartz, "How to protect your Android phone from ransomware – plus a guide to removing it," AVIRA (Aug. 13, 2020), *available at* https://www.avira.com/en/blog/ransomware-android-phones.

[10] Danny Palmer, "This Android trojan malware is using fake apps to infect smartphones, steal bank details," ZDNET (June 1, 2021); Lindsey O'Donnell, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks," THREATPOST (April 21, 2020); Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World," CYBEREASON (July 1, 2020).

on the grounds that they would harm the cybersecurity posture and business prospects of small mobile software and connected device companies.

Small firms also leverage the cybersecurity capabilities of cloud services to better protect themselves. As Microsoft president Brad Smith pointed out in February in his testimony on SolarWinds, cloud hosting (as opposed to maintaining on-premises servers) enables better situational awareness and defense measures, especially against the routine—yet recently effective—components of an attack designed to gain incrementally greater levels of access.[11] For example, in the SolarWinds breach, Russian attackers gained access to some credentials by using a "password spray" approach, where attackers try a couple of common passwords on a high volume of accounts. This way, they avoid account lockout triggered by multiple attempts on a single target, and the odds are someone in any given organization is using a common password. As Smith points out, "[w]hen Microsoft's cloud services are attacked, we can detect anomalies and indicators of compromise in ways that are not possible in an on-premises environment." [12] Although on-premises servers are not necessarily inherently less secure, it is simply more resource-intensive to maintain robust cybersecurity protections around them, especially for small companies. For many of them, migrating to cloud services has provided access to the platform-level intelligence on threat and compromise indicators, as well as real-time patches to vulnerabilities that employees would otherwise have to install on their own with on-premises servers.

III. The Statutory and Regulatory Environment Should Encourage Encryption and Similar Technical Protection Measures

Although encryption is not a complete solution by itself, it is an essential tool, especially for SMEs, to protect data. App makers rely on the trust consumers have in their devices and software. Especially in the mobile space, consumers take their most sensitive data with them everywhere on their secure mobile devices. The ability to encrypt these devices without a third party maintaining a separate key or vulnerability is an important aspect of continuing down the path we are on now to unlock the potential of smart devices to handle our finances, manage our health information, and access work. Mandating that messaging providers build "backdoors" into end-to-end encryption—or that device makers keep separate vulnerabilities for device encryption—for the purposes of government access would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. The existence of mandated vulnerabilities like these make the business prospects for cyber crime much more attractive. Hackers might spend hours or days

[11] Joint Hearing on "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and the Ongoing Campaign," before the U.S. House Committee on Homeland Security and the U.S. House Committee on Oversight and Reform (Feb. 26, 2021) (statement of Brad Smith, President and Chief Legal Officer, Microsoft Corp.), *available at* https://homeland.house.gov/imo/media/doc/Testimony-Smith.pdf.
[12] *Id.* at 12.

trying to determine if a vulnerability exists at all and then might give up if they think there is no way in. But if they know it has to exist because the law mandates it, suddenly the resource investment of attacking the service is worth it—eventually someone will discover it.

Occasional calls for "responsible" end-to-end or device encryption are simply not responsible for your constituents and App Association members' customers. This is a lesson we learned with the Clipper chip, which was a mistake that should not be repeated. "Responsible" encryption is just another word for *broken* encryption. In fact, encryption is in many ways a far better tool for crime prevention than investigation. We want to stop the bad guys before they harm your constituents. Not only that, but the federal consensus currently seems to be that strong encryption should either be required or encouraged. The Federal Trade Commission describes encryption of sensitive customer information when transmitting it as a "basic step" to maintain security, confidentiality, and integrity of customer information for financial institutions.[13] Similarly, the Department of Health and Human Services in its Health Insurance Portability and Accountability Act (HIPAA) rules make encryption an "addressable implementation specification" that must be implemented if, "after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard . . ."[14] Weakening encryption to facilitate investigations would also facilitate the success of criminal hackers and limit our ability to keep them out.

