

PROTECTING SMALL BUSINESSES AGAINST EMERGING AND COMPLEX CYBER-ATTACKS

HEARING

BEFORE THE
SUBCOMMITTEE ON HEALTH AND TECHNOLOGY
OF THE
COMMITTEE ON SMALL BUSINESS
UNITED STATES
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

HEARING HELD
MARCH 21, 2013



Small Business Committee Document Number 113-008
Available via the GPO Website: www.fdsys.gov

U.S. GOVERNMENT PRINTING OFFICE

80-172

WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing 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

SAM GRAVES, Missouri, *Chairman*
STEVE CHABOT, Ohio
STEVE KING, Iowa
MIKE COFFMAN, Colorado
BLAINE LUTKEMER, Missouri
MICK MULVANEY, South Carolina
SCOTT TIPTON, Colorado
JAIME HERRERA BEUTLER, Washington
RICHARD HANNA, New York
TIM HUELSKAMP, Kansas
DAVID SCHWEIKERT, Arizona
KERRY BENTIVOLIO, Michigan
CHRIS COLLINS, New York
TOM RICE, South Carolina
NYDIA VELÁZQUEZ, New York, *Ranking Member*
KURT SCHRADER, Oregon
YVETTE CLARKE, New York
JUDY CHU, California
JANICE HAHN, California
DONALD PAYNE, JR., New Jersey
GRACE MENG, New York
BRAD SCHNEIDER, Illinois
RON BARBER, Arizona
ANN McLANE KUSTER, New Hampshire
PATRICK MURPHY, Florida

LORI SALLEY, *Staff Director*
PAUL SASS, *Deputy Staff Director*
BARRY PINELES, *Chief Counsel*
MICHAEL DAY, *Minority Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Hon. Chris Collins	1
Hon. Janice Hahn	2

WITNESSES

William H. Weber, Senior Vice President, General Counsel, Cbeyond, Atlanta, GA, on behalf of COMPTEL	4
Justin Freeman, Corporate Counsel, Rackspace, San Antonio, TX, on behalf of the Application Developers Alliance	6
Dan Shapero, Founder, KlikCloud, on behalf of CompTIA	8
Phyllis A. Schneck, Ph.D., Chief Technology Officer Public Sector, McAfee, Inc., Reston, VA	9

APPENDIX

Prepared Statements:	
William H. Weber, Senior Vice President, General Counsel, Cbeyond, Atlanta, GA, on behalf of COMPTEL	17
Justin Freeman, Corporate Counsel, Rackspace, San Antonio, TX, on behalf of the Application Developers Alliance	24
Dan Shapero, Founder, KlikCloud, on behalf of CompTIA	43
Phyllis A. Schneck, Ph.D., Chief Technology Officer Public Sector, McAfee, Inc., Reston, VA	49
Questions for the Record:	
None.	
Answers for the Record:	
None.	
Additional Material for the Record:	
NTCA - The Rural Broadband Association	57
NAFCU - National Association of Federal Credit Unions	59

PROTECTING SMALL BUSINESSES AGAINST EMERGING AND COMPLEX CYBER-ATTACKS

Thursday, March 21, 2013

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
SUBCOMMITTEE ON HEALTH AND TECHNOLOGY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:00 a.m., in Room 2360, Rayburn House Office Building. Hon. Chris Collins [chairman of the subcommittee] presiding.

Present: Representatives Collins, Luetkemeyer, Hahn and Schrader.

Chairman COLLINS. Good morning. The hearing will come to order.

We are going to have votes called sometime in the next—between the next five minutes and the next 30 minutes, at which point we will have to adjourn for maybe a half an hour and then we will come back, but just to put everyone on notice. We are not too sure; it could be as early as 10:05 and as late as 10:30 that we are going to be voting on the budget today.

I want to welcome our new members to the Subcommittee, especially Ranking Member Hahn. I look forward to working with you and all of our members during the 113th Congress. I also want to give special thanks to our panel of witnesses for taking time away from your full-time jobs and making the trip to Washington for this important hearing, and I certainly also want to welcome the high school students today who are seeing how democracy works. Welcome.

Our nation's digital infrastructure has become an essential component of how small businesses operate and compete in the 21st century. It provides access to a variety of innovative tools and resources to help reduce costs and increase productivity. E-mail, social media, online sales, and global video conferencing are just a few of the examples. New innovations and capabilities are being developed every day as a result of the Internet, and this means new jobs for Main Street America, new tools for small business. The rapid development in information technology is truly fascinating to watch. A couple of the most dynamic industries that have emerged are cloud computing and mobile applications. It is now easier than ever for small businesses to store and access their information from anywhere in the world without purchasing thousands of dollars in IT equipment. In addition, the boom in mobile applications is a great success story for both entrepreneurs looking to create the next best app and for small businesses that use them. From mobile banking to online marketing there is a plethora of applications available to help small business firms increase produc-

tivity. In considering the NCAA tournaments set to tip off any minute now, I am sure there may be some even in this room who may stream the games from an application on their mobile device.

Unfortunately, the growth of information technology has also attracted a growing number of cyber criminals looking to steal sensitive information, including intellectual property and personal financial information. These attacks can be catastrophic, leaving many small businesses unable to recover. A recent report shows that nearly 60 percent of small businesses will close within six months of a cyber-attack. The recent string of cyber-attacks on high profile companies is a stark reminder of the current threat, and although small businesses do not make the headlines, a recent report shows that 20 percent of cyber-attacks are on small firms with less than 250 employees. Small businesses generally have fewer resources available to monitor and combat cyber threats, making them easy targets for expert criminals. In addition, many of these firms have a false sense of security, and they believe they are immune from a possible cyber-attack. The same report shows that 77 percent of small firms believe they are safe from a cyber-attack, even though 87 percent of those firms do not have a written security policy in place.

There is clearly a gap in education and resources. Moreover, the sophistication and scope of these attacks continues to grow at a rapid pace. A report by the Office of National Counterintelligence Executive indicated that tens of billions of dollars in trade secrets, intellectual property, and technology are being stolen each year by foreign nations like China and Russia. These are not rogue hackers. They are foreign governments engaged in complex cyber espionage with a mission to steal our trade secrets and intellectual property. As the leader in producing intellectual property, the United States and small businesses will continue to be a primary target for cyber criminals seeking an economic advantage.

Protecting our digital infrastructure is complex and no one federal agency or private business can do it alone. It takes a true public-private partnership to identify, combat, and share information regarding the sophisticated cyber-attacks. As we consider new cyber legislation, we must work to identify the correct balance between imposing new onerous regulations for small business and protecting proprietary information and our digital infrastructure.

Again, I want to thank our witnesses for participating today. I look forward to hearing how we can better assist small businesses in utilizing new technologies while protecting them against cyber-attacks. I will now yield to Ranking Member Hahn for her opening statement.

Ms. HAHN. Thank you, Chairman Collins. I am proud to be serving as a ranking member of this Subcommittee, and I know that there is a lot of work that we can do together to empower our small businesses to put technology to work for them and to help them access all the resources that are available to them to strengthen their businesses hire, and grow. And of course, while the Internet and new information technology offers tremendous possibilities for our small business, as you said, it exposes them to cyber threats that can be particularly difficult for them to counter. Developing new innovations is fundamental to our prosperity in the 21st century, but

even more essential is enabling the nation's small firms to adopt these new technologies and become even more successful and efficient. Over the next decade, we can expect the growth of this field to produce good-paying jobs for millions of Americans. The number of jobs dependent on technology is expected to grow, creating opportunities for large and small companies in every sector of the U.S. economy.

Internet and telecommunication technologies have not only changed how we communicate, but also how business is conducted. America's 23 million small businesses are some of the savviest users of technology by using the Internet to access new markets to grow and diversify. In fact, small businesses are the driving forces behind further technological innovation as they produce about 13 times more patents per employee than other businesses. For the established small business, modern technology can expand a firm's client base using a company website, social networking, or other forms of online advertising. Firms can utilize voice and video communication as a low cost method to connect with customers around the world and reach previously untapped markets. They can store data online, access office productivity tools, and even improve the energy efficiency of their business.

Yet for all the benefits technology brings to the equation, it also creates more challenges for small business owners, consumers, developers, and vendors. One such challenge is cybersecurity because being connected also means being exposed to new threats. Cyber threats can come in many forms but they are all devastating to both business owners and their customers. A single attack can wipe out a small business, which is why cyber crime poses severe problems for small businesses that are not prepared to mitigate this kind of risk. According to studies, 40 percent of all threats are focused on firms with less than 500 employees and reveal that a total of nearly \$86 billion is lost with companies incurring an average of \$188,000 in losses. Sadly, some small companies fail to recognize the benefit of cybersecurity as an investment until it is too late. On the other hand, those firms that understand the importance of such an investment often lack the resources to implement an effective security system.

The testimony we hear today will not only highlight the variety of opportunities created by new technology but it will also help to better protect the nation's small businesses from growing cyber threat. This Congress, the strengths and weaknesses of comprehensive cybersecurity, including issues of privacy and notification, will once again receive significant consideration. Small businesses have much at stake in how this debate plays out. It is my hope that today's discussion will shed light on what these policies mean for online entrepreneurship.

In advance of the testimony I want to thank all of the witnesses for their participation and insights into this important topic. Thank you, Mr. Chairman, and I yield back my time.

Chairman COLLINS. Thank you. Before we get started and hear testimony from our four witnesses I would like to take a moment and explain the timing lights for everyone. You each have five minutes to deliver your testimony. The light will start out as green. When there is one minute remaining, the light will turn yellow,

and finally, it will turn red at the end of your five minutes. And if we can stick to that time limit we would certainly appreciate that.

Our first witness is Mr. William Weber. Bill is the senior vice president and general counsel for Cbeyond in Atlanta, Georgia. Cbeyond is a communications service company that provides specialized services, including Internet and cloud computing exclusively to the small businesses nationwide. Bill received his B.A. from the U.S. Naval Academy and his J.D. from the University of Georgia. He spent 12 years in the Marine Corps. Thank you for your service. He is testifying on behalf of COMPTEL, that is a trade organization. Thank you and welcome. You have five minutes to present your testimony.

STATEMENTS OF WILLIAM WEBER, GENERAL COUNSEL, CBeyond, INC., TESTIFYING ON BEHALF OF COMPTEL; JUSTIN FREEMAN, CORPORATE COUNSEL, RACKSPACE, TESTIFYING ON BEHALF OF THE APPLICATION DEVELOPERS ALLIANCE; DAN SHAPERO, FOUNDER, CLIKLOUD, TESTIFYING ON BEHALF OF COMPTIA; PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR, MCAFEE, INC.

