# FEDERAL GOVERNMENT AND SMALL BUSINESSES: PROMOTING GREATER INFORMATION SHARING FOR STRONGER CYBERSECURITY

## HEARING

BEFORE THE

## COMMITTEE ON SMALL BUSINESS
## UNITED STATES
## HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

HEARING HELD
NOVEMBER 15, 2017

Small Business Committee Document Number 115–048
Available via the GPO Website: www.fdsys.gov

U.S. GOVERNMENT PUBLISHING OFFICE
27–719 WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*
STEVE KING, Iowa
BLAINE LUETKEMEYER, Missouri
DAVE BRAT, Virginia
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
STEVE KNIGHT, California
TRENT KELLY, Mississippi
ROD BLUM, Iowa
JAMES COMER, Kentucky
JENNIFFER GONZÁLEZ-COLÓN, Puerto Rico
DON BACON, Nebraska
BRIAN FITZPATRICK, Pennsylvania
ROGER MARSHALL, Kansas
RALPH NORMAN, South Carolina
NYDIA VELÁZQUEZ, New York, *Ranking Member*
DWIGHT EVANS, Pennsylvania
STEPHANIE MURPHY, Florida
AL LAWSON, JR., Florida
YVETTE CLARK, New York
JUDY CHU, California
ALMA ADAMS, North Carolina
ADRIANO ESPAILLAT, New York
BRAD SCHNEIDER, Illinois
VACANT

KEVIN FITZPATRICK, *Majority Staff Director*
JAN OLIVER, *Majority Deputy Staff Director and Chief Counsel*
ADAM MINEHARDT, *Staff Director*

# CONTENTS

## OPENING STATEMENTS



## WITNESSES



## APPENDIX

# FEDERAL GOVERNMENT AND SMALL BUSINESSES: PROMOTING GREATER INFORMATION SHARING FOR STRONGER CYBERSECURITY

**WEDNESDAY, NOVEMBER 15, 2017**

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

The Committee met, pursuant to call, at 11:00 a.m., in Room 2360, Rayburn House Office Building. Hon. Steve Chabot [chairman of the Committee] presiding.

Present: Representatives Chabot, Brat, Radewagen, Kelly, Blum, Marshall, Velázquez, Evans, Murphy, Lawson, Adams, Espaillat, and Schneider.

Chairman CHABOT. The Committee will come to order.

I want to thank everyone for being here this morning.

This Committee has made cybersecurity a top priority in recent years and with good reason. It has become one of the most serious challenges for small businesses and major corporations and the Federal Government itself. We have heard from cybersecurity experts, government officials and small business owners on numerous occasions and the message is clear, cyber threats remain a top concern for America's small business community.

Advances in information technology, IT, have helped small businesses rapidly increase their productivity, enter new markets that were once out of reach, and offer consumers new and innovative services and products. However, IT has advanced so quickly that it has been difficult to keep pace with the ever-growing cyber threats. Cybercriminals and foreign bad actors have more opportunities than ever to steal intellectual property, consumer data, and hold small business IT systems hostage for financial gain.

In 2016 alone, the United States Department of Justice recorded nearly 300,000 cybersecurity complaints. Our Committee's examinations of these increasing concerns have revealed that federal agencies are making a serious effort to better coordinate and distribute cybersecurity resources directly to small businesses. However, there are still challenges to ensuring that small businesses are as protected as possible from cyber attacks. One of the major hurdles continues to be the lack of information sharing between public and private sectors. Information sharing is a fundamental component for a strong and effective cybersecurity defense, not just for small businesses, but for America's network as a whole. The federal government must make every effort possible to ensure that

small businesses have both the resources and the confidence they need to actively engage with the federal agencies tasked with protecting our critical infrastructure.

Today, we will hear from several members of the small business community about what steps we can take to encourage greater information sharing. We will examine how Federal agencies can provide assistance and resources more quickly to small businesses suffering from a cyber attack.

Earlier this year we learned that the federal government has become increasingly active in protecting our nation's critical infrastructure and IT systems, and has gone to great lengths to develop an overall framework for cybersecurity protocols to incentivize information-sharing practices with businesses. However, it has also become abundantly clear that the development of this framework is not enough. Last Congress, the President signed into law legislation aimed at increasing information-sharing practices through the Cybersecurity of Information Sharing Act, CISA. This legislation provided some important liability protections to small businesses to give them trust and confidence in their federal partners.

Yet many businesses continue to be slow to adopt these practices. That is why this Committee has been working on legislation to provide small businesses with greater assistance in their cybersecurity needs. In July, my colleague Representative Dwight Evans and I introduced H.R. 3170, the Small Business Development Center Cyber Training Act of 2017, perhaps the longest name for a bill in congressional history. This bill will direct SBDCs to establish a program for certifying some of their employees to provide cybersecurity planning assistance to small businesses. It is my hope that through this program we will be able to encourage even more small businesses to start partaking in information-sharing activities and create a comprehensive cybersecurity defense for all Americans.

I would now like to yield to the Ranking Member for the purpose of her making her opening statement.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

The frequent recurrence of cyber attacks reminds us just how fundamental it is for individuals, businesses, and governments to guard against unwanted foreign interception. From hackers orchestrating the Equifax breach to Russia's attack on our democratic institutions, cybersecurity merits our attention more than ever before. The truth is, online commerce has facilitated business opportunities and growth for mom-and-pop shops across America, but few small businesses make investments in security solutions to protect the data they hold. Many entrepreneurs do not even view themselves as targets. Criminals, on the other hand, view them as particularly attractive. The combination of customer data and the lax implementation of cybersecurity make them much more appealing to cybercriminals.

While it is widely known that cyber attacks often result in personal and business losses, small firms often do not recognize their exposure until it is too late. Given that small firms make up over 99 percent of businesses, the small business community plays a critical role in ensuring the nation's internet infrastructure is secure. And preventing the harsh financial consequences that cyber

intrusions have is critical for their survival because criminals will continuously seek to profit by stealing data from both their government and the private sector.

Cyber incidents are not diminishing in the near future. That is why we all must take the appropriate steps to strengthen cybersecurity.

For nearly two decades, the federal government has actively created a policy framework that seeks to prevent cyber attacks by incentivizing data sharing and collaboration between federal and private actors. Doing so is just one step to enhance readiness against external threats. Encouraging businesses to share information regarding cyber intrusions could help federal agencies design solutions before problems occur. If the private sector and the government collaborate to identify vulnerabilities, both small businesses and the government will be better prepared.

Mr. Chairman, over the last year we have seen cybercriminals prey on one of the largest credit rating agencies. We have witnessed hackers publicly releasing tools stolen from the National Security Agency, and most disturbing, as we all know, our democratic institutions were remarkably vulnerable to Russia's cyber meddling, potentially impacting the outcome of our elections. This event make clear cybersecurity issues will become more prominent every day in all aspects of our society.

In that regard, I look forward to learning how we can better maximize the flow of information between small businesses and the federal government to help improve the resiliency of our cyber infrastructure.

Thank you all for being here today and offering your insights.

I yield back, Mr. Chairman.

Chairman CHABOT. Thank you very much. The gentlelady yields back. And if Committee members have opening statements prepared we ask that they be submitted for the record.

And I would now like to take just a moment to explain our lighting system and rules. You get 5 minutes basically. The green light will be on for 4 minutes. The yellow light will come on to let you know you have a minute to wrap up, and then the red light will let you come on and let you know you are supposed to stop. We will give you a little bit of leeway there, but do not take advantage of it.

And I would now like to introduce our very distinguished panel here this morning. Our first witness is Rob Arnold. Mr. Arnold has worked in internet security of over 20 years and is the Founder and Chief Executive Officer of Threat Sketch, LLC. Threat Sketch provides risk management tools and education to small businesses to help them prevent cyber attacks. We appreciate you being here with us today.

Our second witness is Ms. Ola Sage. Ms. Sage is the CEO of e-Management in Silver Spring, Maryland, where she oversees e-Management's information technology and cybersecurity services. In addition to her role as CEO, Ms. Sage chairs the Executive Committee of the National IT Sector Coordinating Council and serves on the board of the George Mason University Women in Business Initiative. And we welcome you here as well this morning.

Our third witness will be Mr. Morgan Reed. Mr. Reed serves as the President of ACT/The App Association. The App Association represents more than 5,000 app companies and information technology firms in the mobile economy. Mr. Reed has previously appeared before the Small Business Committee last year, and we welcome him back here today.

And I would now like to yield to the Ranking Member for the introduction of our fourth witness.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

It is my pleasure to introduce Mr. Tom Gann, the chief public policy officer for McAfee, a computer security software company. Mr. Gann has over 20 years of experience in the technology industry, 12 of which have been focused on cybersecurity issues. Mr. Gann holds a bachelor's degree from Stanford University in political science and a master's degree from the London Business School. Welcome and thank you for being here today.

Chairman CHABOT. Thank you very much.

Mr. Arnold, you are recognized for 5 minutes.

## STATEMENTS OF ROB ARNOLD, FOUNDER & CHIEF EXECUTIVE OFFICER, THREAT SKETCH, LLC; OLA SAGE, CHIEF EXECUTIVE OFFICER, E-MANAGEMENT; MORGAN REED, PRESIDENT, ACT/THE APP ASSOCIATION; THOMAS GANN, CHIEF PUBLIC POLICY OFFICER, MCAFEE, LLC

### STATEMENT OF ROB ARNOLD

Mr. ARNOLD. I would like to thank the chair, ranking member, and the entire Committee for the opportunity to testify today. It is truly an honor.

My company, Threat Sketch, makes extensive use of shared information to educate small businesses and guide their investments in cybersecurity. We are a small business ourselves, thus I truly understand the needs and challenges around sharing cybersecurity information.

The most fundamental problem in accessing data right now is fragmentation. The DHS, FBI, NIST, and the NSA are just a few of the agencies collecting cyber information. Each has multiple repositories and programs. Some are well advertised, while some are part of work groups and not widely available. Others are hidden by classification. Simply having a list of all the data-sharing initiatives available would help us tremendously.

Another problem with sharing information is the overuse of classification. There is a myriad of rules governing the declassification of information, but declaring valuable information as secret is almost effortless. It takes no more than two words uttered with a grave tone to play keep away with vital information. "That is classified," and just like that, our cyber equivalence of neighborhood crime statistics and sex offender registries are taken away in the name of national security. While secrets definitely have their place, we have a right to know what is going on around us, and every data point that gets classified degrades our ability to make good decisions.

But there is a more pressing issue which I need to draw your attention to, and it is the byproduct of two distinct disadvantages that small businesses face.

First, as these larger companies armor up, attackers are turning to less protected small businesses.

Number two, small businesses cannot afford to compete with big companies for the cybersecurity talent and solutions they need to protect themselves. These are circular issues with one begetting the other. In their wake, the demand for affordable solutions will rise dramatically, creating yet another threat. Small businesses, desperate to meet the cybersecurity demands of larger clients, government regulations, insurance carriers, and lending institutions, are going to become victims once again. Adversaries will use this opportunity to sell cheap software and services that are subsidized by selling data and secrets out the backdoor, while giving them a toehold into the supply chain of larger organizations.

My written testimony offers one possible solution, which is to deputize small businesses that commit to providing services that are all-American in origin. In addition to tapping our SBDCs, I believe the government has two resources that can help in the collection and dissemination of cybersecurity information. Our Bureau of Labor Statistics is very good at aggregating, summarizing, and making data available in easy to digest forms. Meanwhile, the IRS is the one agency to which every small business owner is happy to report some losses.

In summary, small businesses need local solutions that can tap into a national network of trusted solution providers. The SBDCs have proven effective in helping small businesses navigate a myriad of State, Federal, and local resources, and with training, I think they can rise to this challenge as well.

Thank you for allowing me to testify before you today. I look forward to answering your questions after we hear from my fellow witnesses.

Chairman CHABOT. Thank you very much.

And Ms. Sage, am I pronouncing it correctly?

Ms. SAGE. You are, Chairman. Thank you.

Chairman CHABOT. Okay. Very good. You are recognized for 5 minutes. Thank you.

**STATEMENT OF OLGA SAGE**

Ms. SAGE. Good morning, Chairman Chabot, Ranking Member Velázquez, and the distinguished members of the Committee. Thank you for the opportunity to testify today as a small business CEO.

In the last 12 months, 61 percent of small businesses have reported that their companies have experienced a cyber attack, and a stunning 71 percent of small businesses are not prepared to address cybersecurity threats to their organizations. Solving this problem requires greater information-sharing between the Federal Government and the small business community to help our companies better identify threats, protect our infrastructure, detect anomalies, respond to and recover from significant cyber events.

The Cybersecurity Information Sharing Act, which I will refer to as CISA, can help, but small businesses do not know about it.

While significant progress has been made in implementing the law in general, several challenges still persist for small businesses.

First, small business are still unaware of CISA or how it helps them. The government has the opportunity to increase the visibility of the law through its existing outreach and awareness programs to the small business community and to highlight the law's protections, particularly in the area of liability protections. Small businesses are still confused by the myriad of information-sharing initiatives. A small business guide for cybersecurity information sharing would be a useful tool to help companies better understand the value these various public and private information-sharing options provide.

Third, cybersecurity information can be costly. While data provided by the government may be free, many small businesses do not have adequate resources to make the best use of this data. For some, signing up with a commercial information-sharing organization may be the best option. However, many of the options available today cost thousands of dollars per year putting them out of reach for many.