IV. Congress Should Continue to Invest in Workforce Development to Expand the Software and Cybersecurity Workforce

Despite providing a median annual salary exceeding $89,000,[15] more than 500,000 computing jobs remain unfilled in America. With just 65,000 U.S. college graduates earning computer science degrees each year on average, recent American graduates are filling a mere fraction of the available computing jobs. Moreover, the number of computer and information technology occupations is projected to grow 11 percent from

[13] Fed. Trade Comm'n, Financial Inst. And Customer Information: Complying with the Safeguards Rule, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[14] U.S. Dep't of Health and Human Svcs., Health Information Privacy FAQs, Is the use of encryption mandatory in the Security Rule?, *available at* https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html.

[15] Computer and Information Technology Occupations, Occupational Outlook Handbook, US Bureau of Labor Statistics, *available at* https://www.bls.gov/ooh/computer-and-information-technology/home.htm

2019 to 2029, much faster than the average for all occupations in the United States—with the number of software developing jobs expected to grow by 22 percent. [16]

That's not to say that some of the solutions to upskilling don't already exist in the private sector: In summer 2020, Microsoft launched its Global Skills Initiative[17] to provide discounted certification exams, technical courses, and online skills courses. As Portia Wu outlined in congressional testimony earlier this year, "Online learning can be a tremendous tool for individuals to gain skills—particularly for those who cannot access education during traditional hours or cannot physically go to learning institutions." The private sector can help, but policymakers must create an environment in which employers and educators can equip those in our current and future workforce with the skills needed to succeed in their jobs. Access to and removing barriers from resources to attain these jobs constitutes a huge part of this effort.

There are several items Congress should consider in supporting the robust development of the American workforce in the 21st century:

- Pass the CHampioning Apprenticeships for New Careers and Employees in TECHnology Act (CHANCE in TECH Act, H.R. 720). This legislation would require the Department of Labor to enter into competitive contracts with intermediaries that manage apprenticeship programs on behalf of employers. By enabling would-be employers to streamline their apprenticeship processes, which many employers need to fully train developers and others, the CHANCE in TECH Act would help connect workers to the employers that need them.

- Appropriate at least $250 million to the science, technology, engineering, and math (STEM) Master Teacher Corps (MTC) program. Our schools' failure to provide computer science courses is rooted in part in a lack of training and professional development for teachers to attain an advanced formal education in teaching computer science. Congress must adequately resource the STEM MTC program to prepare our kids for the jobs of the future and maintain our position as the global leader in tech-driven industries.

- Pass the Computer Science for All Act (H.R. 3602). This legislation would authorize $250 million in new grants to support a diverse tech pipeline in pre-K through grade 12 education. By investing in low-income and underserved communities, the diversity gap in STEM careers can begin to be bridged while encouraging the growth of the next generation of tech talent.

[16] Software Developers, Computer and Information Technology Occupations, Occupational Outlook Handbook, US Bureau of Labor Statistics, *available at* https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm

[17] Global Skills Initiative website: https://opportunity.linkedin.com/skills-for-in-demand-jobs

V. Conclusion

We applaud the Committee's exploration of this issue and appreciate the opportunity to offer our perspective. Our ability to prevent cybercrime depends on how quickly we allow ourselves to move. Information sharing is central to quick action, and this requires close coordination between government, experts, and the private sector. If the conditions are right, small companies like App Association members will set the pace.

Appendix: App Economy Innovators in Your Districts

Majority

Chairwoman Nydia Velázquez (NY-07)
Company: ChAPPerone

Founded by a high school physics teacher after taking 100 sixteen-year-olds on a two-week trip to Spain, ChAPPerone is a platform that allows teachers and chaperones to get important information to students without needing their personal cell phone numbers. The app includes up-to-date alerts and planning functions for before and during the trip.

Rep. Jared Golden (ME-02)
Company: Sephone Interactive Media

Sephone Interactive Media is a web and mobile software development company with a focus on marketing and online brand management solutions. Sephone helps their clients design and launch apps, websites, and digital marketing campaigns, to name a few. Their team of 10 employees has been serving clients in their Maine community and beyond since 2001 and, depending on the size of the project, will contract with developers across the country.

Rep. Jason Crow (CO-06)
Company: Peafowl Inc.

Based in Aurora and founded in 2007, Peafowl is a cross platform app development firm that takes projects from inception to completion through development, design, and testing. Peafowl has a specific focus on digital marketing and creates dynamic websites and mobile applications across several devices and disciplines for their clients. From rapper Nicki Minaj all the way to small businesses like Groundwurk, Peafowl's clients span sizes and industries.