STATEMENTS OF WILLIAM WEBER

Mr. WEBER. Mr. Chairman, Ranking Member Hahn, Distinguished Members, thanks very much for the opportunity to speak with you today about what is an incredibly important issue for small businesses across the United States.

My company, Cbeyond, represents 60,000 small businesses and that is the only group of companies that we represent. We do not represent large enterprises or microbusinesses. So we have a lot of experience in dealing with the kinds of security issues that they face. But I wanted to start out today to talk to you a little bit about cloud services, what they really are, and how they are being used by small businesses today because it is easy to get confused about what kind of cloud services small businesses are utilizing.

When people talk about cloud services, there are three kinds that they will talk about. Software is a service, and there are a lot of consumer-focused cloud services. Technically, software is a service. Netflix is a one. Facebook is another. Small businesses tend to use software as a service provider such as Salesforce.com to help run their sales force.

You also have platform as a service, which is much more complex. Small businesses tend not to use it. It is kind of an operating system in the cloud. And then the people that we have here talking today are primarily going to be discussing infrastructure as a service. When you hear people in the cloud industry talk about infrastructure as a service, what we mean is taking things that in the past were physically located on a business's premises and moving them off the premises somewhere. And I think giving you a concrete example of a business that might do this would be helpful.

Let us take a typical small business that we might serve, like a doctor's office. They have got three physicians working. They have got staff people, 10 PCs, and they very likely have a server on their

premises. When we say a server, it is just simply a computer that does not necessarily have a monitor hooked up to it but that the other doctors and administrative staff could access their billing software on that server that would be located on their premises. And that would be connected into their premises network via Ethernet cables like you see all over the place. There is a green one right here. You probably have some in the desk in front of you.

When we talk about infrastructure as a service, what we are really talking about is taking that server and if you can imagine extending that Ethernet cable 250 miles into a data center, and now instead of sitting on the premises, that server, with all their billing software on it, customer records on it, is sitting in a data center. And instead of having to buy that as a capital expenditure for the company, that server is rented from a company like mine, Cbeyond or Rackspace or any of the other companies that provide servers in the cloud.

Now, what are the advantages of doing that? Well, some of the advantages are the small business can preserve capital. Instead of having to do a \$2,000 or \$3,000 outlay to buy that server they can rent it by the month from us. Physically, it is much more secure. It is in a datacenter that has all the most up-to-date firefighting equipment and power backups and everything you can imagine to protect it physically. So those are two of the major advantages they get. Do they get security advantages? They do get security advantages because we can move not only servers off their premises, we can move firewall devices off their premises and they can rent those from us. We can move storage devices off their premises and they can rent those from us. So from a security perspective, rather than being responsible for maintaining the cybersecurity that server themselves, which they are not professionals doing—they want to run a doctor's office and that is what they are professional at—they shift that burden to the cloud provider, and we are experts in that—maintaining the firewalls, maintaining the operating system, making sure virus software is kept up-to-date and doing all those things for them. So it sounds like a complex thing but if you do think about it as simply moving that server that is on your premises into the cloud and letting people who do nothing for their job but think about security for those things maintain it, it can be of tremendous value to small business. Thank you.

Chairman COLLINS. I think we can do one more witness and the two of us will jog down to the floor to vote.

Thank you, Mr. Weber. I think that was a good explanation of what cloud computing is all about. Maybe we can have some questions on that later.

Our next witness is Mr. Justin Freeman, corporate counsel for Rackspace. Rackspace is a global leader in providing cloud computing services for all types of businesses, including mobile applications for small firms. Justin has expertise in both the legal and technical areas of the rapidly expanding field of cloud computing law. In his role he oversees complex technical agreements and directs their public policy strategy. He received his J.D. from Southern Methodist University and is a certified information privacy professional. He is testifying on behalf of the Application Developers

Alliance. Thank you for being here. We look forward to your testimony.

STATEMENT OF JUSTIN FREEMAN

Mr. FREEMAN. Thank you, Chairman Collins and Ranking Member Hahn and the rest of the Committee members.

On behalf of both myself and Rackspace and the Application Developers Alliance, thank you for your time today and for this opportunity to discuss contemporary cybersecurity challenges, which are all the more difficult for our small business community to address.

I would like to begin by providing a little bit of background on Rackspace hosting founded in 1998 and headquartered in San Antonio. With our focus on fanatical support, which is a fierce commitment to a customer-oriented set of core values, we have grown rapidly and currently serve more than 170,000 customers across 120 countries. Rackspace focuses on providing the cloud infrastructure and support technologies, which enable businesses both large and small—especially small these days—to benefit from the cost savings that cloud computing provides.

Our latest focus is on open stack, an open source cloud platform which we jointly developed with NASA. Open cloud technologies are at the forefront of this information technology revolution. They make previously inaccessible technology available to businesses, small and large alike, without initial investment in research and development costs, and they eliminate proprietary lock-in which helps foster industry standards for cloud computing providers and it is a critical first step in allowing users to move their applications and data from provider to provider as they see fit.

There is no doubt that small businesses face growing cyber-threats, especially in the form of intellectual property theft and business disruption, such as what happens when a small business's website is knocked off the Internet by a denial of service attack. It is more important than ever for small businesses leveraging new technologies to provide innovative services and solutions to ensure that they have a trusted provider ecosystem on which they can rely.

Rackspace has increasingly supported small businesses via start-up programs which provide free or discounted cloud resources to new enterprises. This helps remove some of the initial roadblocks to success. The mobile application space is particularly explosive with small business-led innovation as entrepreneurs are able to leverage diverse and powerful cloud computing resources to deliver innovative, integrated, and mobile application experiences to customers, professionals, and enterprises with little or no barrier to entry. And that is really the key point in the application space.

To further support this innovative sector, Rackspace has joined with the Application Developers Alliance, an industry association dedicated to meeting the unique needs of application developers as creators, innovators, and entrepreneurs. The Alliance includes more than 20,000 individual application developers and more than 100 companies, investors, and stakeholders, and it strives to deliver essential resources, serve as a collective voice on policy issues for all the small businesses who might not otherwise be able to be present, and act as kind of the connective tissue in the app eco-

system. Rackspace-assisted start-ups have run the spectrum of the mobile app space, including iPad applications to support physicians and information management, literature apps to help book lovers share the reading experience, language learning and test prep apps, and app systems that frankly make it easier to make even more apps.

Turning back to the critical question, what can the federal government do to help protect small businesses from cyber-threats, it is first important to acknowledge that because of a lack of resources to invest in expensive security appliances or with which to maintain a large staff of security professionals, many common prescriptions have limited effectiveness when it comes to protecting the small business environment from cyber threats. That is not to say that these challenges are by any means insurmountable. Policies which focus on education and training can help equip small business professionals with the know-how necessary to respond to cyber threats and economic incentives to implement security appliances can help offset the cost of maintaining a secure infrastructure. It is crucial that privacy and security regulations are implemented in addressable fashion so as to provide a foundation of security principles while allowing businesses to retain the flexibility necessary to remain competitive and innovative.

We must avoid regulating small businesses out of the marketplace by imposing retrospective or overly burdensome requirements to implement security measures which ensure or outright guarantee that no data can be breached. Instead, we should focus on requiring reasonable and appropriate controls to address threats in the context of a competitive business environment, disseminating critical information about current threats and best practices to the small business community, and promoting a coherent set of sector-specific regulations, privacy protections, security requirements, and collaborative commitments. While it may be impossible for any company to guarantee the security of its systems, together we can lay a foundation to keep the American technology sector secure, innovative, and internationally competitive.

Thank you very much for your Committee's time.

Chairman COLLINS. Thank you, Mr. Freeman. We will have to adjourn now for I am thinking about 30 minutes to go cast our votes. You can see what is going on right now, at which point we will be back. Thank you.

[Recess]

Chairman COLLINS. The Committee will now reconvene. Ranking Member Hahn had to catch a flight so I would now like to introduce our third speaker. Dan Shapero is the founder of KlikCloud, a company that provides cloud-based digital marketing services for the IT service channel. As an entrepreneur, Dan has extensive experience growing his own company and helping other SBAs grow their businesses by leveraging cutting edge technologies to gain strategic advantages over larger and better capitalized competitors. He is testifying on behalf of CompTIA.

Welcome. You have five minutes to present your testimony.

STATEMENT OF DAN SHAPERO

Mr. SHAPERO. Good morning, Chairman Collins, Ranking Member Hahn, and Distinguished Members of the House Subcommittee on Health and Technology. I would like to thank you for holding this important hearing. This testimony is submitted on behalf of the Computing Technology Industry Association (CompTIA).

My name is Dan Shapero. I am a CompTIA member and founder of KlikCloud, a company I launched in 2010 focusing on offering a variety of IT services, such as digital marketing, website hosting, search engine optimization, blogging, e-mail newsletters, and other business advisory services.

I am a California native and I am a graduate of the University of California in San Diego. Prior to KlikCloud I spent over 20 years working in the IT sector in various capacities. I have also launched or helped other entrepreneurs launch several IT startups. My past clients include Vicinity, which is now Microsoft Maps, and Avamar, which is now part of EMC.

My colleague on the panel will share with you some more technical details of cybersecurity threats and attacks prevailing on our Internet ecosystem. I hope to contribute to the discussion by sharing with you my perspective from an IT small business owner. I can assure you that cybersecurity is one of the most pressing issues facing the small business sector, but first I would like to provide you a quick overview on CompTIA.

CompTIA is a nonprofit trade association and its members include thousands of small computer service businesses, as well as nearly every major computer hardware manufacturer, software publisher, and service provider. In addition, CompTIA is also the leading global provider of IT workforce vendor-neutral certification and there are over 1.4 million CompTIA IT vendor-neutral certification holders worldwide. Many of those are for IT security.

As a baseline, the IT security infrastructure for small business is as vulnerable to cyber-attacks and threats as large companies and firms. Unfortunately, small businesses are less resilient than their larger counterparts because they have fewer IT resources in terms of personnel, hardware and software to combat the onslaught of cyber threats and attacks that many SMBs encounter on a daily basis.

Some small businesses are comprised of as few as 5 to 20 employees, so resources come at a premium. As a small business owner, I have to rely on my own expertise to implement adequate measures to ensure that the IT infrastructure that supports my business is secure. I also have to make sure that my clients understand cybersecurity risks and the threats to their business. I advise them on the types of cybersecurity compliance measures that they must implement to keep their IT systems secure.

In the last five years, we have seen a steady transition from a server environment to a cloud-based environment. This has created tremendous opportunity for the small business sector. The emergence of cloud technologies is now allowing small businesses affordable access to IT infrastructure, including software that was financially beyond reach just a few years ago, so it is even more critical now that we ensure that adequate measures and controls are in

place to protect small businesses from cybersecurity threats and attacks.