Let me now turn to some ideas for incentives that Congress might consider to encourage greater information sharing and cyber threat reporting between small businesses and the Federal Government.

First, expand CISA to add additional protections for small businesses. CISA does not currently shield companies from potential liability in the event of a data breach or cyber attack. Congress might consider providing a positive incentive by extending liability protection up to a maximum threshold to small businesses that exhibit a measurable commitment to voluntary information sharing. This could be through demonstrated use of the NIST cybersecurity framework, voluntary participation in one or more public or private information-sharing forums, and maintaining active cybersecurity insurance.

Second, introduce tax incentives. Congress might consider introducing incentives that could include deductions and credits for cybersecurity and information-sharing related capital investments and personnel among others.

Third, include participation in a public or private information-sharing program as a selection criteria for government procurements. The government has and continues to use preferential consideration in the procurement process to promote or influence desired behavior. These include considerations for minority groups, quality and process improvement standards, and research priorities. The GSA Alliant Small Business Governmentwide Acquisition Contract provides one example for quality standards.

Four, recognize small businesses that commit to cybersecurity information sharing. Voluntary programs, such as Energy Star, which is a joint program of the Environmental Protection Agency and the Department of Energy, can serve as a blueprint to design a public recognition program for small businesses participating in voluntary information-sharing programs.

Lastly, simplify the entry point for cyber threat reporting for small businesses. Most small businesses either do not know who to call or are overwhelmed by the choices and, therefore, will not

bother reporting. Last year, the Critical Infrastructure Partnership Advisory Council, CIPAC, formed a working group with the DHS Office of Infrastructure Protection to investigate how to get a national tip line started that would serve as a single point of contact for reporting emergency cybersecurity information. Using this example, one could envision a scenario where a small business calls a national emergency response number, and based on information provided, is immediately connected to the appropriate resource or resources.

In conclusion, CISA is still early in its life cycle, but I believe holds tremendous promise for the small business community as more companies become aware of the law and how it can help them. Thank you again for the opportunity to testify and I look forward to your questions.

Chairman CHABOT. Thank you very much.

Mr. Reed, you are recognized for 5 minutes.

**STATEMENT OF MORGAN REED**

Mr. REED. Chairman Chabot, Ranking Member Velázquez, and distinguished members of the Committee, my name is Morgan Reed, and I am the president of ACT/The App Association. I thank you for holding this important hearing.

I represent more than 5,000 companies who make the apps you love in the devices you depend on. We are the driving force behind a nearly $150 billion industry and we continue to grow and create American jobs in every congressional district. And our members are building the tools that underpin this jump from the desktop world to our new world of mobile plus cloud. But for small businesses trying to create new products and sales opportunities, cybersecurity threats seem incomprehensibly vast and inevitable. In 2014, 71 percent of companies admitted they fell victim to a cyber attack. Moreover, the amount of data online is expected to increase fiftyfold by 2020, adding new attack vectors and, frankly, sweetening the pot for potential cybercriminals. And we have not even mentioned the new world of IOT and self-driving everything that is right around the corner.

At The App Association, we sit at the crossroads of this topic. We have dozens of members who are key players in cybersecurity, like PhishLabs, Alchemy Studios, and Citara, and on the frontlines of anti-phishing, anti-botnet, and DDOS attacks. But we also have members who build all the amazing apps you use every day, that you rely on to do your banking, to monitor your child's homework, buy a house, and communicate with your doctor. With a foot firmly in both sides of the industry, we know policymakers must remain mindful of the fact that large companies have budgets and staff available. For our members, chief security officer may be just one of five hats that they wear.

Small- and medium-size tech companies, like our members, exist to solve problems. Take Canned Spinach, for example. It is a company in your district, Mr. Chabot. Canned Spinach, led by Andrew Savitz, built a product called Speak Easy. It allows for people inside of a company to distribute coupons and secret deals that their family members might want. The problem he ran into is based on phishing attacks and other cybersecurity attacks. Users were un-

sure where they were getting this from, who provided it, and so he had to essentially design the product from the ground up to deal with the cybersecurity threats so that people could get good deals from their friends inside of companies. And our clicks-and-mortar businesses have this problem as well. For Chairman Velázquez, she knows Etsy quite well, headquartered in her district. They have requirements for strong data security methods to handle the consumer data on their platform.

And I should point out that Mr. Brat and Mr. Schneider, you both have health companies in your district that deal with thousands of patient records. For you, Mr. Kelly, there is a company in your district that does home restorations. They go into a house, take pictures of the damage. But think about what they now know about that person. They know their address. They have photos of their valuables, and it is all stored on their cloud service. It is a great product, but what do they do about cybersecurity?

And so when you think of it from their perspective, of problem-solving, and then thinking about it on how do they enter the space, you can see how government information sharing is really not meeting the challenge that we have today.

The first thing that we do in private sector is we rely on our private sector platform partners. We use products like Microsoft cloud services and Azure for cloud, Apple Health Kit for health, the latest Intel Sawtooth chip for making block chain more practical and efficient. But that symbiotic relationship only takes us so far. We need Congress to do some major changes to how we do info sharing.

First, we need to improve the sharing activities. The Federal Government should make the cybersecurity threat information it shares timely, more accessible, and, frankly, more useful to SMEs. When a business is hit with a cyber attack, with whom do they share it? Do they call the attack while the attack is occurring as opposed to after the fact? Do they call somebody at Endkick? Do they even know what Endkick is? Somebody at their local fusion center or their ISAC? And where are these entities located and how do companies share the information with them?

Second, the Federal Government should take steps to make cybersecurity frameworks and best practices more workable for SMEs. Helping SMEs to improve their understanding, whether it is through Lunch and Learns at SBDCs or other activities, we need to see developed, widely published, targeted, and user-friendly best practices and guidance built on the NIST framework.

And third, the Federal Government needs to ensure a legal and policy environment that enhances SME's ability to manage the dynamic cybersecurity risks, and this part falls squarely on Congress. Congress must take steps to provide legal and policy certainty that SMEs can rely on. Specifically, Congress should pass the International Communications Privacy Act, known as ICPA—for this year's Congress it is H.R. 3718—to clarify SME's legal liability and data requests especially with data abroad, and they need to maintain this legal environment to help support our investment in cybersecurity.

And I would like to take a moment to thank Chairman Chabot and Ranking Member Velázquez for cosponsorship of this legisla-

tion in the last Congress, and I ask all of you to join with them in support for it in the 115th.

Thank you very much, and I look forward to an engaging conversation on this topic.

Chairman CHABOT. Thank you very much. That was very interesting.

Mr. Gann, you are recognized for 5 minutes.

**STATEMENT OF THOMAS GANN**

Mr. GANN. Good morning. Thanks for the opportunity to testify today. I am Tom Gann, the chief public policy officer from McAfee. McAfee is one of the largest cybersecurity companies in the world. Indeed, we take great pride in protecting consumers and businesses and organizations of all sizes.

As the Committee has ably pointed out in the past, small businesses face many of the same cybersecurity risks as large ones. Some cyber attack methods, such as malware and those that begin with spear phishing are particularly well suited for small businesses who might be an easy target because of their lack of cybersecurity resources. Small businesses store information, implement operational requirements, and own valuable intellectual property just as large enterprises do, so they need to have strong cybersecurity protections.

Investing in more than just very basic cybersecurity tools requires time, money, and other resources, like an IT staff, that too often small businesses just do not have. We have to acknowledge the fact that for most small businesses, cybersecurity is an expense that they do not want to incur when they are simply trying to make payroll and be profitable.

So what is the solution? Should small businesses participate in DHS's cyber threat information-sharing program that was mandated by CISA? This is a question worth exploring. In talking with our customers, it is clear that many small businesses are unaware of CISA. They often do not understand how the law can help them and they are confused by the many information-sharing initiatives that are out there. However, I do believe that we should consider how information-sharing efforts, such as those mandated by CISA, can benefit businesses of all sizes.

The DHS initiative, known as the Automated Indicator Sharing Program is open to small businesses, but many small businesses do not have the resources or an educated IT staff to make use of it or benefit from it. Any information-sharing capabilities require time, money, and people that small businesses sometimes are stretched to staff.

This does not mean that small businesses do not need or cannot benefit from cyber threat intelligence. They certainly can, but perhaps we would focus our discussion more on information sharing of a different kind, information that is informative and educational right off the bat.

According to the Better Business Bureau, when asked to judge 10 cyber statements as to being true or false, the average small business owner's score was around 60 percent. This means that for many small business owners there is really a lack of understanding of the cyber challenge at all. The Federal Government should help

develop and fund the standup of a nonprofit, information-sharing, and analysis organization for small businesses. Such an entity could provide education such as basic cyber hygiene and more advanced topics, like incorporating the NIST cybersecurity framework into members' programs. It could share best practices, lessons learned, templates, and processes for addressing threats and assist in understanding problems. Additionally, this organization could serve as a hub in the event of a breach and the first point of contact in determining whether or not to reach out to law enforcement. It could assist the business in addressing the incident and communicate the situation to other members.

Further, we recommend outsourcing IT to a cloud provider that would be responsible for security. That is a real advantage for small businesses. The cloud provider would benefit from an ever-growing network effect of more and more threat data, improving the very cybersecurity capabilities and protections they deliver to their customers' small businesses.

Both infrastructure as a service and security as a service can be economical ways to provide efficiencies and security so that small businesses really can benefit from an ecosystem of information sharing that is bidirectional with the government and the private sector.

Small business owners, however, cannot contract all of their security obligations out, particularly in the area of strong blocking and tackling, making sure that passwords are updated and information is backed up on a regular basis. Small businesses would also benefit from more cyber insurance. The government could act as a reinsurer for the cybersecurity market that really in many cases is in early stages. Indeed, the idea of providing tax benefits and credits to small businesses so they can purchase cyber insurance is a very good idea and would help pump prime what is today still an emerging market.

Finally, the government should devote additional resources to fighting cybercrime. Too often it is our small businesses that are impacted by ransomware attacks, and small businesses need all the help they can get. Investing in additional Federal, State, and local crime-fighting capabilities to help take down the bad guys to protect our small businesses, well, those are good investments that should be made.

In conclusion, I would like to thank you for inviting us to testify. It is very kind. We take very seriously our small business customers, and I welcome the opportunity to answer any questions you may have.

Chairman CHABOT. Thank you very much. I would like to thank all the witnesses for their really excellent testimony here.

And Mr. Arnold, I will begin with you. I recognize myself for 5 minutes.

You noted that the large number of data-sharing initiatives offered by the federal government in nongovernmental partnerships can be pretty overwhelming for a small business. Do you believe it would be beneficial if there was a single portal for small businesses to engage federal agencies to begin the information-sharing process? And if so, could you identify any particular agency or entity

that would be best suited for that task, specifically for handling requests from small businesses?

Mr. ARNOLD. Sure. So I do think at a base level we need just a simple directory. What information is out there and for each of these? What kind of information is being consumed by that sharing initiative? What kind are they making available and what are the membership requirements? And I think that the SBDCs actually are well positioned for that because they already do this with so many other government programs and initiatives. They seem like a logical fit.

Chairman CHABOT. Okay. Thank you very much.

Ms. Sage, I will turn to you next. In your testimony, you mentioned that one reason small businesses are reluctant to share cybersecurity information is the perception that shared information gets lost or goes into a black hole causing companies to worry about the security or uses of their data. Can you please elaborate on that concern, and do you have any suggestions for how information-sharing portals could be more transparent in their receipt and use of shared data?

Ms. SAGE. Thank you, Chairman, for that question.

I think that is the reality for a lot of small businesses. It is sometimes referred to as the Black Hole. You know, information is sent in and not exactly sure what happens to it. And it certainly has not helped with some of the recent compromises that have occurred where information has been breached and released. So I think that on the other hand, there have been efforts to really try and address that concern.

I was presenting that comment in the context of cyber information sharing so that if there are general concerns about information sharing, regardless of whether it is cyber or not, my goal was to really highlight the fact that cyber just adds another element of concern because that is even more potentially damaging to an organization. And I think that some of these protections that I mention in my recommendations can help with that. If companies feel like there are protections for them if their information is breached, and they are the victim of this situation, they are not necessarily responsible for also addressing it.

Chairman CHABOT. Thank you very much.

Mr. Reed, can you provide any example of how small business data or shared information practices might invite unwanted regulations for small businesses, particularly in the tech industry? What steps can we, policymakers, take to ensure that small businesses' personal information and IT data is protected from regulatory action?

Mr. REED. Well, I think one of the key elements to start with for this Committee and for Congress in general is our catchphrase at ACT, which is nobody wants technology at the speed of government. And so when you think about where we stand on the regulatory framework, I think you start off on the right foot and ask the question of if we increase the methodologies and reporting requirements and the pathways forward for companies and how they have to engage, then we know what will happen. Either we will not innovate new products at all or the products you see on the shelf will be incredibly limited, or worse, really expensive.

And really quickly, to go to an example that Ms. Sage hit, we took a staff down to South Carolina and we met with a company, PhishLabs. And PhishLabs is one of the leading anti-spear phishing companies out there. And I worry about this talk about regulatory bodies and new agencies. The CEO of PhishLabs, in this room full of staff, including DHS, said, by the way, guys, I want to show you something. Clicked over to US-CERT. So the Anti-Phishing Working Group has this email where you send data if you have a phishing attack. I am a leading phishing expert. I have no idea how to get that data. I have spent months in contact with DHS. They will not provide it. I do not know what is going on, and yet here is this government agency collecting data on phishing. And to Mr. Arnold's point, how is that not something that gets in?