Rep. Sharice Davids (KS-03)
Company: ActiveLogic Labs

ActiveLogic Labs is an innovative digital development agency headquartered in Kansas City with a growing presence across the United States, including an office in the Chicago area. They provide a number of services from web and desktop software development to mobile app development, all with a specific focus on user interface design and a seamless user experience.

Rep. Kweisi Mfume (MD-07), Vice-Chair
Company: Etelligens Technologies

Located in Ellicott City, Etelligens Technologies is a technology firm with a team of more than 100 employees helping businesses leverage technology to improve their customer experience. They offer mobile and web software development, user interface and experience design, as well as digital product development like software as a service (SAAS).

Rep. Dean Phillips (MN-03)
Company: Appikiko, LLC
Founded in 2015 in Excelsior, Appikiko is a mobile app developing business creating both creative and educational apps for consumers. Appikiko is a two-person team responsible for creating seven bright, interactive apps ranging from doodling and creating animated gifs and stickers, to educational K-2nd grade math practice apps.

Rep. Marie Newman (IL-03)
Company: Exemplary Marketing
Founded in 2014 in Tinley Park, Exemplary Marketing is a digital marketing agency focused on social media marketing and mobile app development for their clients. Within these two verticals, they provide an abundance of services including social media growth across Instagram, Twitter, Facebook, and LinkedIn, CRM solutions, IT management, and artificial intelligence solutions and management.

Rep. Carolyn Bourdeaux (GA-07)
Company: Digital Ignition
Founded in 2016 and located in Alpharetta, Digital Ignition is a coworking office space and start up incubator focused on fostering the tech community in North Atlanta. Similar to many coworking spaces, Digital Ignition provides not just an affordable office space, but also access to experienced mentors and investors as well as the ability to meet like-minded entrepreneurs in the area.

Rep. Troy Carter (LA-02)
Company: Jessie Health
Located in New Orleans, Jessie Health's two-person team has worked to create an online marketplace for health services, allowing patients to find the option that is right for them. Their marketplace includes health professionals, products, and services, all tailored to the patient who is able to report their symptoms before being connected to relevant options.

Rep. Judy Chu (CA-27)
Company: Virtualitics, Inc.
Founded in 2016, Virtualitics is a platform that merges artificial intelligence, big data, and virtual and augmented reality to create data visualization experiences. They make data real and actionable, allowing businesses to immerse themselves in the data through VR/AR rather than a traditional two-dimensional format.

Rep. Dwight Evans (PA-03)
Company: The Tactile Group
The Tactile Group is a Philadelphia-based full-service development agency with digital solutions ranging from web and mobile software development to strategic marketing and a strong emphasis on user experience. Their clients are in both public and private sectors, and their projects range from the Philadelphia airport's website redesign to websites for businesses in their community.

Rep. Antonio Delgado (NY-19)
Company: The Mac Works

The Mac Works, located in Bloomington, is a one-man shop providing consulting and technical assistance, primarily on Apple devices and iOS, to businesses looking for expertise on product development and launch. The Mac Works provide services including mobile app development, iOS training, cloud services, and security education and system development for Mac and iOS products.

Rep. Chrissy Houlahan (PA-06)
Company: LMG Web Design

LMG Web Design is a cutting-edge development firm located in Reading with a specialty in customizable web design and branded graphic design. Their team also assists clients with mobile application development with an emphasis on equivalent and seamless user experiences across devices and operating systems.

Rep. Andy Kim (NJ-03)
Company: Micro Integration Services

Founded in 1985, Micro Integration Services is a father and son team who transitioned from selling and maintaining hardware to an entirely software-based consulting business. MIS is focused on solving problems and helping their clients develop software for mobile and web turnkey business solutions. Although they have maintained their two-man team, Micro Integration Services works with major corporations like Kraft and the Philadelphia Eagles.

Rep. Angie Craig (MN-02)
Company: Avionte Staffing and Recruiting Software

Avionte Staffing and Recruiting Software, located in Eagan, provides solutions for payroll, attendance, billing, as well as customer relationship management, new job applications, and onboarding capabilities. Since opening their doors in 2005, they have served more than 900 customers and nearly 25,000 users across the United States and Canada.