I would like to highlight two policy issues. First, the majority of cyber-attacks create exposure across state lines. This is the reason that data breaches are of serious concern. There are 47 different state data breach notification laws in place. In addition to the legal and regulatory compliance costs, there is also an impact of loss of revenue and loss of reputation that can be overwhelming to most small businesses. CompTIA believes that the creation of a national framework for data breach notification can go a long way toward reducing costs and eliminating barriers to entry for small business firms and it will also serve as an incentive towards job growth in the small business sector.

Another issue that we face as small to medium businesses is the ability to recruit and retain in-house talent to help protect ourselves from cyber-attacks. All of our employees have responsibility in keeping us secure, especially those in IT-related roles. However, there is a skills gap that is an issue that is affecting our IT community as a whole. There are approximately 250,000 open IT jobs in the U.S. at any given time. IT training and certification is not a magic bullet; however, it is a critical part of the solution.

In closing, I would like to thank you again for the opportunity to share our perspective on the issue of cybersecurity and would be happy to answer any questions.

Chairman COLLINS. Thank you, Mr. Shapero.

Our final witness is Dr. Phyllis Schneck. She is the vice president and chief technology officer for McAfee and has certainly testified before this Committee a year or so ago. Dr. Schneck received her Ph.D. in Computer Science from Georgia Tech University where she specialized in the field of information security. In addition to her role at McAfee, she serves as the chairman of the board of directors of the National Cyber Forensics and Training Alliance, a public-private partnership used to prosecute cybercriminals worldwide.

Welcome back to the Committee. You have five minutes to present your testimony.

STATEMENT OF PHYLLIS SCHNECK

Ms. SCHNECK. Thank you. And good morning, Chairman Collins and other members of the Subcommittee.

I am Phyllis Schneck, vice president and chief technology officer for Global Public Sector for McAfee. I really appreciate the Subcommittee's interest in this topic of cybersecurity for small business. I am pleased to address the Subcommittee once again.

My testimony will focus on four key areas. The threat landscape and its implications for small business, what in general can we do about that for small business, what are the mitigations, and then what is it that the private sector and the public sector and government can do to address this.

A bit of background. I come from the high performance computing world. Balancing how you take hardware design, software design, and get a CPU to do everything it can do for cryptography. So it is a balance of strong security and strong computing. I also had a startup of my own and understand some of the challenges

in having a small business and was one of the founding designers of our Global Threat Intelligence at McAfee, which enables us as a large company to see 160 million points of light of where bad things may be happening across the Internet and create a weather map that protects everyone else. And as you mentioned, I do run the National Cyber Forensics Training Alliance, and the passion there is the information sharing and collaboration which we need desperately to get to the small businesses so that they, too, can benefit from that even though they may not have the time or the money or the resources to participate in that themselves.

At McAfee, we are relentless. We are dedicated to providing connected security ecosystems that benefit small business, large business, government all over the world but that make sure that every part of the security ecosystem is learning as it protects and as a wholly-owned subsidiary of the Intel Corporation, we go all the way to the hardware and we are able to look at the actual pieces and parts and metal and silicon that run the instructions and make sure that we can detect adversary behavior and protect.

Small to medium businesses make up 99.7 percent of our business fabric. They hold intellectual property, personal information. Many times they are the contractors building the next engines, yet they cannot afford strong security teams and they cannot afford separate resources which is why my colleagues and others today provide amazing services to them so they do not have to buy the equipment; they have the services. What I will address today is how we can help those small businesses that leverage so much on cloud and mobility and also help, as Ranking Member Hahn pointed out, 23 million small businesses. How we help them also gain the information sharing and collaboration that the larger businesses are getting the benefit of right now.

On the mobile space, that has increased from what we have seen 70 percent in the past year. We went from 792 samples in our malware zoo as we call it to 37,000, and 95 percent of that increase was in 2012. Small business leverages these mobile devices because they are inexpensive in many cases. They are easy. They can do their home transactions, their work transactions all at once. They take them on the road and they leverage it with cloud services because there is very little computing resource on the small device so they can outsource the data storage. The threats to this and mobility, we see those threats of the adversary trying to access that device to get your personal information and/or access your computer network, so the small business that cannot afford necessarily a team to watch this has an even stronger vulnerability because they have so much of their infrastructure dependent on mobile.

On the cloud side, you are basically outsourcing the processing and storage of your data. So the key there is to watch the data in motion and at rest. When you plug in that Ethernet cable or a quote or send our data somewhere else, you need to make sure they are encrypted and protected. You need to make sure that that cloud provider has forensics for you when you do want to report a breach and you do want to share information. Some cloud providers will charge extra to do that forensics investigation, so we would ask to look at that to make sure that the best security on the planet is affordable for the biggest business sector on the planet.

When we start looking at what we can do as private sector, focus on security. Cybersecurity is a boardroom risk issue even in the smallest businesses. Design and invest in cybersecurity upfront. Mobile devices can be managed. That policy can be pushed from the boardroom to every phone and every table. It can be pushed to how you categorize what data is outsourced to the cloud and what data perhaps is not.

On the government side, we need to incentivize cybersecurity, incentivize innovation, ensure that small business has the protection that big business has, ensure that small business is not forced into the heavy regulatory compliance side and moreover can do their real business and build the next engines and the next drugs.

On the information sharing side, the Rogers-Ruppersberger bill, it would be a wonderful way to encourage information sharing between the largest companies and the smallest so that you get that 99 percent of the business fabric to be able to contribute what they see in the situational awareness and let them have access to what we see as big business. Currently, the ISACs are not affordable for most small businesses, the Information Sharing and Analysis Centers that are set up with government and private sector. We need to level that playing field and get all that information and all of that security protection, all that safety into our small business infrastructure.

Thank you very much, and I look forward to any questions.

Chairman COLLINS. I want to thank all the panel members. One reason we are having the meeting is to shine a light on the fact that 77 percent of small businesses are not even considering this. They are coming to work every day to make a sale, to have some cash in the bank, pay their bills. It is not on their radar. We want to put it on their radar.

So I guess I will start with the basic question that each of you could address, which is a small businessman comes in unsure if it is malware and it is the old-fashioned, somebody just trying to wreak havoc with his system. You will know it because your system will not turn on and funny things will show up. But today what we are worried about is they are going to steal intellectual property. They are going to steal personal information. How does the small business owner that this is not on his radar even know he was hacked? How would he come in and know someone snuck in a back door and stole that information? Or would he not know?

Mr. WEBER. Mr. Chairman, I am going to do something that you almost never see a witness do. I am going to stop talking immediately because I am not an expert on these things and we have incredible experts on exactly the sort of systems that can detect an intrusion so that you would know about it.

Mr. FREEMAN. I will address a couple of points about that question. The first is that most small businesses that are hacked have no idea that they have been hacked. Most large companies that have been hacked also have no idea that they have been hacked. This is especially applicable to corporate espionage and the theft of intellectual property. Outside of the case of business disruption attacks where you know you have been hacked because your website does not function anymore, the theft on the data breach side is much more difficult to spot. So if you start looking to solve the

problem after a breach has occurred you are way too late. And I absolutely agree with your remarks that this has to be on the radar well in advance. Intrusion has to be detected in order for it to be responded to. And a number of the products from our other witnesses here can help businesses with intrusion detection and analysis but the fundamental answer is that security has to be part of that conversation. As Dr. Schneck put it, it has to be part of the boardroom conversation well in advance. We have to integrate security into our fundamental planning of all types of business development processes. Thank you.

Mr. SHAPERO. I concur with Mr. Freeman. Chances are the small business owner does not really know. Now, if they are relying on cloud infrastructure, it may be incumbent on the cloud provider to notify them if there is a data breach or a data leak which may be conceived as a benefit of having your assets in the cloud. But more often than not, if it was just on their own network within their premises, chances are it went undetected.

Ms. SCHNECK. I will concur, and I will say pretty much everybody is owned, meaning there is a visitor most likely everywhere on every network. The idea is to be able to run well under attack. The trick here is resilience. How is this event—because it will happen—it is just like the human body. You will get a cold but it will not kill you. So how is it that networks keep running? How do we build in resilience? It goes to the boardroom policy issue and it also goes to making your network, no matter how small or large it is, making your network smarter. There are a lot of shiny products out there. We all have them. But making sure when you invest in those shiny products they click together and they talk to each other and they make your network smarter, like an ecosystem. So if part of your body spots a germ, your body attacks it without having a meeting to do it. This is how we build our networks now. This is that connected philosophy. And one of the best things we can do is enable. Part of what we do, first of all at McAfee, is take our global threat picture and apply it to every small point that we protect. But as a community, we can take everybody's global picture, connect it, and protect even the smallest of businesses. So the detection of the intrusion will be earlier, but also the resilience to it will be a lot stronger. You will know how to recover from that. You will probably lose less. A very tactical example is the way intellectual property is "lost" is the access is gained by an intruder that knows how to execute their instruction next on your computer's list so they have control. They look for what they want and they make a copy of it. They copy it and they make a web connection and they send it back to a server that is waiting for it. We can spot that stuff. It is not even expensive. The idea is to know what you are looking for and it is not static. Know what you are looking for based on what the rest of the world is seeing right now, and a lot of that comes from information that would be shared to and from cloud providers.

Chairman COLLINS. Thank you. I mean, again, our concern is it is one thing to say we should address this at the board level and we should, but that starts with an owner who thinks he is vulnerable. Seventy-seven percent of small business owners do not think they are vulnerable. They are. We know it and we just need to

heighten that. So, again, from this Committee, if we said what are the top three things we should as a Committee focus on or explain to small business, besides going in the cloud, right? Number one, go to the cloud. But what are the first three things that we could do to try to highlight this? Or what would you recommend a small business do?

Mr. WEBER. Mr. Chairman, if I was going to make one recommendation, the thing that hurts our customers more than anything else is using poor passwords. It sounds so basic. You would think that today in 2013 that people would know what they ought to be doing but they do not. They are very dumb about password selection. So today a secure password ought to be at least 12 digits long. It ought to have capital letters, it ought to have lower case letters, and it ought to have a number or two in it. A password like that is not going to be cracked. But small businesses do not want to do that because it feels inconvenient. There are all kind of techniques you can use for generating these passwords and make them easy to remember.