So to your question, Mr. Chabot, I think we see that there is often a gap between the regulatory intention of Congress and how it gets played out. And, therefore, I would look to caution additional regulations that could harm small business.

Chairman CHABOT. Thank you very much. And unfortunately, Mr. Gann, I ran out of time before I got to you. I had a pretty good question, but my time is expired.

And I will now recognize the gentleman from Illinois, the Ranking Member of Subcommittee on Agriculture, Energy, and Trade, Mr. Schneider.

Mr. SCHNEIDER. Thank you, Chairman Chabot. And again, thank you to the witnesses for joining us today and sharing your insights.

Cybersecurity for a small business, it is not a one-time transaction. It is not a decision you make at a point. It is not an action you take just once like rent or buy. It is not an investment you make one time. It is a business constant, no different than sales, marketing, or finance. And to be effective, I think it has to start with, as you guys have touched on, it starts with design. It includes implementation. It requires ongoing vigilance. And then if something happens you have event management and ultimately recovery and a response and recovery. For a small business, just the thought of that can be overwhelming. A small business, oftentimes the founder is going to be the chief marketing officer, the chief finance officer, and the chief bottle washer. That is the problem. Those small businesses are going to look to outside resources.

So my question for the panel is, as many small businesses look at the need for cybersecurity understand it, but that the investment and ongoing maintenance of that is somewhat overwhelming, what resources are available for them? What role, Mr. Gann, does insurance play? I know it has changed since the last time we were here. And how do we make sure that we go from not just information sharing, which is important, to helping these businesses have solutions?

Mr. GANN. Well, a couple big recommendations I think can make a difference. The first one is for most small businesses, their priority first and foremost is to make payroll, grow the business, and hopefully become an even larger, more successful business over time. Toward that end, we recommend outsourcing to IT data centers, cloud providers. By doing that it can be cheaper, better, faster. Those large institutions can help with security.

That said, small business owners are still responsible for their endpoints. And so getting basic education in place, putting in place basic blocking and tackling of passwords, really important. Those things can add a lot of value rapidly.

The last point I would make—I did not include it in my testimony, but it is vitally important for all IT organizations that are developing new products to bake security and privacy into their products in the first instance. By doing that first off it can reduce the burden on all businesses and really bring forward the benefits of a much easier look and feel to technology that is secure such that small businesses and all businesses can focus on what they really need to do, and that is growing their businesses and satisfying the needs of their customers.

Mr. SCHNEIDER. Mr. Reed?

Mr. REED. I think one of the key elements that we learned is that we have to divide it between small businesses that are involved in solving cybersecurity problems and small businesses, who, as Mr. Gann pointed out, are busy moving a different product. And I think that platforms play a critical role, but I also think given this Committee's jurisdiction, there is more that can be done out of SBA and SBDCs to provide a Lunch and Learn opportunity.

The number one thing in having started some businesses myself that you run into is that feeling of alone. I do not know what to do. I am not sure who to turn to. And frankly, as you point out, when these things happen you are underwater, so you need to have a friendship circle, so to speak, a circle of trust that you can go to. And I think SBDCs can provide some of that because I think at a certain point the main thing a small business needs from an incident report, and as you say, baking it in early, is to know who to call, how to react, and how to clean up. And so I think there is more that can be done.

Mr. SCHNEIDER. Ms. Sage?

Ms. SAGE. Thank you, Mr. Schneider. I actually agree with Mr. Reed on the point of the different categories of small businesses because a lot of it depends on what kind of business you are.

I would just say, I think incentives are great motivators for small businesses. Fundamentally, what we care about is can we get a new customer? Can we keep our existing customers? And can we stay in business? And so whether it is cybersecurity or, potential lawsuits or sales and marketing, anything that is not going to help us advance one of those three objectives is something that we are less likely to do.

And so to the extent that Congress can provide incentives for us to want to do better in the area of cybersecurity, I think that would help.

Mr. SCHNEIDER. Mr. Arnold?

Mr. ARNOLD. I think one of the best things that the government can do is simply be as transparent as possible with information, allow it to come down to us, and give the small business community an opportunity to wrought solutions for themselves from that raw data. This a role that both myself and Olga Sage play in this, is taking that data and making it accessible.

Mr. SCHNEIDER. Great. Thank you. My time is expired. I yield back.

Chairman CHABOT. Thank you very much. The gentleman's time has expired.

The gentlelady from American Samoa, Mrs. Radewagen, who is Chairwoman of the Subcommittee on Health and Technology, is recognized for 5 minutes.

Mrs. RADEWAGEN. Talofa. Good morning. I want to thank you, Mr. Chairman, for holding this important hearing today, and I want to thank you all for testifying. All of you can answer my two brief questions.

Do you believe the government's responsibilities and small business owners' responsibilities in protecting businesses are balanced?

And as a follow up, what educational outreach efforts should the Federal Government be making to inform small business owners about cybersecurity information-sharing practices?

Mr. Arnold?

Mr. ARNOLD. Yes. So, I think the question of balance, it is very hard to balance the desire to keep information secret in the name of national security, yet also make it available to the people that need it. And I would encourage the government to err on the side of making it available. Unfortunately, security by obscurity does not work and I think the best policy the government can take is one of transparency.

And then with regard to education, I think we need to broaden the topic of cybersecurity to include legal, insurance, and even marketing, because there is a need to reestablish a tarnished image after an attack.

And I will yield to the other witnesses.

Mrs. RADEWAGEN. Ms. Sage?

Ms. SAGE. Thank you, Mrs. Radewagen.

On the question of balance, I think that is something that we are constantly trying to, for lack of a better word, balance. I think to Mr. Arnold's point in the whole area of classification, one of the things we see is that information may be classified when it comes to sources and methods, but the actual issues or concerns are not necessarily classified. The challenges that perhaps with all of the information overload that we all have, sometimes it is not apparent which of these unclassified areas or topics or issues really need to be paid the most attention to. So I think that is an opportunity for our government partners as they are putting out this information, even in an unclassified format, to be able to provide some level, I do not know if it is a ranking or scoring or some level of identification to help companies understand while everything is bad, you know, but here are the things that we want you to pay particular attention to.

When it comes to education awareness, I actually think that several agencies are really doing their best to really get the word out there. It is a big issue. It is a big topic. So whether it is SBA or DHS with their CQ program, NIST, Federal Trade Commission has some really good products, I think this is going to be a whole-of-government effort. I do not necessarily think that just one agency will be able to address all of the educational awareness needs.

Mrs. RADEWAGEN. Mr. Reed?

Mr. REED. I want to agree with Mr. Arnold and Ms. Sage about the issues about classification. And let me put a fine point on it.

You ask about balance. If an agent decides to classify something, what happens to him if he is wrong? Nothing. If a small business does not have that information, they go out of business, and worse, their consumers and their customers, and frankly, your constituents, are harmed. And so when you ask the question about balance, I think that we do not have a good balance on it because ultimately, the small business goes away and people are harmed and the government's impact of making the more cautionary decision is nothing. So I think we have to remember what the impact of not sharing equals.

On the education side, I would say that it is important to not undervalue the platforms. Most of us are looking to build some cool, interesting product on top of other technologies. And whether it is a cloud provider or another security company or anyone else in the space, look at ways that you can do public-private partnership with platforms to push that education to their customers. And if it is meaningful for them in an economic sense, it will be meaningful for us as small businesses.

Mrs. RADEWAGEN. Mr. Gann?

Mr. GANN. So on the question of balance in the area of information sharing, the big thing that one needs to remember is that small businesses are part of a much larger information-sharing ecosystem, whether they are interacting with a cloud provider, whether they are interacting with an endpoint security provider, making sure the government is doing a very good job of managing equities in terms of what data to release, what data not to release in the cyber domain is absolutely critical to the health of that entire ecosystem. We always encourage the government to be prudent in what it classifies. If you are at the NSA or one of those organizations, you may be seeing 3 or 5 percent of the threats that are truly——

Mrs. RADEWAGEN. I am out of time, Mr. Gann.

Mr. GANN. Oh, sorry. That are truly driven from sources and methods. Those need to be held back. The other types of data that are more mundane should be shared.

Chairman CHABOT. Thank you very much.

Mrs. RADEWAGEN. Thank you, Mr. Chairman.

Chairman CHABOT. Thank you. The gentlelady's time has expired.

The gentleman from Florida, Mr. Lawson, the Ranking Member of the Subcommittee on Health and Technology, is recognized for 5 minutes.

Mr. LAWSON. Thank you, Mr. Chairman. And welcome to the Committee.

This discussion underscores the dilemma that small firms have in protecting their companies' and their clients' data, while also sharing information not only with each other, but with the Federal Government. And I want you to know I am from the government and I am here to help you.

Can the panel please explain what a good balance looks like for companies to have adequate protection while also working cooperatively with various agencies and authorities to share data?

Mr. ARNOLD. Thank you for the question.

So how do you achieve this balance? I think that, again, erring on the side of transparency first, one of the things I suggested in my written testimony is that maybe we let the frontline responders classify everything initially, but then have some central clearinghouse like DHS that can go through with the specific objective of declassifying everything to the point where it gets good information out without undermining the needs of the Nation state security.

Mr. LAWSON. Anyone else care to respond?

Ms. SAGE. Thank you, Mr. Lawson.

Actually, in my testimony I really kind of focused on the area of liability protection and explicitly asked for your consideration of expanding that liability protection to small businesses in the event of a data breach or attack, because I think part of the concern, and it kind of speaks to part of my earlier written testimony, where I talked about some of the concerns small businesses have with providing information, particularly negative information to the government, that in some way it can either be lost or misused, et cetera.

And so I think that that combination of the worry of providing information that may someday come back to haunt you, and God forbid you actually have an event, I think that would help small businesses to feel more comfortable sharing.

Now, in my written testimony I do not say, well, just give us liability protection. I do say that there has to be some measurable commitment by these small businesses to cyber hygiene and cyber readiness. And so I think it is a formula of both requiring or asking or incentivizing small businesses to share information, but also providing protections in the event that there is a breach.

Mr. REED. I think most of everything has been covered, but in thinking about it, I think part of it is also how do people assemble what they view as valuable information? In your district there is a company that is called Tech for Vets that works with a lot of veterans' information. As you can imagine, they do great work for the veterans community, but that also means they have access to an enormous amount of very sensitive data. And so when considering what that balance looks like and how do we engage, we agree with Ms. Sage that I think liability protection is absolutely essential, but it also, it reflects the fact that when you have that data and it is breached, your reaction is going to be, oh, my goodness, how do I staunch the bleeding? How do I stop the pain? And oftentimes your first reaction is not to tell everybody how you are in pain.

And so finding a way that removes that liability or creates other frameworks where you can say I tried my best, I did not make it, help me next time. And so whether it is through incentives or liability protection, I think you have to understand the emotional state of somebody when they are going through an incident because I think it helps inform how you do a better job the next time.

Mr. GANN. So the single best thing that policymakers can do in the area of cybersecurity is continue to keep the issue very bipartisan. If you go back 10 to 15 years and move forward from where we have started to where we are today, an awful lot of progress has, in fact, been made. CISA was passed. We have stood up authorities in the civil government domain, putting DHS in the first chair on cyber. We have increased information sharing. We have broadly educated the population, large business, small business to

some degree on the cyber threats. Keep that work up and continue to update laws. Continue to update CISA. Allow more robust sharing of information beyond simple indicators of compromise. Look at creative ways to put in place the right incentives to increase security. Keep the work up and I think we will make a lot more additional progress.

Mr. LAWSON. My time is about to run out, but one other thing after hearing the testimony from Mr. Reed, I was trying to equate how small—and you do not have to answer because my time has run out—how small of businesses are concerned with cybersecurity? And that is the ones that are 45 and stuff before we get into the level that you are talking about. Maybe at some point in time, Mr. Chairman, he might be able to answer.

Mr. REED. Can I give a really short answer? Companies of one person can have records of hundreds of thousands of people.

Mr. LAWSON. Wow. I yield back, Mr. Chairman.

Chairman CHABOT. Thank you very much. The gentleman yields back.

The gentleman from Kansas, Dr. Marshall, is recognized for 5 minutes.

Mr. MARSHALL. Good morning, everybody.

Mr. Reed spoke of fusion centers. Are the other witnesses familiar with fusion centers as well? Okay. When I visited our fusion center in Kansas, terrific facility, it is more of a regional facility I would describe it, the private sector interaction were several big utilities as I can recall, maybe a big bank. How are small businesses accessed? Ms. Sage, are you familiar with the small business access to the fusion centers?

Ms. SAGE. It is a challenge because, first of all, a lot of these fusion centers are used for briefings at the classified level, et cetera. And so if you do not have those credentials to get in, you are not even in——

Mr. MARSHALL. Right. Getting the top secret clearance.

Ms. SAGE. Exactly.

Mr. MARSHALL. And you cannot participate with them unless you have—you cannot say here is our problem without them divulging stuff to you in any way.