Minority

Ranking Member Blaine Luetkemeyer (MO-03)
Company: WASHMO Media, LLC

After working as a developer for nearly a decade at companies like Mastercard and IBM, Jason Oesterly founded WASHMO Media in 2006, offering a range of services including web development and system integrations to local businesses in the area.

Rep. Roger Williams (TX-25), Vice Ranking Member
Company: App Aptitude

App Aptitude has been serving the Austin area since 2008. The team of seven provide a variety of technology related app development services for other businesses working to build out their digital presence. They create custom apps ranging from messaging and IoT to healthcare, e-commerce, and finance.

Rep. Jim Hagedorn (MN-01)
Company: AgVantage Software
AgVantage Software has been providing diverse digital accounting solutions for agribusinesses since 1976 through offerings like live accounting—which allows for inventory management—financial statements, and a variety of other features all available at the touch of a button. Located in Rochester, their software allows businesses to digitally track, analyze, and manage accounting workflows.

Rep. Pete Stauber (MN-08)
Company: Creative Arcade
Located in Duluth, Creative Arcade is a digital marketing agency that specializes in digital marketing and advertising, design and identity, web development, and inbound marketing. With five employees, Creative Arcade has a wide range of clients from West Virginia University to Fairview Range Hospital.

Rep. Dan Meuser (PA-09)
Company: LaunchDM
Located just outside of Reading, LaunchDM is a creative digital marketing studio with six employees that has been around since 1997. LaunchDM has a mix of artists and developers who help businesses with their digital branding through design, social media, web and mobile software development, branding, and search engine optimization (SEO).

Rep. Claudia Tenney (NY-22)
Company: cny apps
Located in Utica and founded by a husband and wife team, cny apps helps local businesses and restaurants connect better with their customers. They create mobile applications across both the App Store and Google Play and serve restaurants, local radio stations, and credit unions.

Rep. Andrew Garbarino (NY-02)
Company: Juiced Tech
Prior to founding Juiced Tech, the co-founders, who also happen to be brothers, had worked at large companies in IT throughout the ‘80s and ‘90s. After realizing that the industry’s growth potential, they founded Juiced Technologies in 2005 on Long Island. Juiced Technologies has now grown to 17 employees and serves primarily as a custom software development firm for businesses of all sizes providing them with apps, websites, and software to help their businesses reach the next step.

Rep. Young Kim (CA-39)
Company: Pegasus One
Based in Fullerton and with development teams across the globe, Pegasus One is a software development company whose services include artificial intelligence, custom software solutions, cloud services, and dev-ops as well as data analytics and intelligence. In addition to their development work, Pegasus One creates detailed case studies highlighting their work with each client and providing insight into the customer’s unique problem, solution, and road map to implementation so that future clients (and fellow developers) can understand their process and learn from their experiences.

Rep. Beth Van Duyne (TX-24)
Company: aTeam-Texas
Founded in 2019 in Southlake, aTeam-Texas is a full-stack software solutions firm that offers several services for their clients. They focus on Amazon Web Services, helping to find businesses experienced contract developers, and custom web and mobile software development.

Rep. Byron Donalds (FL-19)
Company: FieldEdge
Founded in 1980 and located in Fort Myers, FieldEdge is a platform that allows home service contracting organizations to digitally manage customers, work plans and execution, and important financial information. Their product includes features such as scheduling and dispatching, performance, customer management, and provides QuickBooks Integration.

Rep. Maria Salazar (FL-27)
Company: SDSol Technologies
With 68 employees today, SDSol Technologies is a software development firm located in Coral Gables with more than two decades of experience. They serve businesses and startups through the development of mobile apps, IoT products, and other custom web and software solutions. Notably, SDSol Technologies partnered with the University of Miami on a large-scale research project into the cognitive capacity of children in a range of subject domains, their technology providing the backbone of the research and enabling the university's research team to expand their subject pool.

Rep. Scott Fitzgerald (WI-05)
Company: Xorbix Technologies
Founded over 20 years ago with a location in Hartland, Xorbix Technologies is a custom software development firm helping businesses meet their customers online. They offer a number of services such as full-service custom software development, mobile app development, and general IT consulting.