I will give you just one example of a problem that we had with this. Our company has a website called Cbeyond Online where you can go to modify your services, whether it is cloud servers or your phone services. And we had a large law firm in Atlanta with 90 attorneys who use our service, and one of the attorneys who had access to Cbeyond online had a very, very weak password. It was the name of his college mascot and they got hacked. And the hackers came in and, forwarded the firm's main telephone number to their cell phone. They then went to the firm's bank and deposited checks in their name worth \$40,000. The bank called the law firm to verify. We had not seen this vendor before. We want to make sure that we should release these funds. Of course, their phones were forwarded so it rang to the criminal cell phones. They said, "Absolutely. This is a top shelf vendor of ours. Please release those funds." And they lost \$40,000 that way, just because of a weak password.

So if I were going to focus on one thing, the first line of defense is strong passwords. And if every small business in the United States started using appropriate passwords it would have a very significant impact on cyber crime.

Chairman COLLINS. Thank you.

Mr. FREEMAN. To carry on the notion that passwords are a first line of defense, I would just like to also emphasize it is critical to maintain a variance of passwords. At Rackspace, the number one threat we see to customers are when their systems are compromised because a malicious third party has garnered a list of passwords from another service. When you reuse the same password on your Evernote account as your Gmail account and someone is able to hack one or the other, they get a list of the passwords and they are able to use that against all of your infrastructure. And routinely third parties will go out and simply bang against every provider available to see if the same user name and password combination exist.

In combination with that, another practical approach is that business need to utilize encryption of all sensitive data, both economically sensitive and regulated data. Encryption really is the

only means that has the fundamental integrity with which to protect data. Because systems will be compromised because we cannot guarantee that an intruder will not get access to a system, the only thing we can do is really secure the data that they might get access to, and encryption is far and beyond the gold standard when it comes to that type of security.

From sort of the broader approach, I agree with you there is sort of a chicken and egg problem. How do we have the security conversation when no one is having the security conversation? I think it is critical to look at policies that promote the conversation amongst users, businesses, and then the businesses' providers. So the providers consider it just part of doing business when they go and enter, whether it is with a cloud service provider or security provider or with another vendor, that security of information is simply integrated into that conversation and becomes part of the ordinary course of business.

One possibility in order to incentivize that is to incentivize economically the use of security resources rather than to attempt to incentivize it through punitive regulations. I think that small businesses in particular are going to be much more responsive to economic incentives rather than to changing their behavior out of fear of punitive regulations, which often they do not have time to review in their mass and complexity. Thank you.

Mr. SHAPERO. Well, first I would like to acknowledge the Committee for starting the dialogue. You asked what could the Committee focus on, exactly right, and it is great to know that small business is part of that dialogue—small businesses and their customers, frankly—and I urge you to continue on with the debate. For the business owners themselves I start off tip number one advice is make sure that your network is compliant. And when I say compliant, you do not just have anti-virus, anti-malware software, a firewall in place, but you are making sure that all your definitions are up-to-date, meaning that you are up-to-date on what the latest threats are. That your firmware on your firewall is up-to-date so that you have got the latest and greatest to protect yourself from those threats. And also your operating systems. So all those patches that come out on a regular basis. They might seem like a nuisance to many small business owners and it may be a basic thing like passwords, but make sure that you are applying them as recommended by your IT service provider. Encrypting your data is also an important part of ensuring that you have a compliant network. Doing a periodic network scan is something that you should do as part of making sure that you have a compliant network. So there is a whole list of checklists to make sure your network is compliant.

The next thing is policies. So you pointed out most companies do not have a written policy for their employees. It might be something like acceptance use for mobile devices in their organization. Am I allowed to have corporate data on my personal device? Am I allowed to have personal data on my corporate device? Because it can get really tricky when a device might be lost or stolen and you are trying to lock down that data if you do not have those policies in place. Policies for what to do in case of a breach. Who do I notify? Which of those 47 states am I required to disclose to when

I have lost data from my consumers? So having those policies in place is really important.

And then I actually have four on my list so I will cut the last one off. The third is training. So it is really an educational process, not only for the business owner but for their staff as well so the employees understand the importance of why they cannot just have that 12 digit alpha numeric with caps and character password, but why it is important not to paste it on a post-it and stick it on your cubicle because you might forget it. So just making sure that you have the employees onboard as well because they really are the first line of defense. And as Mr. Weber pointed out, might be the ones taking that phone call, giving out or leaking out data in the organization. So it is really important that we raise the level of education of the business owners and their employees.

Ms. SCHNECK. So I will echo. A lot of these comments are right on. This is not just a technology problem; this is a people problem. So a lot of emphasis on the training and education. When you incorporate a new business there are a lot of steps that people know they need to go through and not one of them is cybersecurity. So that is an afterthought completely, so already you start off behind. Many small businesses are harboring some of the neatest inventions for the next decades. They do not necessarily think about where they store stuff or categorize those assets and how you protect it. So it is very much a legal and policy challenge.

As a "security vendor" I will say something potentially funny but anti-virus is not so much the way of the future; it is all the other things that were mentioned. But it is not having one of each; it is taking a step back and making a plan that fits that company, one that fits that budget, and that can get done when a company is incentivized to take a really good nontechnology look at the cybersecurity they need. What are my assets? What are my risks? I absolutely will have an intrusion. And then how do you bounce back from that and how do you create a culture of security, a culture of resiliency? And the modern maturity models that we see show that a good upfront investment in cybersecurity—and it does not mean an expensive one, it means a smart one, an educated one—is the upfront investment. And over time you actually spend less money and get more resilience because that connected security system is learning. Anyone can protect against an attack we know about. What we get hurt by as a community are the attacks that we have never seen before, and those are very well crafted because our enemies are innovating. So the only counter to that is innovation itself. And what I would ask for and suggest is something like tax breaks or insurance breaks. Those things are very attractive to new businesses. So when you stand up that new business, what are the things I can do to save the most money and be the most secure that look good to the three people that work for me or to the venture capitalist that put his money into me? And I think so from the training perspective, the people perspective, and overall holistic risk perspective. Then you can start adding all these wonderful technologies that we all have.

Chairman COLLINS. Well, thank you. I want to thank all the members for participating because I just think this is a step in the direction for the Small Business Committee on an awareness front

and I think also interfacing with the SBA. I think just saying to someone who calls up and says I am creating a business, making sure that the issue of cybersecurity and the importance of it is on the checklist. I mean, let us just for one thing get it on the checklist. So I think there is a lot we can do just shining a spotlight and we have done some of that today. We intend to do more. We are going to make sure that at the end of this meeting that we do send a letter to some of the key federal agencies and summarize the findings here. We will also be talking in a broader perspective with some of the news media about cybersecurity, and we are going to ask the federal agencies to come back to us and detail what they are doing to deal with the issue of cybersecurity, the importance, and especially as we said today, small companies do not even know they just lost their strategic plan, they just lost their bank statement, they just lost a list of all their employees and their employees' social security numbers, their strategic plan. I mean, if you could imagine setting them in the lobby for someone to copy, to some extent that is what they are open to. So we are just going to step forward and make sure that small business understands the risk. It is real. It is more severe today than it was 10 years ago, and so your testimony today is helpful, and certainly your list of suggestions. We will make sure that we include that. They were very common sense and in many cases not that expensive.

So I will ask unanimous consent from the members. Seeing there is no objection I will so order that. And this meeting is now adjourned. Thank you very much.

[Whereupon, at 11:32 a.m., the Subcommittee was adjourned.]

STATEMENT FOR THE RECORD
WILLIAM WEBER, GENERAL COUNSEL, CBeyond, INC.
BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON SMALL BUSINESS
SUBCOMMITTEE ON HEALTHCARE AND TECHNOLOGY
HEARING ON
PROTECTING SMALL BUSINESSES AGAINST EMERGING AND COMPLEX
CYBER-ATTACKS
MARCH 21, 2013

Mr. Chairman and members of the Subcommittee, Cbeyond appreciates the opportunity to provide a statement for the record for today's hearing. Cbeyond provides cloud and communications services to more than 60,000 small and medium businesses (SMBs) nationwide; in our most established markets including Atlanta, Dallas, Denver and Houston, we provide services to more than 15% of all businesses with between 5 and 250 employees. Our annual revenue is nearly \$500 million, and we have approximately 2000 employees. Last year, Forbes magazine named us one of America's Most Trusted Companies and—together with Kraft Foods and Timberland—we were given the Points of Light Corporate Engagement Award of Excellence.

I hope today to give you a brief overview of what cloud computing is, why it matters to SMBs, the cyber-security threats facing these companies and ways that those threats can be mitigated.

What is Cloud Computing?

Unfortunately, I am old enough to remember the giant computers of the 1960's with their punch cards and putty-colored terminals with ghostly green type. These machines differed from the computers our children grew up with in that their computing power was not in the terminals themselves; the computing power was in a mainframe computer located in another room or another building. This was why you sometimes heard the machines you typed on described as "dumb terminals."

Beginning in the late 70's and moving through the 80's, computing power gradually migrated from the network core to the network edge. This was the rise of the personal computer, and as competition blossomed and prices tumbled, true computing power became available to home and small business users for the first time. This democratization of computing resources remade our economy and fundamentally changed the way many of us work.

As PCs became ever smarter, faster and cheaper, we began to make demands on them that were difficult to achieve without a network. So we built a new kind of network. These new networks were fundamentally different from the old because now the computing power resided primarily at the edges. The networks themselves served to route information (like email) from PC to PC and to store information in central locations that needed to be accessed by many people simultaneously (like databases).

Soon, though, we discovered a need to return some real computing power to the network itself. Let's take a law firm as an example. By the mid-90s, law firms got tired of having to buy the same programs for all their computers, particularly the programs they used to bill their time, store and access important documents and organize their calendars. Software makers responded by creating versions of their software that could reside on a central server connected to individual computers via the Ethernet cables of the law firm network. Now multiple attorneys and assistants could access the same central information, bills could be generated automatically and the vast document databases that made legal work simpler could be shared, searched and accessed by dozens of people simultaneously.

This model worked well, but it had one major drawback: it required the law firm to maintain what amounted to a server farm on their premises and extensive Information Technology (IT) staff to take care of the servers and the internal network. It was also capital intensive because the firm had to purchase enough servers to run their enterprise software applications and back all those applications up. And, of course, they had to buy more resources than they actually needed to account for potential growth and be able to respond immediately to problems with an individual server. For a law firm—as with any other business—downtime would mean lost revenue. And this brings us to what people call “the cloud.”

So what is the cloud? At a high level it is the movement of server-based computing power off the premises and onto servers that users access in a remote location over a private network or, in many instances, over the Internet. You already know about more consumer-focused, cloud-based services than you may think. Netflix's streaming video service is one. Facebook is another. Both these applications store vast amounts of information on remote servers somewhere on the Internet and deliver that information (and the computing power necessary to process it) to you on demand.