Mr. Reed, you mentioned——

Mr. REED. Right. I think that gets to the education. And having recently been in your wonderful district and talked to some of your small businesses there, I think there is a huge education gap on how those fusion centers can play a role. And so I think that the questions we have to ask is, is there something that can be done to give them the credentialing and the entry point? Because as you point out right now it is primarily critical infrastructure that understands how they fit into this equation, but as we have talked about here, literally hundreds of thousands of small companies have the information that could compromise critical infrastructure if we are not careful. So yes, we need to do a better job with getting access to those fusion centers.

Mr. MARSHALL. My next question centers around it seems like we are always on defense when it comes to this rather than going on offense. It is almost like someone is trying to rob the bank 10 times a day, 20 times a day, and it seems like we have accepted

that is okay and we do not go after those people hard enough and we are not going on the offense with them. We are not releasing these hunt viruses back at them and trying to be more aggressive. Maybe I am wrong. But who is out there doing a great job saying we are not going to take this anymore? We are not going to sit there and just get attacked. I will sit there and watch 20 or 30 attacks on some of my companies back home in the matter of an hour when I am there.

Anybody have a comment about who is doing a good job on offense? Mr. Arnold does.

Mr. ARNOLD. Well, actually, I was going to say that I do not think the small businesses are actually equipped to do offense at that level because they are going to invite a counterattack by going on the offensive.

Mr. MARSHALL. So we need to empower them. Who is trying to say here is the software to go on the offensive?

Mr. Gann?

Mr. GANN. So let me take that one on. It depends on how you define offensive activity. We actually have to be careful with overbroad rules that allow unqualified people to hack back because you never quite know who the attacker is and you can get subsidiary effects.

That said, there is a lot of innovative work being done in the cybersecurity sector on machine learning, on analytics, on doing a much better job of understanding threats as they are starting to occur and starting to react early on to zero day attacks that have not been seen before. The science is really moving much beyond the traditional blacklisting anti-virus model.

So that innovation is occurring in large companies and you are seeing a lot of small players doing a lot of innovating, and you have seen a massive increase in the amount of venture capital money flowing through the cybersecurity sector. Billions of dollars, in fact. And so I think the trend lines overall are pretty good, but we still have some rough spots.

Mr. MARSHALL. I need to move on to my next question.

My opinion is most companies are afraid to report. They are afraid if they report it shows a weakness. Their customers might find out how vulnerable they are. How do we overcome that?

Mr. ARNOLD. We need to help them plan ahead for the eventuality of that happening. Small businesses do not even do the normal tabletop exercises that larger organizations do that generally put larger organizations in a better spot to respond to an adverse event, even just from a marketing and PR standpoint. So helping educate small businesses on how to do that would be very helpful.

Mr. MARSHALL. Any other?

Mr. REED. And I think it ties back to your previous question, which is where do you find the consultants and others in the space that can help you build ahead? I think you work through platforms that exist, larger platforms, but also you look at some of the consultancies that exist out there and find ways to do, as you said, table-topping, but remembering always the primary goal of the business. So I think it is about informing the IT professionals that set up that web presence or that customer store or your database and saying to them, how are we prepared? And I think that goes

to Ms. Sage's point, which is we have got to change the incentive structure.

Ms. SAGE. I agree with both gentlemen. And I would just like to add, Dr. Marshall, that the cybersecurity framework that was developed by NIST in industry I think really provides a good model to help both large and small because it addresses that specific area of how do we respond to and recover from some of these cyber events?

Mr. MARSHALL. Thank you. I yield back.

Chairman CHABOT. Thank you. The gentleman yields back. Those are some excellent questions, really, and the answers were good, too. Thank you.

The gentlelady from North Carolina, Ms. Adams, who is the Ranking Member of the Subcommittee on Investigations, Oversight, and Regulations, is recognized for 5 minutes.

Ms. ADAMS. Thank you, Mr. Chairman. Thank you all very much for your testimony. I have learned a lot just listening.

Let me ask Mr. Gann this question. Why should it be a priority for the Federal Government to pay attention to the vulnerabilities that small businesses face against cybercrimes?

Mr. GANN. Well, it is a great question. Indeed, we have gotten so many great questions. It has been really a very fine hearing.

Small businesses, it is worth remembering, oftentimes can be part of the most innovative pieces of the economy. Small businesses, whether in tech, biotech, machining, any number of areas, are oftentimes there because their founders left big companies because they wanted to do something new that maybe a large organization did not allow them to innovate on. So protecting those assets, those pieces of intellectual property that are really the seed corn of the future of our economy, that is absolutely essential. That is, I think, number one. Beyond that the issue of PII that so many small businesses own today, that is number two. But small business is absolutely a piece of the challenge that needs to be addressed.

Ms. ADAMS. Thank you.

Mr. Arnold, how can small business development centers help with the collection and the dissemination of cybersecurity information?

Mr. ARNOLD. Well, let's talk about first the collection thereof. When events happen, some of them have grave economic impact. Some of them maybe do not have horrible economic impact, but they have some technical issues and indicators that all need to get reported. And so the SBDC has kind of become a triaging place so the small business can say, hey, I have had this kind of attack. Who do I need to report this to? And they can give a list of the agencies that are best suited to gather that data.

And then likewise, on the back side of disseminating the information back out, as Ms. Sage has pointed out a couple of different times, each small business is very unique in its needs and there are a lot of different programs out there and there is a need for that diversity, but we also need to have a phonebook, if you will, a directory of, okay, well, these are the information programs that are out there. These are the educational pieces that are out there, and the SBDCs could connect the small businesses to those.

Ms. ADAMS. Thank you. And anybody who wants to answer this question.

Based on your experience as a small business working with other small businesses, why is it that most small firms do not understand the full scope of their risk to cyber threats? And do you believe we need more outreach, more education? Anybody can respond to that. I would appreciate it.

Mr. REED. So having been a founder of a couple of small businesses, what makes you motivated to build a small business is to solve a problem, whether it is to sell food on the street corner or to build the next great social media application. Your focus is on delivering a product and solving a problem as you see it. And that is what burns inside of you. That is what takes the risk. That is what gets you to borrow money from your mom's house to put it out there. And so the problem starts with if cybersecurity is not something that you are in the business of, and it is not the problem you are trying to solve, you are pouring every amount of your heart and soul into solving that specific problem.

So I think that what we have to do is early on the education effort has to be if you want to see your dream realized, then you need to make sure that you are taking care of business at the very beginning before you see your dream dashed because you lost that information. So I think it is about structuring the question that you asked. And I think it is a vital question. And you need to turn it back on that small business and ask them, I am here to help you get your dream, but what are you doing to make sure it can live for the long term, not just for the short?

Ms. ADAMS. Okay. Does anybody want to respond quickly to that?

Mr. ARNOLD. I would like to add, too, that small businesses, well, will frame cybersecurity as an IT program. It needs to be reframed as a business problem, one that the business owners have to address, and I think that is critical.

Ms. ADAMS. Ms. Sage?

Ms. SAGE. I just want to say amen.

Ms. ADAMS. Okay.

Ms. SAGE. I also think that to the points that have been made earlier, if cybersecurity is not going to help us ultimately accomplish our business goal, it will go the way of every other issue or concern that small businesses have to deal with, which is we do not deal with them until we have to. So to the extent that we can help, as you rightly pointed out, educate business owners, and to Mr. Arnold's point, that this is not just a technology problem, educate business owners that it is the same like if you do not have an EIN number for doing business, you cannot do business. It does not matter what kind of service you want to provide. There are certain things you just have to have in place. And I think if we can get our small business community to understand that this is one of those kinds of things, I think we will be in a much better place.

Ms. ADAMS. Thank you very much. I am out of time.

Chairman CHABOT. Thank you very much. The gentlelady's time is expired.

We want to thank the panel here for your very insightful information that you have given us here today. I think you have an-

swered the questions very well and cybersecurity is clearly one of the principal, one of the greatest issues a lot of small businesses face today. They know it is important, but they are not quite sure exactly what to do about it. And this Committee wants to work to help them to the extent that we can. So thank you for helping us to help them. We appreciate it greatly.

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

Without objection, so ordered.

And if there is no further business to come before the Committee, we are adjourned. Thank you very much.

[Whereupon, at 12:08, p.m., the Committee was adjourned.]

# APPENDIX


**Testimony Submitted by**
**Rob Arnold, CEO & Founder of**
**Threat Sketch, LLC**
**https://threatsketch.com**
**before the**
**House Small Business Committee November 15, 2017**

## Data Sharing

My company, Threat Sketch, makes extensive use of shared information to educate small businesses and guide their investments in cybersecurity. We are a small business ourselves, and I have written extensively on the subject of managing cyber risk using information based tools and methods[1]. Thus, I truly understand the needs and challenges around sharing cybersecurity information, of which there are two broad types.

1. *Incident reporting* refers to an after the fact report of companies that were attacked. It includes victim demographics, methods of attack, and losses incurred.
2. *Cyber Intelligence* generally refers to leading indicators of attack, and examples include newly discovered software vulnerabilities, suspicious activity, signatures of malicious software, and information about adversaries such as new capabilities.

[1] Arnold, Rob (2017). *Cybersecurity: A Business Solution.* ISBN 978-0692944158.

**Fragmentation**

The most fundamental problem in accessing this data right now is fragmentation. The DHS, FBI, NIST, and the NSA, are just a few of the agencies collecting cyber incident and intelligence information. Each has multiple repositories and programs. Some are well advertised, while some are part of workgroups and not widely available. Others are hidden by classification. Simply having a list of all the data sharing initiatives available would help tremendously.

Such a list might start with the various information Sharing and Analysis Centers (ISAC's) and Information Sharing and Analysis Organization Standards Organizations (ISAO's), and expand to include to programs like DHS's Automated Indicator Sharing (AIS) program. The inventory would include what information sources they consume, how they make the data available, and the membership criteria for each. The intermediate organizations like ISAC's and ISAO's are, in many cases, doing a great job of making otherwise inaccessible data available to small businesses [2].

Small businesses are extremely resourceful. Having quality incident reporting and cyber intelligence flowing to the small business community lets us build solutions for ourselves.[3] Our biggest challenge, in that regard, is collecting and aggregating data from a wide array of sources. In truth, even the largest multi-national companies cannot collect data on the breadth and scale that US government agencies can provide. Access to quality data for companies of all sizes helps level the playing field between large and small businesses and will spur economic development alongside novel solutions.[4]

**Overuse of Classification**

Another problem with sharing information is the overuse of classification. There are a myriad of rules governing the declassification of information, but declaring valuable information a secret is almost effortless. It takes no more than two words, uttered in a grave tone, to play keep away with vital information. *"That's classified."* And just like that, our cyber equivalents of neighborhood crime statistics and sex offender registries are taken away in the name of national security. While secrets have their place, we have a right to know what is going on around us, and every data point that gets classified degrades our ability to make good decisions [4], [5].

The other problem with classifying information is that it creates another digital divide between the have's and the have not's. Small companies are generally much better at raw innovation. When we cannot get access to the raw material for building novel solutions, our security posture will not improve and we lose economic opportunities to create jobs around our innovations.

---

[2] See Appendix: How the IT-ISAC makes AIS affordable
[3] See Appendix: Email Interview: Douglas M. DePeppe—Cyber Resilience Institute
[4] See Appendix: Economic Trends And How Shared Information Helps
[5] See Appendix: How Classification Impacted the Wannacry Outbreak and Response

As you contemplate the role of classification, please keep this in mind: When this country was founded, we were colonists living under the boot of a government that exerted control by keeping secrets and forcing access to information it deemed might be incriminating. Our adversaries would like nothing more than to goad our government into keeping secrets, then unleash those secrets to draw the ire of the citizens and undermine trust. Remaining transparent is the only solution that works in the long run. It is better that we let our enemies know we see them coming and face them head on, then to have us bickering with one another while they steal all our trade secrets [5].

**Pressure to Keep Up Poses Major New Threat**

There is a more pressing issue to which I need to draw your attention. It is a byproduct of two distinct disadvantages that small businesses face:

1. As big companies armor up, attackers turn to less protected small businesses.
2. Small businesses cannot afford to compete with big companies for the cybersecurity talent and solutions they need to protect themselves.[6]

These are circular issues with one begetting the other. In their wake, the demand for affordable solutions will rise dramatically, creating yet another threat. Small businesses desperate to meet the cybersecurity demands of larger clients, government regulations, insurance carriers, and lending institutions are going to become victims once again. Adversaries will use this opportunity to sell cheap software and services that are subsidized by selling data and secrets out the back door and give them a toehold in the supply chain of larger organizations.

The driver here is that cybersecurity is also economic warfare and a geopolitical game of chess that knows no borders. These higher-level battles manifest as foreign and domestic espionage, extortion, and economic disruption. They encompass aspects of both organized crime and the Cold War. A central issue that impacts small businesses is the ability to vet vendors who may have ties to either the criminal underground or nation-state adversaries.

**Deputizing Small Business Cyber Solution Providers**

I believe we can get ahead of this problem with your help. Fixing the problem with American-made products and services will not only protect the sector, but also stimulate job growth and economic development. I suggest that the SBDC's work with local, state, and federal law enforcement to certify local vendors as All-American solution providers, then connect those vendors with other SBDC's within their state and across the nation.

Participants would be bound to:

---

[6] The federal government is also snapping up scarce talent. For example, students can receive scholarships worth up to $60,000 for NSA accredited degree programs, but then they are obligated to work for the government. Small businesses cannot compete with that kind of recruitment.