NAFCU

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

July 19, 2021

The Honorable Nydia Velázquez
Chairwoman
Committee on Small Business
U.S. House of Representatives
Washington, DC 20515

The Honorable Blaine Luetkemeyer
Ranking Member
Committee on Small Business
U.S. House of Representatives
Washington, DC 20515

Re: Tomorrow's Hearing, "Strengthening the Cybersecurity Posture of America's Small Business Community"

Dear Chairwoman Velázquez and Ranking Member Luetkemeyer:

I am writing on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in conjunction with tomorrow's hearing, "Strengthening the Cybersecurity Posture of America's Small Business Community." As you are aware, NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve nearly 125 million consumers with personal and small business financial service products. We appreciate the committee's attention to the threats small businesses face in the cyber- and data-security space. We thank you for holding this important hearing and applaud your continued leadership on this matter.

Data security is an important part of the cybersecurity discussion and every time a consumer uses a plastic card for payment at a register or makes online payments from their accounts, they unwittingly put themselves at risk. The pandemic has accelerated payment card use, especially at many small businesses. This has led them to have more access to personal financial data than ever before. Cybersecurity is now more important than ever for them, as both merchants and financial institutions are targets of cyberattacks and data thieves.

However, there is not a national data security standard for retailers, as there is for financial institutions, including credit unions. Financial institutions have been subject to standards on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA) while retailers and many other entities that handle sensitive personal financial data are not subject to these same standards, and they become victims of data breaches and data theft all too often. While cyber- and data-security can be daunting for small businesses, it does not have to be, as standards should be scalable and flexible based on size and risk.

We recognize that finding a legislative solution to cyber- and data-security is a complex issue, and thus have established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to enact legislation to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other depository institutions are required to meet certain criteria for safekeeping consumers' personal information and are held accountable if those criteria are not met through examination and penalties. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers other entities that collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on depository institutions under the GLBA.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by those that retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the negligent entity that incurred the breach.

Thank you for your continued interest in enhancing the security of the small business sector and for holding this important hearing. NAFCU urges Congress to come together in a bipartisan way and put forward legislative recommendations to protect financial institutions and small businesses while ensuring other entities that handle financial data are subject to strong national data security standards.

We thank you for the opportunity to share our perspective on this important topic in advance of this hearing. Should you have any questions or require any additional information, please contact me or Janelle Relfe, NAFCU's Associate Director of Legislative Affairs, at (571) 289-7550.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the U.S. House Small Business Committee

THE NATIONAL CYBERSECURITY SOCIETY

Information Request

From

U.S. House Small Business Committee

July 27, 2021

Prepared By:

The National Cybersecurity Society
1215 31st Street, #3921
Washington, D.C. 20027

INTRODUCTION

The National Cybersecurity Society (NCSS) appreciates the opportunity to submit a statement for the record hearing held on July 20, 2021, "Strengthening the Cybersecurity Posture of America's Small Business Community." As a national nonprofit organization, the NCSS's mission is to enable and empower small and medium businesses to obtain cybersecurity services; assist them in understanding their cyber risk; and advise them on the type of protection needed. We support small businesses through the entire cybersecurity life cycle -- from protect and prevent to respond, recover and remediate. Our paper is focused on the gaps that exist in programs and to highlight the ones that contribute to the safety of small businesses.

STATEMENT OF THE PROBLEM

Small business is the economic backbone of American prosperity. Employing over 58.9 million people and representing 99.9% of the nation's 30.7 million businesses,[1] small businesses are particularly vulnerable to the risks posed by cybersecurity threats. According to the Federal Communications Commission (FCC), crimes involving theft of digital information far surpass theft of physical property. Yet, in the face of this threat, many small business owners naively believe that because of their size, they are not of interest, and therefore not at risk of a

[1] SBA, Office of Advocacy, 2018 small business profile; https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

cybercrime. Many fail to install antivirus software due to cost. Others lack the knowledge or skills to adequately back-up data. One in three have no safeguards at all [2].

Reports are that as many as 50% of the nation's small businesses were victims of hacking in 2016,[3] the results of which can be devasting — a whopping 60% go out of business within 6 months of an attack[4]. According to a report by the U.S. Chamber of Commerce[5], 75% of businesses are self-financed, and when a business fails, the crime directly affects the business owner, his family and his employees. Aligning this statistic with the metric that 60% of businesses fail due to a cybercrime, this crime affects nearly 17 million business owners; and 26 million employees[6] who lose their job when the business fails.