Why Do SMBs Care About the Cloud?

Understanding the basics of cloud computing is important, but it is just as important to understand how the businesses in your home districts use the cloud. A few examples might look like this:

- A seventeen-location Los Angeles furniture company sending all of its security footage directly to the cloud where they can store it securely and use server processing power to review and search it.

- A major insurance company with its US headquarters in Minnetonka moving its IT test environment to Amazon servers to avoid the capital costs associated with purchasing dozens of servers it will only need several times a year.
- A mid-size law firm with offices in Atlanta, Charlotte and Louisville moving its billing, time-keeping and accounting software to Cbeyond servers so that all of its offices can access the same data at the same time.
- A group of orthopedic surgeons in Denver moving all its patient records to the cloud to avoid the cost of maintaining the servers necessary to store, search and access x-rays and to ensure it meets its HIPPA obligations.

Why would these businesses want to move these applications and information to off-premise servers? There are many reasons, some of which are embedded in the examples above. First, getting someone else to manage their servers allows an SMB to focus on their business rather than their infrastructure. Lawyers want to practice law, doctors want to practice medicine, real estate agents want to close deals and architects want to design buildings. They don't want to spend time taking care of internal IT resources. Cloud computing allows them to realize this dream.

Second, cloud computing allows companies to preserve capital. Rather than buying servers that they then have to pay to maintain and upgrade, the business can rent only the server capacity it needs for the time it needs it. There are no installation cycles and no need for extra square footage or additional air conditioning or electrical upgrades.

Third, cloud computing is fundamentally more secure in a variety of ways. It is physically more secure because data centers—unlike most places of business—are consciously designed to the highest access security and fire control standards. Business data is also more secure because a server operating in a data center is monitored around the clock and potential failures can often be detected and dealt with before they occur; this kind of monitoring and response simply cannot occur in SMB IT environments. Data in the cloud can be backed up to multiple, geographically diverse locations automatically; if there is a tornado that destroys a data center in Indianapolis, a business can seamlessly and without pause access that data from its duplicate in a Denver data center. Security patches and operating system updates on cloud-based servers are installed the instant they become available. And, finally, servers in a data center are sitting behind the most sophisticated, well-monitored firewalls available, and their anti-virus software is constantly updated with no intervention or action required by the business; it's all part of the service a business buys when it moves its data to the cloud.

Fourth, cloud computing gives a business IT flexibility in that they can grow and shrink their computing resources on-demand, preserving both capital and time. If a business needs to test major software releases under heavy loads a few times a year, it can simply spin up cloud servers, run their tests and then spin them down, saving time, saving money and avoiding the cost of infrastructure it has only occasional need for.

Finally, the cloud allows businesses to increase IT velocity. If an innovator has an idea, it can be put to the test immediately. No more waiting for a server to ship and get installed. This compresses planning cycles, keeps our entrepreneurs focused on innovation rather than the infrastructure of innovation and allows new ideas to launch at the speed of the idea rather than the speed of FedEx.

How Does Cbeyond Help SMBs Take Advantage of Cloud Computing?

If my comments thus far make cloud computing sound like the answer to many of the problems that SMBs confront as they launch or grow, good. Because that's an accurate view: cloud computing helps preserve capital, increases security and makes launching or growing a business both cheaper and faster. But SMBs need help to make the best use of cloud computing, help that can only come from their service providers.

Unlike the large businesses that first began making use of the cloud, SMBs do not have extensive IT resources. They don't know how to move the applications that run their business into the cloud, and they don't know how to migrate the associated data. In fact, they generally don't even know what cloud computing resources they actually need to do whatever it is they want to do.

The large telecommunications and large cloud-only providers do a great job serving enterprise businesses with big IT staffs who know exactly what they need. The giant telecom companies and cable providers also provide high-quality services to the small businesses that need basic services like Internet bandwidth, phones and email. But what about the sophisticated SMB that wants to use the cloud to preserve capital for job creation and innovation? They are in a tough spot: they don't have the IT staff to help them with their migration to the cloud, and the big cloud providers are not set up to help them get QuickBooks and similar enterprise applications up and running in their data center. This is where companies like Cbeyond can help.

Competitive telecommunications providers are the experts in the technology needs of SMBs because it's all we do. We have direct sales people who introduce businesses to the power of the cloud and personnel whose only job is to help businesses choose exactly the resources they need for the job at hand. We innovate to serve our small business customers by creating cloud offerings tailored specifically to their needs, building applications specifically designed to migrate their data and providing the kind of personalized support they need to succeed and to learn how to protect their business-critical data and applications.

What Cyber-Security Threats Face SMBs That Move Computing Resources to the Cloud?

While the move to the cloud can be of tremendous benefit to SMBs from a variety of perspectives, many are concerned about security. And they should be: cyber-security must be a primary concern for any Internet-connected business. The first point that needs

to be made there is that the nature of the cyber-threats facing SMBs as they move into the cloud are not much different from the threats they have always faced if they have a network that is connected to the Internet. They still need to protect their internal networks, protect their data as it is transmitted from one network to another and protect their network endpoints—their individual PCs—from compromise.

Most digital attacks on SMBs enter the business through a network connection to the Internet, and the first line of defense is having systems in place to block these threats from crossing into their private networks from the public Internet. Many SMBs, particularly those with more than one location, have multiple internal networks, and they must also ensure that their data is safe as it moves from one secure network to another. To understand these threats more completely, a good—if somewhat hackneyed—analogy is to a medieval castle.

If you think of an SMB's internal network as its castle, a good firewall and content filter is like its drawbridge and moat, controlling access to the castle and ensuring that only authorized people (packets) are admitted. Firewalls filter data at the protocol level to ensure it is authorized, and content filters search inside the data itself to see if there is any spam or malware hidden inside so that it can be stopped before it penetrates the internal network.

But medieval kings were not only concerned about the wrong people sneaking into their castles; they also had to be concerned with threats from afar, and—like guards stationed along the walls and towers of the castle—this is where intrusion detection systems (IDSs) and distributed denial of service (DDoS) defenses come into play. In network security parlance, an intrusion happens when a cyber-criminal breaks into a network without causing any visible damage and then silently extracts information from the network, information like social security and credit card numbers. IDSs are designed to watch for and flag intrusions.

A DDoS attack is designed to make a network unavailable to its intended users by overloading web-connected servers. DDoS attacks are hard to defend against, but they often begin with multiple firewall contacts. Appropriate intrusion detection software can warn an SMB of an impending attack so steps can be taken to deflect the attack and keep the network running.

But what about information that needs to leave the castle securely and travel across open country? This is where a Virtual Private Network (VPN) comes into play. Like the security detail a king might use to surround private communications being sent to another castle, a VPN creates a secure, encrypted link between one private network connected to the Internet and another, ensuring that data traversing the public Internet is safe from compromise. The VPN encapsulates, encrypts and authenticates the data on both ends of the communication so it cannot be intercepted, modified or stolen. A good VPN protects the transmitted data so well that criminals looking for it don't even see it pass by on the Internet.

Unfortunately, no matter how well an SMB takes care of network security issues, there remains the possibility that its security

can be compromised by issues with its network endpoints, its individual PCs. New species of virus can sneak through even the most sophisticated content monitoring systems, and laptops are often taken home where unwary Internet usage or just bad luck can result in infection. The Verizon 2010 Data Breach Investigations Report (which contained information from both Verizon and the United States Secret Service) indicated that 46% of all verified security breaches came from *inside* a business firewall. And these intrusions can be quite serious, as key-loggers steal network passwords or viruses introduced by angry employees destroy data.

To combat the threat of attack from inside the firewall, SMBs can use antivirus, anti-spam and anti-spyware software which—when properly maintained and updated—can catch infections on network endpoints before they do any damage. They can also implement malicious web-site protections that prevent their employees from accidentally visiting sites that are known to cause infections or phishing sites that are designed to fool users into providing confidential information. Most importantly, businesses can make sure that the operating systems on their individual computers are updated regularly so that patches designed to close security holes are installed the instant they become available.

Finally, what about the cloud? One of the tremendous virtues of the cloud is that it allows an SMB to access cloud-based applications and computing resources from anywhere in the world. But its access-from-anywhere convenience also presents a security threat if non-secure passwords are used. There are simple measures a business can take to ensure that its employees each have their own password and that those passwords are secure, meaning that they are at least twelve digits long and contain both lower case and upper case letters as well as numbers. Further, SMBs can ensure that they encrypt all sensitive data on their employee laptops and have the ability to remotely wipe smart phones and other devices that are easily stolen.

How does Cbeyond Help SMBs with the Cyber-Security Threat?

Cbeyond was built from the ground-up to deliver technology services only to SMBs, and we strive to serve as their technology ally. An October, 2012 study of SMB security practices by the National Cyber Security Alliance and Symantec interviewed more than one thousand businesses with less than 250 employees and found that:

- 90% do not have an internal IT manager focused on technology-related issues;
- 87% do not have a formal written Internet security policy;
- 68% do not provide any cyber-security training to their employees; and
- 83% do not have an automated systems that requires employees to periodically change their passwords.

Given these statistics, we view helping our customers with their cyber-security needs to be a key part of our role as their technology ally, and we do this in two ways: through our products and through education.

From an education perspective, we maintain a blog at www.cbeyond.com that regularly addresses security issues faced by SMBs and provides links to in-depth information contained in industry whitepapers. We also draft our own whitepapers on security issues and distribute them to customers and partners. Finally, we educate our vendors and partners at live events on emerging security threats and how to address them with their customers.

From a product perspective, we do everything we can to provide cyber-security protection to our customers so they can focus on running their business rather than focusing on security. Our security products for customer networks include the most advanced managed firewall protection available via our TotalCloud Data Center and—most importantly—a private network that extends a customer's Local Area Network (LAN) into our SOC 2 and SOC 3 compliant data center so that their business-critical data never traverses the public Internet at all. For our multi-location customers and customers who need to be able to access their cloud resources remotely, we offer VPN services to protect data that must transit the public Internet.

Our products aimed at protecting customer endpoints include Secure Desktop which is constantly updated without customer intervention and stops viruses and spyware before they can infect a customer computer. Our customers can check the security status of every PC they own via an online portal. We also offer network security assessments on customer request, and—if they have a problem with a virus or other malware—we will visit their business to take care of the issue.

Cyber-security is one of the most critical issues facing Internet-connected SMBs today, and the role that the Subcommittee can play in educating them about the threat and the ways to mitigate it cannot be underestimated. Mr. Chairman and members of the Subcommittee, I appreciate the Committee's interest in this important topic and thank you for the opportunity to provide this statement for the record.