- defend small businesses under a Hippocratic-like oath,
- affirm allegiance to US interests,
- produce software/services domestically (no offshoring data or talent), and
- report cyber intelligence using uniform methods.

Participants would be subject to steep legal penalties for using offshore solutions, perhaps submitting to spot-check investigations to ensure compliance. However, so long as they rely on American solutions, they (and perhaps their clients) would be protected by good-Samaritan laws much like our first responders. These deputized small businesses would also form a sort of national guard embedded directly in our business communities.

**Improving the Collection and Dissemination of Information**

In addition to tapping our SBDCs, I believe the government has two resources that can help with collection and dissemination of cybersecurity information. Our Bureau of Labor Statistics (BLS) is very good at aggregating, summarizing, and making data available in easy to digest forms. Meanwhile, the IRS is one agency to which every small business owner is happy to report losses.

Obviously there is potential for abuse in reporting losses that did not occur. To offset this, any loss report would trigger (or could trigger in the case of a lottery system) an investigation by law enforcement to validate claims. The investigation would allow for the gathering of valuable incident details and cyber intelligence information.

The DHS was established to bring together intelligence and data from multiple agencies. Therefore it makes sense to have data bubble up to them for aggregation and, when absolutely necessary, apply *judicious and time-limited* classification. Gathering points for information would include the IRS, as mentioned above, but also local/state/federal law enforcement, with SBDC advisors connecting small businesses to them as appropriate. In fact, it may be best to classify all data initially at the gathering points and charge the DHS with declassifying *everything*, except that which is truly vital to national security or conflicts with privacy. Dong so alleviates the SBDC advisors, law enforcement, and any deputize4d businesses from making such decisions.

While DHS has the ability to aggregate and (de)classify data, the Bureau of Labor Statistics (BLS) has the talent, infrastructure, and existing relationships to repackage and deliver it back to the community. Undoubtedly some will insist the data need not be made public. But security by obscurity only builds false hopes.[7] In fact, I would argue that the value added from the statistical expertise to *correctly* interpret raw data would far outweigh the idea of keeping poorly interpreted data secure.

An example of poorly interpreted data is the oft-quoted statistic that sixty percent of small businesses fail within six months of a

[7] See Appendix: How Classification Impacted the Wannacry Outbreak and Response

cyber attack. It is so tantalizing, that even we used it at Threat Sketch early on in our marketing materials. However, we later learned this to be unverified information and have distanced ourselves from it because our clients trust us to deliver accurate data.[8]

**SBDC Advisor Training**

Small businesses need local solutions that can tap into a national network of trusted solution providers. The SBDCs have proven effective in helping small businesses navigate a myraid of state, federal, and local resources, and with training. I believe they can rise to this challenge as well.

With regard to training, the NSA has been busy establishing a network of colleges and universities that are Centers of Academic Excellence (CAE) in Cybersecurity. And NIST, through its National Initiative for Cybersecurity Education (NICE), is helping standardize the language in our industry, which is much needed. I believe that the NSA-CAE community colleges and universities are well positioned to cross-train and up-train existing SBDC advisors on the *business aspects* of cybersecurity. Advisors need not become technical experts, but rather learn the standardized language developed by NICE and delivered through NSA-CAEs. Doing so will let them help small businesses locate and connect with appropriate resources.

[8] https://www.bankinfosecurity.com/blogs/60-hacked-small-businesses-fail-how-reliable-that-stat-p-2464

## Appendix

### How the IT-ISAC makes AIS affordable

The DHS has an information sharing program called Automated Indicator Sharing (AIS) that gathers and distributes cyber intelligence using STIX and TAXII protocols. When I first encountered this program through Threat Sketch, the only commercially supported software systems had six-figure price tags. Although free, open-source versions exist, they require constant patching and maintenance as well as a secure facility to house them. These hidden implementation costs put "free" information well out of the price range of small businesses.

We were referred by AIS to the IT-ISAC, which already has infrastructure in place to receive AIS information via STIX/TAXII and was able to fractionalize the cost among its paid members. The IT-ISAC has since played a vital role in both supplying data and allowing us to share our own knowledge back to the community.

### Email Interview: Douglas M. DePeppe - Cyber Resilience Institute

*Cyber Market Development Project, as well as Sports-ISAO Project Office. Our nonprofit, Cyber Resilience Institute, is the NIPP Challenge awardee (and our project will transition to commercial use under 'c-Market' branding and naming). Our model has a CTI and Information Sharing core, based in a community and adopting a PPP sharing and capacity building model.*

*That as a quick background, we enter communities through students and a workforce program: c-Watch. And, what we're promoting is the linking together of a network of cyber hunters and analysts—that is, graduates of the workforce program—into the Cyber Threat Intelligence Research Network. What CTIRN represents is a national capability of students—a bit like a CyberCorps or a cyber-ROTC equivalent—engaged in populating a commercial Order of Battle (i.e., adversary profiling), that would be available for the private sector and all levels of government, and without incurring IC classification constraints.*

### How Classification Impacted the Wannacry Outbreak and Response

I participated in the national response to the Wannacry outbreak lead by the National Cybersecurity and Communications Integration Center (NCICC; pronounced "N-KICK"). During one of the daily NCICC calls, a large company claimed to have something they wanted to share, but did not want to make it public. A DHS representative came on the line and declared the briefing TLP-Yellow from that point forward. He then invited all companies on the line to share what they knew and there was nothing but awkward

silence. Even under a veil of secrecy, the big company was unwilling to share what they knew. I wonder to this day what it was and if it could have saved even one victim.

And let us not forget that the reason the Wannacry outbreak was able to travel so quickly. It did so by leveraging an exploit discovered by the NSA and kept secret until exposed in a WikiLeaks data dump. I understand why the flaw was kept secret, but that decision was not without consequences. The entire attack may never had occurred had the flaw been disclosed to the private sector when it was first discovered. Not only did that decision lay the groundwork for the ransomware attack, but it created a rift between the government and the private sector. I know of at least one large-scale flaw that was not reported to the government for the reason that cybersecurity researchers have lost faith in our government. It will take a long time and many taxpayer dollars to recover from the tarnished image that results from keeping secrets.

**Economic Trends And How Shared Information Helps**

To describe how shared cyber incident and intelligence information helps small businesses, I need to provide context. At a company level, cybersecurity is a business problem of risk management. At a national level, cybersecurity is economic warfare. At a global scale it is a geopolitical game of chess that ignores physical borders.

At the business level, three trends drive cyber risk in small businesses. They are:

1. An increase in incentives for hackers to make money by exploiting stolen data.
2. A dramatic rise in the liability that comes with handling sensitive data.
3. The use of automation to attack small businesses on an industrial scale.[9]

Let's use a familiar example to illustrate how these three forces have changed the risk landscape. Consider an employee's W-2 form. Ten years ago it was hardly worth the paper it was printed on because there was no mass market for selling personal information. Today, each W-2 is worth $20 or more on underground, black markets. The incentive has gone from nearly zero to $20 dollars per victim.

While the hacker gets $20 for each W-2, the *liability* to the employer and the employee is substantially higher. In the extreme, lawsuits and drained bank accounts can cost the business and the employee hundreds of thousands of dollars. And more subtle losses come in the form of lost morale and the hassle of dealing with damaged credit, which add to the losses.

While there is an incentive to steal W-2s en masse from large companies, the big companies are becoming harder to attack. As a result, hackers are using automation to go after unprotected, unprepared small businesses by the thousands. Due to the volume of

[9] Arnold, Rob (2017). *Cybersecurity: A Business Solution.* ISBN 978-0692944158.

attacks, they only need to compromise a small fraction of them to make a profit. It is a nefarious business model that works.

In the context of trend number one, sharing cyber intelligence about black markets and espionage warns small businesses about emerging incentives for stealing data. To address the second trend, which is victim liability, incident reporting is used to understand trends in the risk landscape and to determine how different attacks relate to losses. Finally, combatting automated attacks means using both types of data to detect large scale operations and respond quickly to undermine the nefarious business model.


Prepared Testimony and
Statement for the Record of

**Ola Sage**
**Founder and CEO, e-Management**
**Co-Founder and CEO, CyberRx**

Hearing on

# "Federal Government and Small Businesses: Promoting Greater Information Sharing for Stronger Cybersecurity"

Before the

Committee on Small Business, U.S. House of Representatives

November 15, 2017

2360 Rayburn House Office Building

# Federal Government and Small Business: Promoting Greater Information Sharing for Stronger Cybersecurity

## Opening Remarks

Good morning Chairman Chabot, Ranking Member Velazquez, and distinguished members of the Committee. Thank you for the opportunity to testify today.

My name is Ola Sage and I am the founder and chief executive officer (CEO) of two small businesses in technology. My first company, e-Management, is an Information Technology (IT) professional services firm that provides a range of cybersecurity services and enterprise IT solutions for federal government clients. Headquartered in Silver Spring, MD, we employ approximately 70 professionals who actively serve our government clients. In our 18th year in businesses, I am proud of the many contributions our small business has been recognized for including a Cybersecurity Achievement Award from the Department of Energy (DOE) for Innovative Technical Achievement highlighting our technical excellence and best practices in cybersecurity detection and risk management. Last year, the U.S. Chamber of Commerce selected e-Management as one of the top 100 small businesses in America and earlier this year, we were delighted to be recognized as a *Best Places to Work* honoree.

Two years ago, I set out with bold plan to create a cybersecurity company, CyberRx, specifically focused on helping small and medium-sized companies (SMBs) improve their cybersecurity readiness. Our CyberRx software platform allows SMBs to assess their capabilities using a unique application of the *Cybersecurity Framework's (CSF)* five key functions: Identify, Protect, Detect, Respond, and Recover to better understand their cybersecurity posture, assess their risks and financial exposure; and provides them with a customized and detailed plan of action to improve their cyber readiness. CyberRx is both accessible and affordable, as we believe the best cybersecurity solutions should be available to all organizations, particularly the most vulnerable—SMBs.

It is also a privilege for me to serve as the first small business chair of the *IT Sector Coordinating Council* (IT SCC) since its establishment over a decade ago. The IT SCC, comprised of the nation's top IT companies, professional services firms, and trade associations, represents private sector interests in cybersecurity and critical infrastructure protection to the U.S. government. The IT Sector, represented by industry via the IT SCC and by Government via the IT Government Coordinating Council (GCC), work together in a public private partnership led by the IT Sector-Specific Agency (SSA), Department of Homeland Security (DHS), to address a wide range of critical infrastructure security and resilience policies and efforts affecting organizations of all sizes.

As a champion and advocate for cybersecurity readiness, I regularly meet with and speak to small business groups and CEOs about cybersecurity. I have also been involved in several efforts to promote cybersecurity information sharing in the SMB community, including the creation of the American Small Business Cybersecurity Xchange last year, a forum designed specifically to bring together SMBs, technical experts, and policy makers to address small business cybersecurity concerns. Last summer, I had the opportunity to testify to the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, of the Committee on Homeland Security on the Cybersecurity Information Sharing Act ("CISA") program and its impact on SMBs.

I am grateful for the opportunity today to testify as a small business owner. As you know, the definition of small business varies by industry. Depending on the industry, a company with 500, 1,000, or even 1,500 employees can still be considered a "small business" based on size standards defined by the Small Business Administration (SBA). The focus of my testimony today is for SMBs that have operational responsibilities to protect data for their employees, customers, vendors, or partners, regardless of size.

The perspectives and recommendations I share are informed by my own experiences running a small business, interactions with other small business owners, as well as my involvement with the IT SCC. Please note however that my observations do not necessarily reflect the views or positions of the IT SCC.

In my testimony, I will discuss:

- Cybersecurity information sharing in the SMB community,
- How the Cybersecurity Information Sharing Act (CISA) can be helpful to SMBs,
- Incentives to improve SMB information sharing and cyber threat reporting with the government, and
- Concluding thoughts.

**Small Businesses Are Reluctant to Share Cybersecurity Information**

Cyber-attacks are hurting small businesses. In the last 12 months, 61 percent of SMBs report that their companies have experienced a cyber-attack. More than half involved exposure of customer and employee information, with an average cost of $1,027,053 due to damage or theft of IT assets and infrastructure[1]. Recent ransomware attacks have been devastating with 1 in 5 companies forced to immediately shutdown operations for three days and in some cases, more than two weeks.[2] And while many believe their organizations are susceptible to external cybersecurity threats, a stunning 71% are not prepared to address them.[3]

Solving this problem requires greater information sharing between the government and the SMB community to help companies better identify threats, protect their infrastructure, detect anomalies, respond to, and recover from significant cyber events. However, there is a reluctance among many SMBs to voluntarily share information with government entities. Some of the frequently cited concerns include:

- Information gets lost or goes into a "black hole" causing companies to worry about what is happening with their data and whether it is being secured
- Requests for similar data from different agencies consumes scarce resources, distracts from business focus, and is costly
- Slow response time to requests/inquiries
- Information is misunderstood or misused
- For SMBs that do business with the government, fear that any negative information that is shared may be used against them in future procurements

For any sharing information initiative to deliver real value and have substantive impact, it must be based on mutual trust, which cannot be mandated or demanded. As the government looks to encourage greater cybersecurity information sharing with small businesses, understanding some of the concerns SMBs have about sharing information, in general, with the government may be useful in developing strategies to overcome potential hurdles to sharing reporting cybersecurity specific information.