Hackers exploit security loopholes and vulnerabilities, stealing employee and customer data, bank account information and intellectual property. Ransomware has become the leading cybercrime exploit – according to an annual report on global cyber security, there were a total of 304 million ransomware attacks globally in 2020. This was a 62 percent increase from a year prior, and the second highest figure since 2014 with the highest on record being 638 million attacks in 2016.[7]

Business owners are threatened to pay or their digital property will either be stolen, destroyed or published. While cybersecurity experts recommend backing up critical data at

[2] https://www.manta.com/resources/small-business-trends/small-business-owners-protecting-cyber-attack/?dest=%2Fresources%2Fsmall-business-trends%2Fsmall-business-owners-protecting-cyber-attack%2F

[3] https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf

[4] Press Release, Congressman Chris Collins' Subcommittee on Small Business Cyber-security Challenges, 2013

[5] U.S. Chamber of Commerce, Small Business Statistics, https://www.chamberofcommerce.org

[6] SBA, Office of Advocacy, 2018 small business profile; https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

[7] Statisca, https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/#:~:text=According%20to%20an%20annual%20report,638%20million%20attacks%20in%202016.

least once a week[8] and not paying the ransom[9], many business owners find that they have not backed up their data sufficiently, nor tested their ability to recover from a cold stop. Therefore, many business owners discover they have no other recourse but to pay the ransom.

Ransomware directly affects the business owner, since in most cases (75%) of their personal funds[10] created the business; their reputation is on the line; and their employees depend on the business owner to pay to maintain their employment.

When the business pays the ransom with the hopes of recovering the data, the business owner experiences severe personal financial harm – ransoms lately are now in the millions vice a few thousands a few years ago. Another similar cybercrime is business email compromise, which often targets the email of the CEO/business owner. According to the FBI, business email compromise and email account compromise represents a significant source of financial loss, accounting for nearly $12.5 billion between October 2013 and May 2018.[11] How this works – the email account of the CEO/business owner is taken over; the criminal threatens the business owner to pay a ransom; or their sensitive data will either be destroyed, manipulated or published on the web. One of the first business owners the NCSS helped was a busines owner with a business email compromise attack. A disgruntled employee gained access to the business owner's email account and funder list (owner was a nonprofit) and sent disparaging remarks to the entire funder list. The remarks were so damaging that although the business owner tried to reach out to her charity's supporters, many were so taken back that they rescinded their

[8] Total IT, https://totalit.com/how-often-should-you-perform-a-data-backup/#:~:text=Important%20data%20should%20be%20backed,of%20the%20day%20or%20week.

[9] Find Chris Wray testimony from week 6/9/2021

[10] Chamber of Commerce, Footnote #5

[11] Secureworks, State of Cybercrime Report, 2018.

financial support. The nonprofit had to close because it was impossible to regain the confidence of her supporters and the nonprofit's reputation. She reached out to the FBI and local law enforcement who were at a loss as to what to do, other than fire the employee, which she had done. Frustrated, she decided to close the nonprofit, it was impossible to recover her reputation.

Business owners can report a cybercrime to the Internet Crime Complaint Center (IC3) which collects complaint data, but does not investigate crimes. The Federal Trade Commission (FTC) collects data on identity theft and other scams, but does not collect data on business-specific cybercrimes. The FBI will only get involved when the loss exceeds $500,000 and local law enforcement may or may not respond, depending on local resource constraints.

These limitations are both recognized and understood. When asked who a victim should contact in the wake of a cybercrime, the response from the Obama Administration's Cybersecurity Coordinator was..."we are still trying to figure that out". Right now, there is really no one to call and nowhere to obtain assistance. Victims lose financially, as well as materially - they can lose their reputation, their ability to rebuild (due to compromised credit worthiness) and lose their unique intellectual property - which is at the core of our nation's global competitive advantage. Embarrassed, confused about where to turn, and fearful of legal, regulatory or reputational retaliation, many business owners pay the ransom.