**House of Representatives
Committee on Small Business**

Protecting Small Businesses Against Emerging and Complex Cyber-Attacks

Thursday March 21, 2013

Written Testimony of Justin Freeman, Corporate Counsel, Rackspace US, Inc.

Table of Contents

I.	About Rackspace – Fanatical Support and the Open Cloud	3
II.	An Overview of the Cloud	4
	Cloud Infrastructure – Different Shapes of Clouds	4
	Cloud Service Models – Different Levels of Control	6
III.	Why the Cloud? The Benefits to Businesses & Consumers	8
	The Cloud and the Coming Mobile Revolution	9
IV.	Security in the Cloud & the Role of the Cloud Provider.....	10
	A. Fundamentals of Cyber-Security in the Cloud	11
	The Increasing Complexity of Security and Compliance Requirements	11
	Compliance Standards and Regulatory Requirements	12
	B. Security Advantages of Utilizing a Cloud Service Provider	13
	The Responsible Service Provider as Security Partner.....	14
V.	Principles of Cyber-Security Policy.....	17
	Responsible Information Sharing.....	17
	A Light Touch – Flexible Approaches Which Reflect New Realities	18
	Respect for International Competitiveness & Consistent Regulatory Regimes.....	18

I. About Rackspace – Fanatical Support and the Open Cloud

Founded in 1998 and headquartered in San Antonio Texas, Rackspace is the service leader in cloud computing — a fast-growing industry that helps businesses avoid the expense and hassle of owning and managing their own computer gear by providing computing resources to them over the Internet. Rackspace now serves more than 170,000 customers in 120 countries, including most of the global corporations in the Fortune 100. More than 4,300 engineers, software programmers, customer support representatives, and others provide famed Fanatical Support, the 24/7/365 customer service and support that has defined Rackspace.

One of Rackspace’s top priorities is focusing on the development and deployment of Open Cloud computing infrastructure, based on the OpenStack platform jointly developed with NASA. OpenStack is a set of open-source cloud computing technologies which are platform agnostic – meaning that a company utilizing OpenStack to run its cloud computing services is capable of migrating between a variety of hosting providers and platforms, instead of selecting only one provider and being stuck with that choice. These Open Cloud technologies represent a sea-change in cloud computing – by eliminating proprietary lock-in they help foster critical industry standards for cloud computing and create a robust ecosystem of services which span multiple cloud providers. Much like a cell phone that a user can take from carrier to carrier, applications built on an OpenStack infrastructure can easily be moved between hosting providers. The broad experienced and developed enterprises which are members of the OpenStack foundation, along with the contributing members of the OpenStack community, help bring a new level of community support and dedication to the project which substantially enhances the security of the OpenStack platform and codebase.

ABOUT RACKSPACE® HOSTING
THE SERVICE LEADER IN CLOUD COMPUTING

4,300+ RACKERS 

180,000+ CUSTOMERS
82,000+ SERVERS 

GLOBAL FOOTPRINT
120+ COUNTRIES 

8 WORLDWIDE DATA CENTERS 

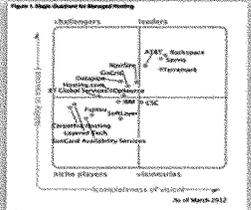
PORTFOLIO OF HOSTED SOLUTIONS
Dedicated - Cloud - Hybrid 



WE SERVE 60% OF THE FORTUNE® 100

OVER \$1 BILLION \$\$\$\$
Annualized Revenue

Figure 1: Magic Quadrant for Managed Hosting



Source: Gartner, "Magic Quadrant for Managed Hosting Providers," 2012. Rackspace is positioned in the Leader quadrant.

A LEADER
Gartner Magic Quadrant
for Managed Hosting

© 2012 Gartner, Inc. All rights reserved. G01212-1

We are proud to have been named a Gartner® Magic Quadrant for Managed Hosting provider as the confirmation that Fanatical Support™ provides great IT solutions for our customers.

Lanham Rieger
CEO, Rackspace

II. An Overview of the Cloud

At its heart, cloud computing is nothing radically new. “Cloud” essentially describes the use of remote computing resources, whether it be storing information remotely (such as by utilizing a web based email account to store emails in a providers cloud, rather than on a local laptop), or processing information remotely (which occurs when a user leverages the processing power of a remote computer to perform calculations – power which may not be available at a local laptop). These two fundamental computing resources, *storage* and *compute*, are the essence of modern information technology.

What is new is the ubiquitous availability of remote connectivity which drives the cloud revolution. During the first stages of the IT revolution, corporations deployed massive mainframes which handled all the storage and compute needs of users, who accessed these remote resources through terminals. Although few consider this cloud computing, because all the systems were local and required a physical link, the terminal-mainframe model informs modern cloud computing approaches.

As modern workstations increased their storage and processing capabilities, an increasing amount of work was done exclusively on a user’s local computer. Even in the early days of the internet, most storage was local, and local compute power was all that a user had access to. Contrast that with today’s cloud, where applications are consumed as remote resources, rather than software running on a local device.

The cloud commoditizes storage and compute resources, permitting companies to save substantial amounts of capital by paying for modern IT costs on a utility basis, just like electricity consumption, rather than invest in large capital intense “homegrown” IT infrastructure. This utility model is the blessing of the modern cloud – it permits IT resources to be dynamically allocated as needed, and allows services to be delivered over the internet to almost any user on any device (whether a laptop, cell phone, or tablet). The enhanced user experience and savings drive modern innovation in virtually all sectors of the economy.

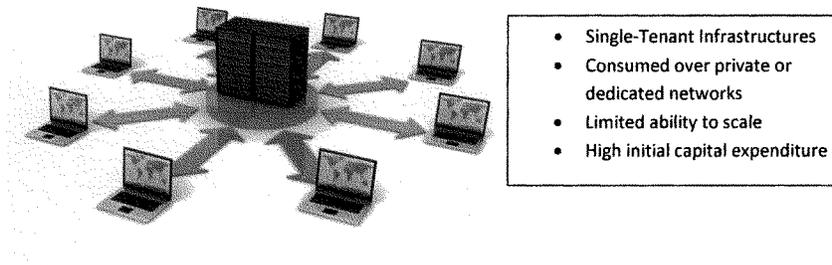
The flexibility of IT models has resulted in a lot of confusion regarding what constitutes a cloud. There is no concrete definition – “cloud computing” has become an expansive term encompassing types of infrastructure (dedicating servers to one company’s use, or sharing them to maximize cost savings) and types of services (such as remote email, or remote office applications).

Cloud Infrastructure – Different Shapes of Clouds

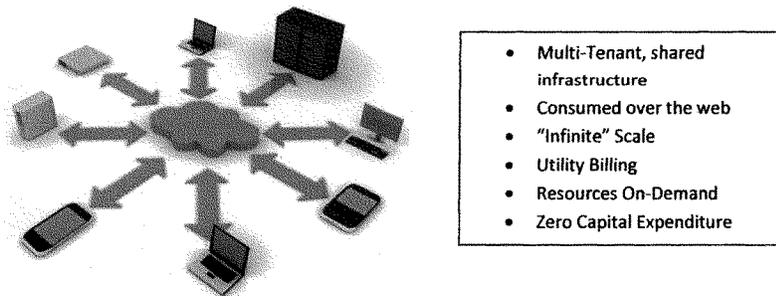
Clouds come in various types and shapes, the configuration of the underlying servers and devices constitutes the infrastructure of the cloud. While the potential for recombination is substantial, there are fundamentally three different types of cloud infrastructure.

Dedicated Clouds or **Private Clouds** are comprised of physical infrastructure dedicated to one company’s use. That company controls the servers and storage devices exclusively. Also known as private clouds, these are the “single family homes” of the cloud. Dedicated clouds can be located anywhere – at a company’s corporate headquarters or at hosting providers data

center. Private clouds are a more traditional version of cloud infrastructure, they are not as scalable and involve greater initial costs, but they can be higher performing, are isolated to single users, and can be more appropriate for some types of data processing or applications. For example banks often operate all critical financial resources on a dedicated private cloud – but all their users are still logging in and sharing access to that cloud in a controlled fashion.

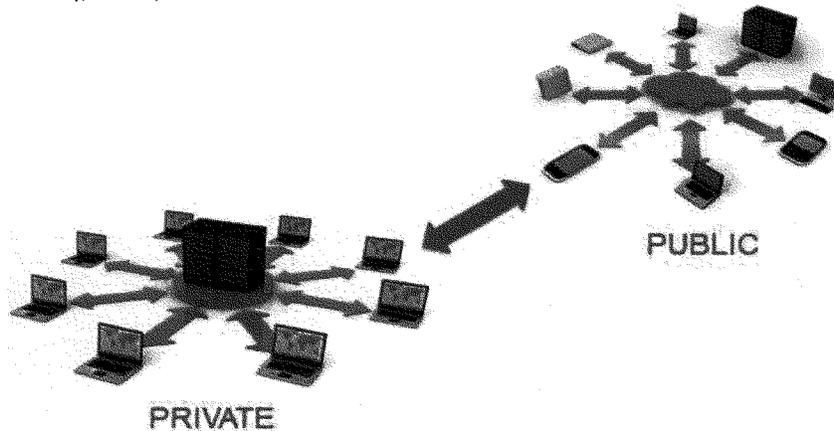


Public Clouds are made up of shared servers whose resources have been virtually partitioned on a per-user basis. These are the “apartments” of the cloud – all users rely on the same set of underlying devices, and a provider typically manages the segregation of those resources by user. These are the most cost effective types of cloud infrastructure, as the overall capital costs are shared amongst the users, who typically pay only for what they use. Because of their shared nature, public clouds are almost always maintained by a hosting provider at premises that it operates. Shared resources (compute and storage) are pooled for efficient pricing, utility billing, and are highly scalable. Public clouds can be provided as services (in the form of applications), or they can be provided as bare resources for businesses to turn on and off as needed.



Hybrid Clouds are the latest and most flexible clouds. They allow an “anchor” deployment of a dedicate private cloud to meet higher security or foundation resource needs, and link the parts of the service that need to scale to a public cloud. So while a commerce website around the

holiday season might want a solid, stable, and powerful payment processing system, their needs for serving ads and displaying inventory in webpages are going to be dynamic and high – they might use a private cloud for payments, and a public cloud for web content like their catalog. A company may split its use of cloud systems between resources dedicated to its use (a dedicated cloud) and resources it shares (a public cloud) in order to balance the need for control provided by dedicated clouds with the cost savings of public clouds. A company may also make use of some computing resources which it runs at its own offices, and some which it outsources to a hosting provider. This balancing act often results as a trade-off between security, control, and cost.