[1] 2017 State of Cybersecurity in Small and Medium-Sized Businesses, Ponemon Institute, September 2017
[2] Second Annual State of Ransomware Report: US Survey Results, Malwarebytes, July 2017
[3] Cyber Threats to Small and Medium-Sized Businesses in 2017, Webroot, 2017

**CISA Applies to Small Businesses, But They Don't Know**

In my testimony last year to the House Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, of the Committee on Homeland Security, I provided some observations on the new law and suggestions for how CISA could be made more relevant to the SMB community. While significant progress has been made in implementing the law in general, several challenges raised last year still persist for SMBs.

1. ***Small businesses are <u>still</u> unaware of CISA or how it helps them.***

   In its Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015, the Inspector General noted that since the law passed, DHS has taken some important steps to: 1) develop adequate policies and procedures and a supporting capability to share cyber threat indicators and defensive measures; 2) properly classify cyber threat indicators and defensive measures and account for the security clearances of private sector users; and 3) use the cyber threat indicator and defensive measure information received to mitigate potential security risks.

   The report, however, did not mention anything about raising SMB awareness of information sharing initiatives and CISA. While there are minimal references to small business in the law itself, arguably CISA does apply to SMBs and addresses some of the barriers to information sharing identified above, particularly in the area of liability protections. To encourage greater cybersecurity information sharing, CISA provides: 1 ) protection of properly designated proprietary information; 2) exemption from Federal and State FOIA Laws for information shared under CISA ; 3) protections against regulatory or enforcement actions taken as a result of information shared under CISA; 4) non-waiver of privileges and other legal protections, including trade secret protection; 5) anti-trust exemption for sharing cyber threat information or defensive measures with other companies; and 6) protections for sharing and receiving information when done in accordance with CISA's requirements.

   There is still an opportunity for DHS and the government in general to increase the visibility of the law through its existing outreach and awareness programs to the SMB community through, for example, DHS' Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) initiatives, Small Business Administration (SBA) programs, or by working with Chambers of Commerce, small business associations, and trade groups.

2. ***Small businesses are <u>still</u> confused by the myriad of information sharing initiatives.***

   The number and variety of information sharing initiatives continue to expand. It is still unclear to many small businesses whether they need them, and if so, which to use and when. Government options include agency resources for specific industries (e.g. Energy, Financial Services), DHS' Enhanced Cybersecurity Services, the Cooperative Research and Development Agreement, the National Cybersecurity and Communications Integration Center, the Automated Indicator Sharing program, among others. On the industry side, Information Sharing and Analysis Centers (ISACS), Information Sharing and Analysis Organizations (ISAOs), and private for-profit and non-profit organizations also offer a range of services. An SMB Guide for Cybersecurity Information Sharing would help SMBs better understand the value various information sharing options provide.

3. ***Cybersecurity information can be costly for small businesses.***

   When it comes to information sharing, one size does not fit all for SMBs who must decide what services are most critical weighed against their risk tolerance, capabilities, and budget One of the distinct advantages the government has in sharing cybersecurity information with SMBs is that the information is "free." However, while the data may be free, many small businesses do not have adequate resources to stand up the necessary infrastructure to exchange data or the technical expertise to manipulate and analyze the data in a useful way. Depending on the type of business, it may make more sense for a particular SMB to sign up with a commercial information sharing organization. Unfortunately, many of the options available today cost thousands of dollars per year, putting them out of reach for many SMBs.

**Incentives to Improve SMB Information Sharing And Cyber Threat Reporting With The Government**

Many studies have been conducted and papers written over the years on incentives and whether or not they have a determinative impact on behavior. While the data may not be conclusive, incentives have been shown to work better when designed with specific outcomes in mind. Below are a few for consideration. Several of these proposals have been offered over the years in various forms, but with the increasing risk facing SMBs, the time is right to take action.

1. **Expand CISA liability protections to protect SMBs from potential liability in the event of a data breach or cyber-attack**

   CISA currently protects companies when sharing cyber threat indicators and defensive measure with other companies, but it does not currently shield companies from potential liability in the event of a data breach or cyber-attack. To provide a positive incentive for SMBs to share information with the government, Congress might consider a solution that extends liability protection up to a maximum threshold in the event of a data breach or cyber-attack to SMBs that exhibit a measureable commitment to information sharing through demonstrated use of the Cybersecurity Framework developed by NIST to increase their maturity above and beyond the partial level, voluntarily participate in one or more public or private information sharing forums, and maintain active cybersecurity insurance.

2. **Tax Incentives**

   Tax incentives are often used by governments to promote specific behavior, in this case improving cybersecurity information sharing. To further encourage voluntary sharing of cyber threat information with the government, an ISAC or an ISAO, Congress might consider introducing tax incentives that could include deductions and credits for cybersecurity and information sharing related capital investments and personnel, incentives for accelerated depreciation of cyber-related equipment, deductions for cybersecurity related expenses, etc.

3. **Include use of the CSF and participation in a public or private information sharing program as a selection criteria for government procurements**

   The government has and continues to use preferential consideration in the procurement process to promote participation or influence desired behavior. Examples include procurement considerations for minority groups, quality and process improvement standards such as ISO, CMMI, and research priorities, among others. To encourage greater cybersecurity information sharing and reporting, Congress might consider use of the CSF and participation in a public or private information sharing program as selection criteria in government procurements. GSA offers recent examples of preferential consideration for quality standards in procurements such as its GSA Alliant 2 Small Business GWAC.

4. **Recognize SMBs that commit to cybersecurity information sharing**

   Public recognition offered by voluntary programs can be important instruments to promote desired behavior while serving as a signal of commitment or quality to the market. Programs such as EPA's Energy Star, a joint program of the Environmental Protection Agency (EPA) and the Department of Energy (DOE), has produced impressive results over the past 20 years, by recognizing and highlighting consumers, businesses, and industry committed to the adoption of energy efficient products and practices. Voluntary programs

like this could serve as a blueprint to design a public recognition program for SMBs participating in public or private cybersecurity information sharing programs.

**5. Simplify the entry point for cyber threat reporting for SMBs**

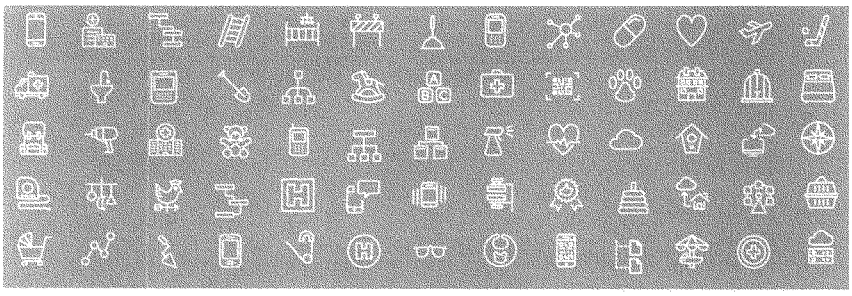
When it comes to reporting cybersecurity incidents, most SMBs either don't know who to call or are overwhelmed by the choices, and therefore, won't bother. For example, on one government website, the following guidance is provided.

> **If Your Business Has Been The Victim of a Cyberattack**
>
> - Inform local law enforcement or the state attorney general as appropriate.
> - Report stolen finances or identities and other cybercrimes to the Internet Crime Complaint Center.
> - Report fraud to the Federal Trade Commission.
> - Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or the US-CERT website

While such guidance is intended to be helpful, most SMBs don't know how or where to get the contact information for several of the resources cited in order to report.
Perhaps the "911" system provides a model. Since 1968, "911" has been designated as the nationwide emergency number for the public to request emergency assistance and provides fast and easy access to a Public Safety Answering Point (PSAP). Last year, the Critical Infrastructure Partnership Advisory Council (CIPAC) formed a working group with DHS' Office of Infrastructure Protection to investigate how to get a National Tip Line started that would serve as the single POC for reporting emergency cybersecurity information. Using the example above, one could envision a scenario where an SMB calls the national emergency response number and based on information provided would immediately be connected to the appropriate resource(s). Initiatives like this are an important step in simplifying the process for cyber reporting and encouraging more SMBs to engage.

**Conclusion**

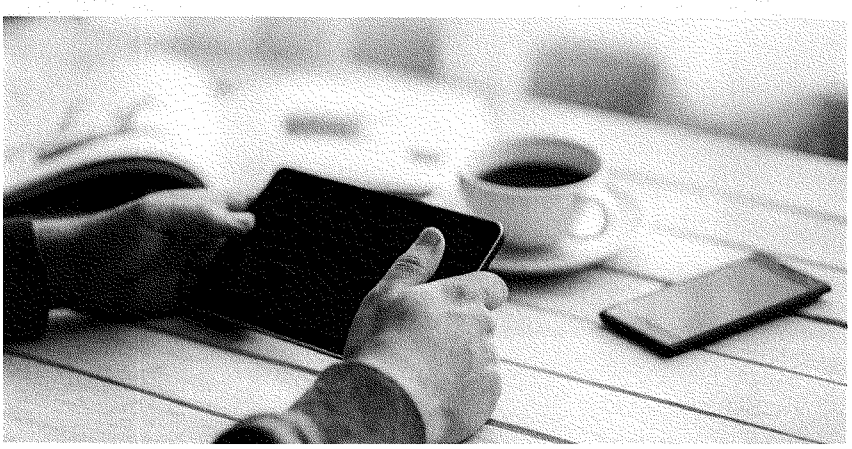
CISA is still early in its life cycle but holds tremendous promise for the value it can bring, in particular, to the SMB community as more companies become aware of the law and how it can help them. We at e-Management and CyberRx look forward to continuing to work with Congress to promote greater information sharing and to make the application of CISA more relevant to the SMB community. Thank you again for the opportunity to testify. I am ready to answer any questions you may have.

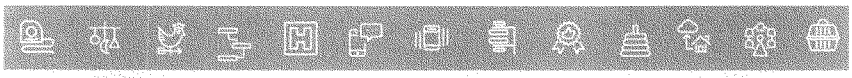


ACT | The App Association

Testimony of
Morgan W. Reed

Before the
U.S. House of Representatives Small Business Committee
November 15, 2017





## Executive Summary

Chairman Chabot, Ranking Member Velázquez, and distinguished members of the Committee: My name is Morgan Reed, and I am the president of ACT | The App Association. I thank you for holding this important hearing on improving cybersecurity for small businesses.

ACT | The App Association represents more than 5,000 app makers and connected device companies across the United States that continue to grow and create American jobs in every congressional district. Alongside the embrace of mobile technology across consumer and enterprise contexts, our members have been creating innovative solutions to improve workplace productivity, accelerate academic achievement, and help people lead healthier lifestyles.

In our current environment, cybersecurity threats can seem incomprehensibly vast and inevitable, especially for small businesses. In 2014, 71 percent of companies admitted they fell victim to a successful cyber-attack.[1] Meanwhile, the amount of data online is expected to increase 50-fold by 2020,[2] signaling accelerated tech innovation but also adding new attack vectors due to increased connectivity and a sweetening of the pot for potential cyber criminals. Cybersecurity risk management strategies must keep pace with this growing threat—a task that evolves as more online traffic and commerce is dedicated to the internet of things (IoT).

We support ongoing and emerging public-private partnership initiatives and strategies to improve the nation's cybersecurity risk management posture. But we believe that the small businesses representing 99.7 percent of U.S. firms[3] require heightened focus and assistance and must play a much more significant role in these strategies. Policymakers must remain mindful of the fact that large companies often have expansive budgets available to create and maintain cybersecurity control processes and have the luxury to hire staff and outside consultants to address cybersecurity risks, but small and medium-sized enterprises (SMEs) do not. For many App Association members, chief security officer may be just one of five hats worn by a single employee. The essential role of American small businesses, along with the unique resource constraints they face, make this Committee's work more important to the security and stability of the nation's economy.

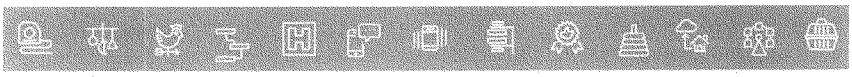
Small and medium-sized tech companies like our members exist to solve problems. Take Canned Spinach for example, an App Association member company based in Chairman Chabot's district. Canned Spinach, led by partner Andrew Savitz, uses cutting-edge security-by-design processes to create custom software solutions that streamline backend processes and enhance business-to-business relationships. The services he provides fill a niche and solve problems, most often helping other small businesses access the opportunity of the app economy in a secure and sustainable way. Canned Spinach's approach is representative of all App Association members' in proactively and responsibly managing cybersecurity risks.

Further, the symbiotic platform-developer relationship drives innovative cybersecurity risk management, providing benefits across consumer and enterprise contexts. For example, the small businesses that use Etsy,[4] headquartered in Ranking Member Velázquez's district, agree to use strong data security methods[5] when they handle consumer data on the platform. In this way, Etsy's contractual terms help drive both dynamic risk management practices and good 'cyber hygiene,' small businesses are not alone when it comes to cybersecurity. Small businesses know the platforms they use to sell their services and goods—whether they be Apple, Microsoft, or Etsy—are there to hold them accountable but also to help them meet their obligations on cybersecurity.