Direct service to cybercrime victims is limited to none. The Identity Threat Resource Center provides direct service to victims of identity theft. The Cybercrime Support Network (CSN) provides information about scams to both consumers and businesses, but does not provide direct support. Some state 211 help desks have been augmented to respond to cyber victims and they refer victims to the CSN website. Some states have developed cyber centers – such as Georgia, Oregon, Colorado and California but the support they provide is primarily focused on education and research. Many private sector companies have been formed to provide direct cybersecurity services from prevention to response, however small businesses who often don't have an IT security person on staff[12] struggle to find a company, wasting time and then giving up and deciding to pay the ransom. Moreover, when faced with the option to negotiate with a cyber hacker, (often Russian) they are at a lost as to what to do, so against these odds, they end up paying the ransom hoping the encryption key will work. There is a large gap in direct recovery services for small business owners[13]. Recognizing this deficit, the Cyberspace Solarium Commission has recommended to President Biden that he direct Congress to fund a Cybersecurity Response Center[14] for both consumers and businesses. We believe our work will complement the Cybersecurity Response Center; however it is unclear when and if Congress will fund this center and what the scope and direction will be. Because many business owners fail to report, reliable data is hard to find, and perpetrators continue to wreak havoc without fear of reprisal. In the 2018 report titled, "The Real Reasons Why Cybercrimes May be Vastly Undercounted[15]" the Slate Group reported many professionals view cybercrime statistics with suspicion. They report, "..the data about cybercrime and cybersecurity breaches is simply very sketchy". A recent article in Cyber Security Online stated, "law enforcement agencies

[12] SBA Office of Advocacy, Small Business Profiles, 2020, https://cdn.advocacy.sba.gov/wp-content/uploads/2020/06/04144214/2020-Small-Business-Economic-Profile-States-Territories.pdf

[13] This deficit is described in detail in the Cyberspace Solarium Commission….see footnote #14

[14] Cyberspace Solarium Commission, 2020

[15] Slate, February 2018, "The Real Reasons Why Cybercrimes May Be Vastly Undercounted, https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html

estimate the number of cybercrimes that go unreported by businesses number in the millions.[16]" Many business owners fail to report for fear THEY will face regulatory fines, their credit worthiness will be impacted and their reputation will be tarnished. Better to stay quiet than face these repercussions, all the while the perpetrator goes free. The NCSS hopes to encourage reporting and collect reliable data on ransomware attacks using the cybercrime taxonomy developed through federally funded efforts of the Department of Homeland Security[17].

The National Cybersecurity Society (NCSS) has spent five years, identifying, studying and classifying gaps in support. Understanding this need for direct service to cybercrime victims, the NCSS is working to enhance the services we currently provide victims and potential victims of cybercrime by creating the National Cybercrime Center – a one-stop-shop for reporting cyber incidents and obtaining help. NCSS serves all communities across the U.S. Of the 30.7 million[18] small businesses, 2.6 million[19] are businesses owned and operated by African Americans[20]. Of the 2.6 million African American firms, 109,137 are African American owned firms with employees[21]. Black owned firms with the largest earnings are health care and social assistance ($24.2 B); retail trade ($17.1B); and professional, scientific and technical ($15.6B)[22]. We believe this community is underserved and needs much needed attention and outreach.

[16] CSO Online, May 2019, "Why businesses don't report cybercrimes to law enforcement," https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

[17] Cybercrime Support Network is developing a cybercrime taxonomy funded by DHS. The NCSS will leverage this work in characterizing cybercrime to ensure better fidelity in crime statistics.

[18] Includes both employer and non-employer firms.

[19]U.S.Census, 2012, African American owned businesses in the U.S. https://www.census.gov/data/tables/2016/econ/susb/2016-susb-employment.html

[20] U.S Census 2012, Businesses by Gender, Race and Ethnicity

[21] IBID

[22] Black Demographics, The African American Population, "Black Owned Businesses"

B. HOW NCSS HELPS SMALL BUSINESS NAVIGATE The REALM OF CYBERSECURITY

The NCSS was created to educate small businesses on cybersecurity with a focus on small disadvantaged businesses in distressed communities. In keeping with this mission, NCSS is committed to providing timely victim services that are sustainable, safe and easy to use. The NCSS has identified a significant gap in responding, interpreting and delivering compassionate, trauma informed response to cyber victims. There is no other entity currently providing the direct support to cybercrime victims. The NCSS provides a number of free resources to educate the small business owner as well as help them navigate the marketplace through our Small Business Toolkit. In addition, we recommend businesses consider joining the NCSS to obtain weekly cyber educational tips, access to greater online content, access to our Ask-an-Expert service, and assistance in reporting their incident through our portal.