These “different types of clouds” reflect different configurations of computing resources, which are then used to provide different types of services in a ‘pay as you go’ approach. Cloud service models often scale control with cost, and reflect different methods of delivering services through the cloud in a utility pricing model.

Cloud Service Models – Different Levels of Control

The different types of clouds (configurations of computing resources) are used to deliver different types of service models. These service models scale control with cost, and are different methods of delivering services in a cost effective utility model. As a user moves from consuming IT resources in the form of dedicated devices (such as servers in a company data center) to consuming IT resources as a service they gradually cede control to providers and third parties.

- **Infrastructure as a Service (IaaS):** In this most fundamental type of IT service, providers control the datacenter, the network, and physical access to servers and storage devices. Users control the rest, and are often responsible for their administration of the IT

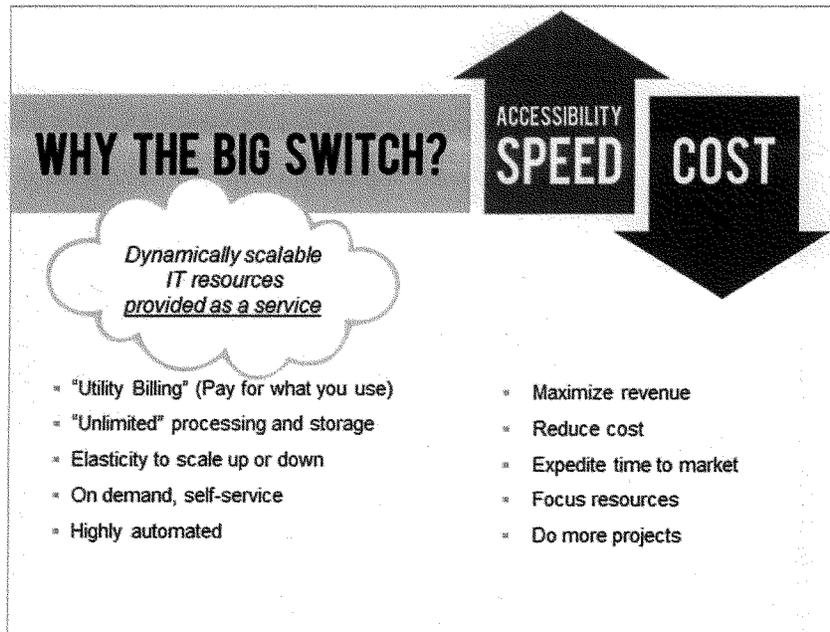
resources. Most IaaS providers will not permit their customers physical access to devices – all their users share the same physical location, although many of the actual devices are dedicated to particular users rather than shared.

- **Platform as a Service (PaaS):** In the platform model, the provider controls the infrastructure (which of course may be subcontracted) and deliver systems ready to run user's applications. Users bring their applications and data and run them on a ready-to-go platform managed by the provider.
- **Software as a Service (SaaS):** In a SaaS model the underlying IT resources are obfuscated from the user, and the provider delivers a ready-to-use application, maintaining responsibility for the underlying platform and infrastructure. This is the most common type of cloud service for consumers (gmail & Office 365 are great examples – the user consumes and email or office application, without having the software installed locally), and is increasingly relied on by businesses looking for customized off-the-shelf applications, without having to make substantial investments in new computing infrastructure.

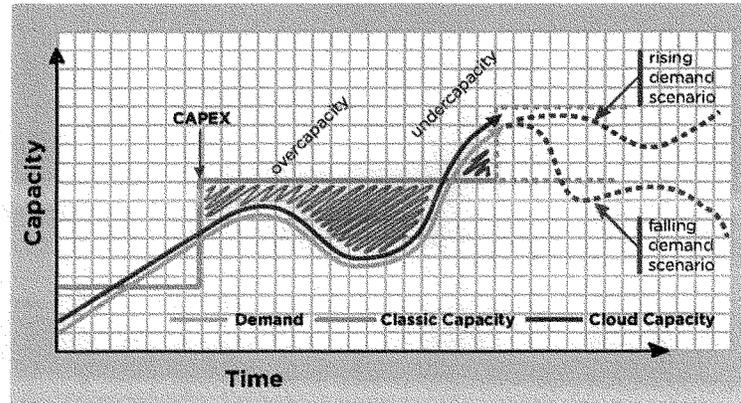
Although the types of resources used by the cloud are not novel, the combination of choice and the ability to hand-off control of IT resources at various levels is. Ultimately, securing the cloud requires you to know who is in charge of what layer of security, and what they are doing about it (how are they protecting your data?). The fundamentals of IT security are quite similar in the cloud; the focus of a responsible cloud user should be on ensuring that at each layer of cloud security, appropriate controls are in place. Ultimately, the party which controls the data has the most fundamental level of security responsibility – they can encrypt sensitive data and thereby truly protect it from malicious or unauthorized access. This paper will focus on cyber-security matters in the cloud, but the fundamental principles remain the same across all IT platforms.

III. Why the Cloud? The Benefits to Businesses & Consumers

The technological revolution that stems from cloud computing adoption well exceeds the level of change that we have come to expect in information technologies. "The cloud" is not just an incremental improvement in how fast or how heavy our laptops are, it is a massive change. One that represents an entirely new era in IT. Especially for consumers and small businesses who now have access to computing resources in ways never previously possible, breaking down barriers to entry and opening an international market of possibilities.



Cloud technologies shift IT to a public utility model. Centralized IT is like centralized power generation. Instead of generating all your power locally, with the cloud you're connected to a power grid, and can consume what you need from the grid. For businesses this results in a revolutionary approach to consuming IT resources – a push button approach to provisioning additional capacity, and the ability to turn capacity down, or even off. This utility approach is something that has never been possible before in the world of IT, and the savings it offers businesses which cannot afford large capital expenditure management cannot be overstated.



Before the cloud, in order to expand computing power, you had to make single, large investments (illustrated in the stair stepped green CapEx line). This meant that businesses were perpetually under-capacity (which resulting in poor user and customer experiences) or over capacity (which resulted in inefficient use of often limited capital resources). With the cloud in play, businesses can ride the demand curve for computing resources. On-demand, on-time, and on-budget is the promise of cloud for businesses.

Uniquely, businesses can utilize the cloud to export services without previously unapproachable overhead. Delivering services over the internet allows U.S. businesses of all sizes to readily offer their expertise and innovative solutions to consumers globally, opening up the ability to export services without locating a physical presence abroad, and thus supporting domestic jobs and economic growth.

The Cloud and the Coming Mobile Revolution

The unprecedented access to readily available, highly scalable and utility priced computing resources is heralding a new age in mobile application development and utilization. To date, most mobile applications have focused on 'phone-sizing' a normal web browsing experience, with many applications simply reformatting a traditional web experience for a mobile device.

No longer held back by local resources, and able to access diverse and powerful remote computing resources through the cloud, application developers are shifting their focus to innovative integrated application experiences. These new application approaches will integrate a contextual approach to mobile application utilization – instead of a user navigating a series of menus akin to our traditional application experience, this new generation will rely on integrating information about a user's location, past habits, configured preferences, capable of seamlessly interacting with all of a user's devices (be it a car, fridge, computer, or home monitoring and automation systems) to provide a "contextual experience" – one where achieving a task is intuitive and easy. Leveraging a complex web of cloud-based resources will provide the foundation for a coming revolution in mobile applications and services.

IV. Security in the Cloud & the Role of the Cloud Provider

Using the cloud safely means using the cloud securely. This consists of four major areas which all cloud users, especially smaller businesses without large compliance and dedicated security teams, need to review. In order to build a secure cloud, it is essential to select the right cloud infrastructure, select the right provider, review the provider's security and operational controls, and to ensure sensitive data is always encrypted.

- **Selecting the right cloud infrastructure:** while an infrastructure dedicated to a single user is typically the most secure, public clouds formed of shared resources can be just as secure. The key element is identifying how data is secured, regardless of the type of cloud it resides in. The best cloud configuration is a nimble cloud: a balance of cost and security which scales both based on your use case.
- **Selecting the right provider:** It is critical that cloud users have a clear understanding of the security practices undertaken by their providers, and that the providers are willing to demonstrate compliance with their controls. There are an incredible number of potential combinations of security responsibilities, so users must make sure they choose a combination that meets their needs and capabilities.
- **Reviewing security controls:** It is increasingly common to require a third-party audit of a provider's security controls, achieving both confidence in the provider and often in order to meet regulatory requirements. Three common audit and control reports are the SSAE16 (a third party review of a company's ability to meet its stated operational controls), a PCI-DSS audit (commonly utilized in the payment card transaction industry), and a Safe Harbor Self-Certification (especially critical in business ventures between U.S. and EU businesses).
- **Encryption, encryption, encryption:** Regardless of who is responsible for the layers of security, there is only one fundamental method of securing data: encryption. Encryption ensures that even when a system is breached (which increasingly seems like an inevitability even with the best security practices in place) the attacker is unable to utilize any data stolen, mitigating the risks to privacy (in the case of personal information), competitiveness (in the case of proprietary business information), and national security or defense (in the case of military information).

A. Fundamentals of Cyber-Security in the Cloud

Ultimately, securing the cloud requires you to know who is responsible for each aspect of the cloud resources, and how each layer of security is being addressed. There are three fundamental layers of security in the cloud:

- **Physical Security:** This most fundamental layer relates to having physical access to the IT appliances. If the servers running a cloud are not physically secured from unauthorized access then there is little else that can be done. A malicious party with physical access to a server can readily engage in obvious sabotage such as data theft (even as simple as removing the physical hardware) and physical damage causing data loss, as well as more complicated security risks, such as injecting malicious code or viruses through a thumb drive.
- **Network Security:** It is critical to secure networked systems both from local threats (other users on the same network, including other employees in the same office for example) and remote threats (malicious attacks over the internet). Network security in the cloud is often split amongst multiple parties, so it is especially important for a security conscious user to understand who is responsible for what portion of the network. Insecure networks can permit unauthorized access, the injection of malicious code and viruses, to the more common denial of service attack – where a third party shuts down the ability of servers to function by overwhelming their network capabilities, without necessarily engaging in theft.
- **Logical Security:** The broadest layer of security, logical security relates to controlling user permissions and securing applications from vulnerabilities. Controlling who can get to what based on their access credentials is a fundamental requirement for a secure system. Role based access restrictions are a mechanism of getting users access to the data they need (like quarterly financial statements) while keeping them out of data they don't (like HR records). It also relates to the security of the applications users run – the most common security gap occurs when a user fails to update their operating systems (such as with Microsoft's routine patches) or their anti-virus definitions (without constant updates, anti-virus programs can easily become obsolete).