Alongside the development of private sector-driven cybersecurity activities, the federal government should take focused, concrete steps to help SMEs succeed in security. To better protect your constituents and our customers, we need your help in three specific ways: First, we need the federal government to improve its information sharing activities; second, the federal government should take steps to make cybersecurity frameworks and best practices more workable for SMEs; and third, the federal government should ensure a legal and policy environment that enhances SMEs' ability to adequately manage dynamic cybersecurity risks. To this end, I will elaborate on three main points in my testimony:

- The federal government should make the cybersecurity threat information it shares timely, more accessible, and more useful to SMEs.
- The federal government should help SMEs improve their understanding of cybersecurity risk management by developing and widely publicizing targeted, user-friendly, and compelling best practices and guidance that is built on key public-private partnership-driven deliverables such as the National Institute of Standards and Technology's (NIST) voluntary Cybersecurity Framework.[6]
- Congress should take steps to provide legal and policy certainty that SMEs can rely on when they leverage the best technical protection mechanisms (TPMs) available. For example, Congress should pass the International Communications Privacy Act (ICPA, H.R. 3718 and S. 1671) to clarify SMEs' legal liability in data requests, and maintain a legal environment that supports investment in cybersecurity.

Thank you for the opportunity to share insights on behalf of our member companies. I look forward to a productive discussion about how we can encourage better cybersecurity practices by SMEs in your districts.



## I. The Federal Government Can Help SMEs Improve Cybersecurity

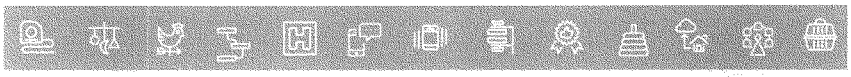
### a. Small Businesses Leverage Security Infrastructure Offered by Large Company Platforms

Fortunately, SMEs are often able leverage the numerous security features and capabilities larger platform and cloud service provider companies offer. In this manner, SMEs can offload security infrastructure overhead. Microsoft's Azure, for example, has worldwide visibility into cyber threats and is able to observe based on what all of its users are reporting to the platform. Azure invests about $1 billion annually to advance its efforts on security, data protection, and risk mitigation, and employs over 3,500 security professionals.[7] These experts take measures such as setting up honeypots to attract cybercriminals and watch how they behave—intelligence that SME users of Azure benefit from directly. Beyond cloud services, Apple HealthKit provides a platform that defends against cyber threats on behalf of the SMEs who build products on top of it. And Intel has created a new Sawtooth chip to enable enterprise blockchain frameworks on which SMEs can innovate in a secure fashion. These various platform-SME relationships point to the many ways SMEs can leverage security infrastructure offered by the platforms. However, these arrangements do not tell the whole story and there remains significant work the federal government can do to improve information sharing for SMEs.

### b. Awareness and Enhancement of Information Sharing Efforts

The Department of Homeland Security (DHS) has undertaken several efforts to facilitate timely cyber threat data sharing over the years. Unfortunately, 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's Office of Cybersecurity and Communications (CS&C). The US-CERT is currently the triage and information sharing branch of CS&C's National Cybersecurity and Communications Integration Center (NCCIC), which opened in 2009.[8] But ultimately it is DHS's 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 by which private sector entities receive and share threat data are often private sector-led information sharing and analysis centers (ISACs). While this construct has helped create a flow of cybersecurity threat information between and amongst public and private organizations, we believe that improvements are needed to bring their benefits to American SMEs, which often lack the resources (financial, time, and staff) to join and actively participate in ISACs. Moreover, most ISACs were created around U.S. government-designated critical infrastructure sectors,[9] and most of our members fall outside the siloed definition of an individual critical infrastructure sector or sectors. Executive Order 13691 created Information Sharing Analysis Organizations[10] (ISAOs) in part to alleviate this problem. Meanwhile, the market has responded to the need for timely cybersecurity information sharing, resulting in organizations that offer such information sharing services (and related cybersecurity threat mitigation services) as a business.

In practice, however, these efforts and initiatives—both government and private sector—have yet to make a meaningful impact on the small businesses that drive the digital economy's growth, innovation, and job creation, and many questions remain unanswered for our members. When an App Association member is hit with a cyberattack, with whom do they share it as the attack is occurring (as opposed to when a breach is discovered after the fact)? Somebody at NCCIC? Somebody at their local Fusion Center or an ISAC? Where are these entities located, and how should companies share threat information with them? While we note that the U.S. government has taken numerous steps to answer these questions, more can be done to educate SMEs like our members about them. For this reason, it is paramount that reinvigorated, enhanced federal outreach do more to communicate the answers to these questions to put us on the road to improving information sharing for small businesses.



Any private sector efforts to stand up an ISAC in the small business tech sector should be accompanied by federal efforts to improve the mechanics of information sharing. DHS should strive to make cybersecurity information that is shared user-friendly and understandable, and of the highest quality possible. We commend federal efforts in this respect (for example, NCCIC and US-CERT work on the Trusted Automated eXchange of Indicator Information [TAXII™], the Structured Threat Information eXpression [STIX™], and the Cyber Observable eXpression [CybOX™][11]). We also note that in a report issued on automated indicator sharing by the DHS's own Office of Inspector General (OIG) last week, the velocity and volume of threat information has improved.[12] This is a commendable improvement from 2015, when a report by Senator Tom Coburn, then-ranking member on the Senate Committee on Homeland Security and Governmental Affairs, found that private threat sharing centers were publishing, and patching, threats before US-CERT could even issue a warning.[13]

However, the OIG report also found that a few obstacles prevent the data US-CERT shares from being valuable and user-friendly. For example, the report noted that the pre-determined data fields limit the usefulness of threat data by restricting the descriptions of "specific incidents, tactics, techniques, and procedures that unauthorized users used to exploit software vulnerabilities."[14] We appreciate the tension between automating and standardizing how cybersecurity attacks are characterized with the diverse and dynamic nature of cyber-attacks; therefore, appreciating the value of TAXII™, STIX™, and CybOX™, we believe that DHS should also strive to permit cyber-attack reports to incorporate some flexibility and allow for the novel approaches attackers use to manipulate attack vectors and penetrate networks. Moving forward, we believe machine learning and artificial intelligence should be a critical tool to help make less structured threat information more useful for the private sector.

Unfortunately, our enemies are already using machine learning to orchestrate their attacks and evade less sophisticated defense measures. In order to prevent truly asymmetrical cyber warfare, our defenses must include cutting-edge methods and strategies, which, ultimately, the cybersecurity information sharing construct available to American SMEs should facilitate.

## c. Publicize Best Practices that are Truly Scalable for SMEs

The NIST Cybersecurity Framework provides a scalable, flexible, voluntary toolbox that any organization can use to reduce vulnerabilities, prevent intrusions, and mitigate damage caused by cybersecurity attacks. However, our SME members often struggle with its detail and complexity, facing other (market-driven) priorities that do not allow them to fully leverage the Framework. Version 1.0 of the Framework is 41 pages long, and the draft of Version 1.1 is even longer, at 61 pages. Small businesses, even those in the tech sector, have precious little time and resources to get through dense documents, much less those that recommend consultation with large suites of risk management standards that often have expensive certifications associated with them.

Despite its complexity, we believe the Cybersecurity Framework is a comprehensive guide and should be the touchstone for efforts to enhance private sector efforts. Therefore, federal efforts around best practices must include references to the Framework and should center on simplifying its recommendations. We commend NIST itself, in recognition of this tension, for developing an SME-focused Framework fundamentals deliverable.[15] Further, the Federal Trade Commission (FTC) promulgates best practices in the form of its "Start with Security" guide for SMEs, which draws on the NIST Framework.[16] These SME-targeted efforts by NIST, the FTC, and other agencies are a great start, but as a nation, we have much work to do. Because bottom lines command business decisions, we suggest that such targeted education focus on making a business case (return on investment) for the use of the Framework.

We believe that this committee can directly assist the federal government's efforts to improve American SMEs' ability to manage cybersecurity risk through a new federally-funded national education campaign focused on improving SME cybersecurity risk management practices. Such education could help avoid the vast majority of cybersecurity breaches, which occur due to lack of basic cybersecurity hygiene. The Small Business Administration (SBA), with an infrastructure in place to reach SMEs in every region of the nation, would be well positioned to champion such a national campaign. As Joe Bonnell, the CEO of App Association member Alchemy Security in Denver, CO, aptly summarizes, "any capital allocated toward driving improved cyber hygiene within this constituency should include outreach programs through either regular lunch-and-learn activities through entities such as the SBA, or by funding user security awareness training similar to the "schoolhouse rock" campaign, which would provide tremendous investment leverage and could also be used to educate everyday Americans as well." The App Association commits to work with this committee to help create and shape such a campaign.

### d. Facilitate Feedback from SMEs

The federal government should work with SMEs to understand the kinds of information sharing activities they are able to engage in and how to leverage federal information sharing resources.

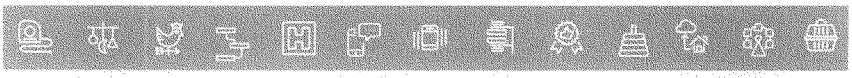
Without a proper understanding of how small businesses are implementing the resources currently available, it is difficult to know what to do with the existing programs and frameworks to improve their accessibility and usability for SMEs. With adequate federal support, the Small Business Administration can assist NIST, DHS, sector-specific agencies, and other federal actors in gathering this input to inform future steps based on robust feedback from SMEs across all sectors as to which approach is most workable. The App Association is committed to assisting the federal government in understanding the unique challenges faced by the small business tech community.

## II. The Statutory and Regulatory Environment Should Encourage SMEs to Effectively and Efficiently Manage Dynamic Cybersecurity Risks

### a. Encryption and Law Enforcement Access to Data

Although encryption is not a complete solution by itself, it is an essential tool, especially for SMEs, to protect data. Any transaction involving data depends on TPMs, including end-to-end encryption (defined as a set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key), to maintain the integrity of data and ultimately the user trust on which our members' success depends. Any transfer of sensitive data—financial, health, etc.—requires that all available means be taken to provide for security and the integrity of the data. Encryption's role should not be understated—without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised.

Not only is the use of strong encryption a business necessity that every App Association member faces, but the U.S. government itself also currently plays an important role in promoting the use of encryption. NIST's Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.[17] NIST also provides the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography-based standards.[18]



Further, NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, lists HIPAA-related storage security needs, and describes the need to encrypt and decrypt electronic protected health information.[19]

Despite the important role encryption plays, various interests persist in demanding that "backdoors" be built into encryption for the purposes of lawful access. Mandating that "backdoors" be built into encryption for government access would not only degrade the safety and security of data, but it would also jeopardize the trust of end users. Backdoors are enticingly simple, but they are dangerously counterproductive—they create known vulnerabilities that any unauthorized parties can exploit. Undermining the technical proficiency of encryption moves us away from, rather than towards, legitimate policy goals such as law enforcement access to data.

Recent calls for "responsible" encryption simply are not responsible for your constituents or for our customers. This is a lesson we learned in the 1990s with the Clipper chip, which was a mistake that should not be repeated. "Responsible" encryption is just another word for broken encryption, especially when encryption can serve as a far better tool for crime prevention than investigation. We want to stop the bad guys before they act, and encryption can keep them at bay. We want to make data security for our customers and your constituents stronger, not weaker.

When investigations must take place, SMEs have been known to work well with local, state, and federal law enforcement officials. The App Association supports a collaborative approach between companies that retain customer data and law enforcement officials who seek access to it. To that end, legislation introduced in the House and Senate helps clarify when and how law enforcement may access communications data stored overseas using a warrant. The App Association strongly supports this legislation, the International Communications Privacy Act (ICPA, H.R. 3718 and S. 1671), and we urge members of the committee to cosponsor it. We will continue to look for opportunities to facilitate the mutually beneficial relationship between law enforcement agencies and SMEs in a manner that preserves the integrity of data security and encryption.

## b. Liability Certainty for SMEs Seeking to Share Timely Cybersecurity Information

The Cybersecurity Information Sharing Act of 2015 (CISA) helped define private sector liability from sharing cyber threat data. As mentioned above, private sector information sharing efforts usually take place through ISACs or ISAOs. While only time will tell, the passage of CISA appears to have helped encourage more timely sharing by establishing liability protection for those responsibly sharing "cyber threat indicators," as long as personal information not directly related to the cybersecurity threat is "scrubbed." While CISA has provided some clarity, SMEs sharing cybersecurity information must take great care to meet these scrubbing requirements before they share. They cannot afford to absorb prolonged and expensive lawsuits like large multi-national corporations can in the event liability attaches to the sharing. Moreover, even though liability protections may exist, SMEs must also trust that those protections will apply to them in specific contexts. It takes time and effort to foster trust between SMEs and the federal regulators that can put them out of business for missteps. Practically, when such a question is presented to an SME's general counsel or outside counsel, it is much easier to simply say "no" than it is to engage in timely information sharing constructs and take on any liability.

Despite this reality, using DHS guidance for CISA compliance, more legal certainty exists for companies to share threat information, particularly through ISACs and ISAOs. However, as we discuss above, belonging to an ISAC or an ISAO often may present resource issues for SMEs (with a few exceptions).[21] We understand that ISAOs were developed specifically to fill the increasingly visible gaps between ISACs, as well as to permit other affiliations that may organically become attractive (e.g., based on location in a geographic region), but the ISAO standards process does face some criticism, and has not yet been completed. The App Association continues to educate its members on the legal issues associated with sharing cybersecurity information with other private entities and the government, and we offer our support to work with this committee and all stakeholders to further streamline the process.