The NCSS is an Information Sharing and Analysis Organization (ISAO), which provides an added layer of protection to the companies that become members and work to improve their cybersecurity posture. As an ISAO, if a company reports a cyber incident to a government entity, ISAC or ISAO, under the Information Sharing Act of 2015, these companies are protected from litigation and other liability concerns. The NCSS has an approved Automated Information Sharing portal, that our member companies can use to report the incident autonomously, if so desired. Our portal is DHS approved -- that automates cyber incident reporting – machine-to-machine.

Another affirming effort we have seen recently, is there are several states that have implemented safe harbor laws, to protect business owners from legal liabilities if the company has adopted a cybersecurity framework. Ohio in 2018 became the first state in the country to enact a safe harbor protocol for organizations hit by a data breach, Utah followed suit, and it appears Connecticut may be next. This enabling effort is needed as we have seen many small businesses haven't implemented basic cyber hygiene, nor report incidents to law enforcement.

CHALLENGES: The biggest challenge we have faced, as other nonprofits in this space have faced, is the lack of funding. Private industry recognizes the need, as they are concerned about their supply chain, but funding is scarce. Another challenge is there is no organization to provide direct assistance to companies who have suffered a cyberattack. Often these companies lose many weeks to months trying to recover and then decide the recovery is too costly to implement, so they close their operations. Another challenge in this area, is the fear to report the incident, due to reputational harm as well as the possibility of tough fines. This hampers the entire ecosystem such that others could benefit from the event and learn what protection measure could have been in place to prevent the hack. When one business falls, and doesn't report, the criminal benefits – he gets away with the bounty – money and data. In our viewpoint, It is imperative that businesses report to a protected safe harbor, so that others can benefit and law enforcement may catch the criminal. The reporting needs to be at the national level so that all data can be aggregated. The Internet Cyber Crime Center (IC3) collects data on cybercrime, yet there is no incentive to report like the Information Sharing Act of 2015 provides.

However, against these challenges are two foundations that stand out – the Craig Newmark Foundation and the Gula Foundation – both have funded cybersecurity for the ecosystem, not specifically for small businesses. Other funders in this area are: DHS, DoJ and

NSF. If interested, the NCSS could provide a listing of known grants to grantees over the past several years in the area of cybersecurity to help demonstrate this patchwork of funding.

OPPORTUNITIES

Given the number of businesses that need to be reached, we believe the best approach is to utilize the Small Business Development Centers (SBDCs) and the Department of Homeland Security (DHS). Leveraging the SBDC's reach and DHS's technical guidance, a nonprofit like the NCSS, could be funded to lead the effort to provide educational resources and training to the 63 SBDCs. A project lead could ensure that the training is consistent among SBDCs; aligned with the appropriate cybersecurity framework; and is tailored so that a small business owner can understand and utilize. In addition, this program could be expanded to create a national Small Business Toolkit – companies who are vetted and approved by the SBA. In our experience, small businesses don't have the time or talent to research the marketplace to find a particular service. Helping curate these services would go a long way to opening up the marketplace for the small business owner and incentivize the cybersecurity vendors to produce services that are cost effective and easy to implement.

E. CONCLUSION

There is a number of companies who are distributing cyber hygiene advice and utilizing the opportunity to advertise their product or service. These tips are flooding the Internet, and the number of cybersecurity webinars during the pandemic has led to webinar fatigue, system overload, and not contributing to a safer small business ecosystem. Ransomware and business email compromise continues to be the FBI's top two cyber incidents. We believe information sharing should be incentivized – such that the business owner is able to report the incident anonymously – such as the Information Sharing Act of 2015 – to protect against regulatory fines. Our nation's innovation starts with small business --- we need to protect their most critical asset – their intellectual property.

Thank you for your time and consideration Stay safe!

Mary Ellen Seale, CEO/Founder
National Cybersecurity Society
me@thencss.org
703-340-7757