## III. Conclusion

We applaud the committee's attention to 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 requires close coordination between government, experts, and the private sector. If the conditions are right, our SME members will set the pace.

1- https://cloudblogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/
2- https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html
3- https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf.
4- https://www.etsy.com/
5- https://www.etsy.com/legal/terms-of-use/#privacy
6- NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214final.pdf; see also 79 Fed. Reg. 9167 (Feb. 18, 2014).
7- https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi35bKX2bvXAhWD64MKHYuxA3cQFgg5MAE&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F4%2F6%2F8%2F4680DFC2-7D56-460F-AD41-612F1A131A26%2FMicrosoft_Cyber_Defense_Operations_Center_strategy_brief_EN_US.pdf&usg=AOvVaw1ax_GFcYWY67kEBbU4XbZp
8- https://www.us-cert.gov/nccic
9- https://www.dhs.gov/critical-infrastructure-sectors
10- https://www.dhs.gov/isao
11- https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.
12 -https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-10-Nov17_0.pdf
13- https://www.hsgac.senate.gov/download/?id=B92B8382-DBCE-403C-A08A-727F89C2BC9B
14- https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-10-Nov17_0.pdf
15- http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
16- https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
17- http://csrc.nist.gov/
18- http://csrc.nist.gov/groups/STM/cmvp/
19- http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
20-https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf
21-See https://www.fsisac.com/faqs#576

**STATEMENT FOR THE RECORD OF**

**THOMAS GANN, CHIEF PUBLIC POLICY OFFICER, MCAFEE, LLC.**

**BEFORE THE U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SMALL BUSINESS**

**ON "FEDERAL GOVERNMENT AND SMALL BUSINESSES: PROMOTING GREATER INFORMATION**

**SHARING FOR STRONGER CYBERSECURITY"**

**November 15, 2017, 11:00 AM / RAYBURN HOUSE OFFICE BUILDING ROOM 2360**

Good morning, Chairman Chabot, Ranking Member Velazquez, and distinguished members of the committee. Thank you for the opportunity to testify today, I am Tom Gann, Chief Public Policy Officer for McAfee, LLC. I have over 20 years of experience in the IT industry, having run government relations and public sector alliances functions for Digimarc, Siebel Systems and Sun Microsystems. During the last decade, I have focused on cybersecurity and identity management issues. I hold degrees in business and political science from the London Business School and Stanford University.

I am pleased to address the committee on this important matter. My testimony will address the cybersecurity challenges small businesses face, why sharing technical information is particularly difficult for small businesses, the types of information sharing that could be most useful to them, and general recommendations that can enhance the cybersecurity capabilities of small businesses.

## MCAFEE'S COMMITMENT TO CYBERSECURITY

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other industry products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, we secure their digital lifestyle at home and while on the go. By working with other security players, we are leading the effort to unite against state-sponsored actors, cybercriminals, hacktivists and other disruptors for the benefit of all. McAfee is focused on accelerating ubiquitous protection against security risks for people, businesses and governments worldwide.

Before beginning my comments, I want to express how extremely pleased McAfee is in seeing the focus on improving the cyber threat landscape for small businesses. Through the past several years, a great deal of time and effort has been focused on larger organizations with resources to invest, but attention on risks to small busi-

ness—the backbone of our nation's economy—is long overdue. For too long, small businesses have been a target of malicious actors with little or no way to protect themselves due to education and resource constraints. Thank you for investigating ways to better protect this vital segment of our digital economy.

## CYBERSECURITY RISKS FACED BY SMALL BUSINESS

There's no doubt that small businesses face many of the same cybersecurity risks as large ones. Some cyber-attack methods, such as ransomware and those that begin with spear-phishing, are particularly well-suited to small businesses, who might be an easy target because of their lack of cybersecurity resources. Small businesses store personal information, implement operational requirements and own valuable intellectual property just as large enterprises do, so they too need strong cybersecurity protections. In fact, more than 50 percent of cyber-attacks are launched on firms having fewer than 50 employees, according to cyber expert Steve Morgan. A 2016 report from Keeper and the Ponemon Institute found that only 14 percent of small and medium-sized businesses say they have the ability to effectively mitigate risks and vulnerabilities. Further, 50 percent say they had been breached in the past 12 months. This is not at all surprising, given that many small businesses might not even have IT staff, let alone cybersecurity staff.

Not addressing these risks have real consequences for the businesses themselves, larger businesses and local economies. For example, an August 2017 analysis by Tech Republic found that a single cybersecurity attack could cost a small business $256,000. And we've seen at least one instance of a small business breach affecting a larger one in the Target hack.

An October study by the Better Business Bureau, The State of Small Business Cybersecurity in North America, found that half of small businesses could remain profitable for only one month if they lost essential data. Further, while small businesses may be adopting solutions like antivirus software, one of the most cost-effective tools, employee education, is used by fewer than half the companies surveyed. The report also found that while awareness of cybersecurity risk among small business owners is growing, they are not at all certain what to do about it.

According to an August 2017 survey from BizBuySell, the Internet's largest business-for-sale marketplace, 90 percent of small businesses believe it's at least important to protect themselves from a cyber-attack. Yet moving from cyber protection being important to it being essential, practical and affordable is a big step. Investing in more than just very basic cybersecurity tools requires time, money and other resources—like an IT staff—that small businesses often don't have. We have to acknowledge the fact that for most small businesses, cybersecurity is an expense they don't want to incur when they're trying to simply make payroll and remain profitable.

"Profitability is the ultimate test of risk," one of the Better Business Bureau report's authors said, adding that small business own-

ers have to do a cost-benefit analysis of cybersecurity." It doesn't do any good for a small business to adopt a $10,000 solution if the potential risk reduction is worth $5,000," he added.

**THE INFORMATION SHARING CHALLENGE FOR SMALL BUSINESS**

So, what's the solution? Should small businesses participate in the Department of Homeland Security's (DHS) cyber threat information sharing program mandated by the Cybersecurity Information Sharing Act (CISA)? This is a question worth exploring. In talking with our customers, it is clear that many small businesses are unaware of CISA, often don't understand how the law can help them, and are confused by the many information sharing initiatives out there.

However, I also believe we should consider how information sharing efforts, such as those mandated by CISA, can directly benefit small businesses.

The DHS initiative known as Automated Indicator Sharing (AIS) is open to small businesses, but few have the resources or an educated IT staff to make direct use of or benefit from it. The kind of information shared via AIS is comprised of indicators of compromise (IOCs). While the overall program has been a strong step in the right direction, it still provides far too little real value. IOCs are just the breadcrumbs that network security staff look for to uncover clues as to what may be occurring inside their organizations. Typical IOCs include registry keys, MD5 hashes of potential malware, IP addresses, virus signatures, unusual DNS requests, and URLs. While these can be useful, they are not enough to provide the defensive information needed to protect an organization.

The information shared must be both useful and actionable to the receiving parties and, in the case of AIS, it also must be automated. As many small businesses outsource functions like their point of sale systems, or even their entire IT needs, they may not have access to the information contained there, let alone be able to ensure it is useful and actionable. Even if they had their own IT support infrastructure, small businesses would have to acquire and set up systems and software to collect, share and use the information. The reality is any information sharing capabilities require time, money and resources that many small businesses just do not have.

Additionally, it should be understood that we are not sharing information just for sharing's sake. There needs to be a valuable purpose for the sharing if a business is going to spend the money needed to set it up and maintain it going forward as a core business practice. If the information being shared is not useful, actionable and automated, then the entity sharing it doesn't bring much value to the table—nor would the small business get value from it. Today, the type of simple information via IOCs exchanged by AIS is hard for small businesses to get value out of.

**A DIFFERENT KIND OF INFORMATION SHARING**

This doesn't mean that small businesses don't need or can't benefit from cyber threat intelligence; they certainly can. But perhaps we should focus our discussion more on sharing a different kind of information—information that is more informative and educational right away.

The Better Business Bureau study found that when asked to judge 10 statements on cybersecurity as either true or false, the average score was below 60 percent, meaning that there are still opportunities to better educate small businesses and dispel some myths. And regarding what to do first in a data breach, only about 20 percent of respondents answered correctly. Granted, the laws vary from state to state and can be complicated, but this just points out the need for more education on the benefits of having a plan before a breach occurs.

Education and awareness efforts are essential. The Federal Trade Commission (FTC) just last month launched a new site for Protecting Small Business that offers advice on cybersecurity basics, protecting personal information and what to do in the event of a data breach. Likewise, the Small Business Administration (SBA) also provides resources on its website. We need even more initiatives like these that make it as easy as possible for small businesses to learn more about how to protect themselves.

The federal government can also help raise awareness among vendors and solutions providers of the role small businesses play in protecting the nation's critical infrastructure. Many important government contractors are small businesses and, as we learned in the retail attacks of 2014, small businesses are attractive attack conduits for breaching larger business or government targets rich in high-value data or other assets.

**DEDICATED INFORMATION SHARING ORGANIZATION FOR SMALL BUSINESS**

The federal government should also help develop and fund the standup of a non-profit Information Sharing and Analysis Organization (ISAO) focused on U.S. small businesses. Small businesses do not have the resources to address the problem of gathering and analyzing cyber threat intelligence on an ongoing basis, but a highly targeted ISAO with initial support from the federal government could help. A small business-focused ISAO could use the economies of scale to be able to supply appropriate information to those business that lack the resources but still need current cyber threat intelligence. Such an ISAO could provide education services to its members as a part of their services, such as basic cyber hygiene and more advanced topics like incorporating the NIST Cybersecurity Framework into their security program. Cyber education is critical to the success of small business being able to understand the problems in order to begin addressing them.

The ISAO could provide its members with best practices, lessons learned, templates and processes for addressing incidents, the ability to get help understanding the problems and act as a hub in case a breach occurs. In the event of an incident, small businesses need to know where to go and what to do. The ISAO could also act as

the first point of contact in determining whether or not to reach out to law enforcement and to assist the business in addressing the incident. This would also allow the ISAO to communicate the situation to its other members so that they too could be informed.

An information sharing organization such as this would be also able to spread costs among its members. We encourage the government to consider providing the initial startup funding for a national small business ISAO.

## ADDITIONAL RECOMMENDATIONS FOR PROTECTING SMALL BUSINESS

Move to the Cloud

Advances in technology can also serve to protect technology. For example, outsourcing infrastructure to a cloud provider is becoming more common. This practice could have real advantages for a small business, as the cloud provider would be responsible for security. Both infrastructure as a service and security as a service warrant attention from small business, as both can be economical ways to provide efficiencies and security without the business owner having to think about it. The growth of cloud applications has made these "as-a-service" technologies real possibilities. Leveraging them could enable a small business to focus on becoming a medium-sized business, for example, rather than having to be an IT and security expert.

At the same time, cloud providers have the opportunity to gain the insight from the threats they see on the endpoints of their small business customers, benefiting from the ever-growing network effects of more and more threat data, which in turn can enhance their ability to improve their customers' security. Cloud providers should also be able to leverage their economies of scale to share threat information with their partners in the private and public sectors.

While the move to the cloud has real benefits, small business owners cannot contract out all of their cybersecurity obligations, particularly in the area of strong blocking and tackling—making sure that passwords are updated on a regular basis and backing up information on a regular basis.

Improve DHS's Automated Indicator Sharing (AIS) Program

While the AIS program is still in the startup phase and needs to broaden the type of information it receives and shares, we should not give up on its potential. Policymakers need to enable the administration to move beyond simple indicators supplied via AIS and provides a means to enrich the effectiveness of shared information. The administration should increase its efforts with the private sector to further evolve the way cyber threat information is represented, enriched and distributed in a timely fashion. Dong so will help create a high-functioning ecosystem of information sharing that will help all organizations, both large and small, to compete with global networks of sophisticated hackers.

Encourage Cyber Insurance for Small Businesses

Small businesses would also benefit from cyber insurance, which is specifically designed to protect an organization from risk. This is still a small but growing part of the insurance market. It deserves more attention, as does the idea of having the government act as a reinsurer for the cybersecurity insurance market during its early stages. Alternatively, the government could establish a program similar to the National Flood Insurance Program to help support the private market in the event of catastrophic, widespread attacks.

Invest in Fighting Cyber Crime

The government should also devote additional resources to fighting cybercrime. Too often, it is small businesses in sectors like health care and finance that are being hacked by cyber criminals. These criminals are perfecting the art of ransomeware, and small businesses are all too often being forced to pay to protect their data. Law enforcement at all levels—federal, state and local—need to have the resources to identify and take down hackers who have been terrorizing the small business community.

**CONCLUSION**

It's important to recognize that technical information sharing is only one piece of the puzzle. Small businesses need, first of all, to get the basics of cybersecurity right. Information sharing efforts designed to educate and raise awareness are more important—at least at this point—than those intended to share automated, actionable indicators of threats. Small businesses can benefit greatly from moving their infrastructure and security to the cloud and the economies of scale of ISAOs dedicated to their unique requirements. Cyber insurance also holds promise, as does doubling down on investments to fight cybercrime. We also need to support efforts to boost the effectiveness of the Automated Indicator Sharing program to ensure that everyone wins over time.

Thank you for giving McAfee the opportunity to testify on this important topic. I'm be happy to answer any questions.

○