The Increasing Complexity of Security and Compliance Requirements

The most important reason that organizations struggle with security is that the security landscape is complex. There are three dimensions to this complexity:

- First, there are many **attack vectors and security disciplines**. These include identity, access management, encryption, data protection and trust management, denial of service attack mitigation, vulnerability assessment, end-point security and regulatory requirements, just to name a few.

- Second, there are **multiple layers in a given application's architecture stack**, from the network, systems, operating systems and databases, to the application and its multiple access points. The modern web application is built on multi-tier service-oriented architectures with a myriad of moving parts, and deal with many types of access devices (mobile and desk based). Each one of these layers represents a subset of potential security weaknesses.
- The third is time: **security is an ongoing operation**, not a point-in-time individual project. There is a need for continuous management to maximize the investment one makes in security.

All of this complexity creates the opportunity for specific breakdowns of communication or of operational responsibility. But the most obvious change in the way application services are delivered is that companies and cloud providers have partial ownership over the whole computing stack of a given service. Sometimes, a cloud provider is responsible for the whole compute stack, as occurs with SaaS applications. More commonly, both the customer and the cloud provider take responsibility over a subset of the application stack. For example, it is possible that the customer manages the application-level components while the provider manages the network and the infrastructure (as is the case in many of our public cloud and dedicated offerings). It is this shared scope over the computing stack that complicates the processes and procedures that must be undertaken to deliver a service that reduces security weaknesses.

Compliance Standards and Regulatory Requirements

Cloud users should be especially sensitive to regulatory requirements (whether industry or governmentally based) regarding the types of data they store in the cloud. Below are some examples of the different types of data commonly stored in the cloud and applicable U.S. regulations.

Data Types	Examples	Example Regulations
Personally Identifiable Information (PII)	Credit Card Processing Information	PCI-DSS, Gramm-Leach-Bliley
Protected Health Information (PHI)	Health Records	HIPAA/HITECH
Sensitive Corporate Governance Data	Corporate Audit & Financial Reports	Sarbanes-Oxley
Sensitive Business Information	Forecasts, Development Plans, Strategic Proposals	None – High Economic Value
Generally Public / Non-Sensitive Information	Marketing Collateral, Miscellaneous Documentation	None – Low Economic Value

Cloud providers offer a host of services which enable customers to meet their regulatory requirements with regard to sensitive data types, although a discussion of these requirements is outside the scope of this comment, a key advantage of cloud services is the ability to implement cost-effective security and regulatory controls with a trusted and audited cloud service provider.

B. Security Advantages of Utilizing a Cloud Service Provider

Both the cloud provider and the customer have to work together to ensure security best practices are followed and met. Given the role of the customer in the configuration and consumption of their cloud environment, it's imperative for the cloud provider and cloud customer to both put controls in place to manage the risks that multi-tenant environments can present. Both the cloud provider and cloud customer must accept responsibility for different aspects of the system and both must implement a range of controls in order to properly secure the service. Cloud security isn't a sprint – it's a marathon. It can also be thought of as a relay: strong cloud security comprises products and services from various players.

A recent Alert Logic whitepaper¹ (the twice-yearly data-driven analysis called the State of Cloud Security Report) addressed many of the common fears about “ceding control of data to the cloud” – the sense that a business gives up control and capability to deal with security challenges when it chooses a cloud services partner. Contrary to many concerns about security, the study found:

- When compared to traditional in-house managed IT environments, service provider environments show lower occurrence rates for every class of incident examined.
- Service provider customers experienced lower threat diversity (i.e., the number of unique incident classes experienced by a customer) than on-premise customers.
- On-premise environments were twelve times more likely than service provider environments to have common configuration issues, opening the door to compromise.
- While conventional wisdom suggests a higher rate of Web application attacks in the service provider environment, Alert Logic found a higher frequency of these incidents in on-premise environments.

Much of this difference can be explained by evaluating the relevant “IT surface area.” Service providers offer a discrete, centrally managed security environment with tightly controlled network access and enforced partitions between users. A large part of a service providers value stems from their operational expertise and dedication in managing large IT datacenter infrastructure, necessarily architected with security as primary consideration. In contrast, in-house IT deployments often grow as needed in spurts, without the benefit of

¹ Removing the Cloud of Insecurity, State of Cloud Security Report, Spring 2012. Alert Logic. Available at: http://www.rackspace.com/knowledge_center/sites/default/files/whitepaper_pdf/Alert%20Logic%20Cloud%20Security%20Report%2C%20Spring%202012.pdf

advanced central planning which is essential to secure network environments, and are composed of a broad array of operating systems and applications. In-house IT deployments typically also suffer from a greater number of 'entry points' – routes that a malicious attacker can take to access systems and servers – because their networks include mobile devices, desktops, laptops, and other user-facing systems which co-exist in the same network infrastructure. This mixed and broad environment substantially increases the security challenges compared to a dedicated hosting environment. A service provider can also uniquely offer technologies which protect the entire datacenter network, but which are typically prohibitively expensive to single users. The cloud permits economies of scale both in security solutions and compute resources.

The Responsible Service Provider as Security Partner

A well rounded service provider offers a robust approach to a customer's security in the cloud environment; there are four areas to focus on when evaluating a service provider's commitment to providing a secure environment to combat existing and emerging cyber-threats while helping customers meet regulatory requirements:

- Security Oriented Product Services. A service provider should offer both fundamental security solutions (such as firewalls, intrusion detection and prevention systems) as well as advanced compliance or security services (such as log management and review, and Denial of Service prevention systems). Often a robust service provider will partner with other trusted enterprises to deliver a broad range of security expertise to meet the myriad of niche compliance requirements facing customers. The provider should act as a trusted guide and advisor, helping a customer navigate the available security services in light of a customer's anticipate risk and compliance needs.
- Clearly defined roles, access rights, and responsibilities. A service provider and its customers should work together to identify areas of explicit control (such as the service providers exclusive control over physical security of a datacenter, or a customer's responsibility for securing user-access rights) and establish an on-going understanding regarding areas of shared control (such as management of firewall rules). Security controls documents should identify where a service providers existing controls end, and a customer's responsibility begins.
- Protect data responsibly. Service providers should commit to utilizing their customers data in a responsible fashion, including with regards to both civil and criminal data disclosure requests in accordance with applicable law. These commitments can be critical to enabling small businesses without an international presence to compete in an international environment flush with complex and sometimes contradictory privacy and information disclosure requirements.

- Provide audit documentation. Security and compliance is a shared commitment, and no service provider can offer a ready-made cloud compliance solution in a box – but they can lay the foundation for a customer’s use to be secure and meet compliance requirements (whether private or regulatory). A provider should have a commitment to annual third-party audits which it shares with its customers, and its datacenters and services should adhere to recognized certification frameworks. Still, a provider should have a deeper commitment than just having controls in place, it should actively and routinely revisit its security posture and systems controls in light of the evolving nature of cloud systems and threats.

At Rackspace, we believe that security is a partnership, a shared responsibility between our customers and our architects, security experts, and operations personnel. We believe that this is the only way to not only create a technical architecture that reduces the possibility of introducing vulnerabilities into your application, but also to create clarity and understanding about the processes and the proactive and reactive measures that must be put in place. More importantly, realizing that Security is a shared responsibility helps our customers and Rackspace focus on providing transparency on the roles and responsibilities of each party.

The sophistication level of the next generation of cloud-based applications is increasing, and with it, the security landscape is turning more complex. Businesses must pay attention to the details of the relationship as they consider any hosting or cloud provider and dive into the details of the technology, processes and policies to provide an appropriate security level.

A sample of Rackspace’s security controls follows this page, identifying our approach to several security areas.²

² Available at: <https://www.rackspace.com/security/>

<p>Physical Security</p> <p>Physical Security includes locking down and logging all physical access to our data centers.</p> <ul style="list-style-type: none"> • Data center access is limited to only authorized personnel • Badges and biometric scanning for controlled data center access • Security camera monitoring at all data center locations • Access and video surveillance log retention • 24x7 onsite staff provides additional protection against unauthorized entry • Unmarked facilities to help maintain low profile • Physical security audited by independent firms annually 	<p>Operations Security</p> <p>Operational Security involves creating business processes and policies that follow security best practices to limit access to confidential information and maintain tight security over time.</p> <ul style="list-style-type: none"> • ISO 27001/2 based policies, reviewed at least annually • Documented infrastructure change management procedures • Secure document and media destruction • Incident management function • Business continuity plan focused on availability of infrastructure • Independent reviews performed by third parties • Continuous monitoring and improvement of security program
<p>Network Infrastructure</p> <p>Network Infrastructure provides the availability guarantees backed by aggressive SLAs.</p> <ul style="list-style-type: none"> • High-performance bandwidth provided by multiple network providers • Elimination of single points of failure throughout shared network infrastructure • Cables properly trunked and secured • Proactive network management methodology monitors network route efficiency • Real-time topology and configuration improvements to adjust for anomalies • Network uptime backed by Service Level Agreements • Network management performed by authorized personnel only 	<p>Environmental Controls</p> <p>Environmental Controls implemented to help mitigate the risk of service interruption caused by fires, floods, and other forms of natural disasters.</p> <ul style="list-style-type: none"> • Dual power paths into facilities • Uninterruptible power supplies (minimum N+1) • Diesel generators (minimum N+1) • Service agreements with fuel suppliers • HVAC (minimum N+1) • VESDA / fire suppression • Flood detection • Continuous facility monitoring
<p>Human Resources</p> <p>Human Resources provides Rackspace employees with an education curriculum to help ensure that they understand their roles and responsibilities as they relate to information security.</p> <ul style="list-style-type: none"> • Background screening performed on employees with access to customer accounts • Employees are required to sign non-disclosure and confidentiality agreements • Employees undergo mandatory security awareness training upon employment and annually thereafter 	<p>Security Organization</p> <p>Security Organization includes establishing a Global Security Services team tasked with managing operational risk, by executing an information management framework based on the internationally recognized ISO 27001 Standard.</p> <ul style="list-style-type: none"> • Security management responsibilities assigned to Global Security Services • Chief Security Officer with oversight of Security Operations and Governance, Risk, and Compliance activities • Direct involvement with Incident Management, Change Management, and Business Continuity

V. Principles of Cyber-Security Policy

Federal regulations have several key roles to play in helping provide for a safe, secure internet which supports innovation, protects consumers, and permits U.S. businesses to export services and remain globally competitive. As in all complex environments, there is no magic bullet, but a coherent and informed set of sector specific regulations, security policies and practices, privacy protections, and collaborative commitments can provide a strong foundation on which U.S. businesses and providers can continue to operate safely and securely.

Sector specific regulations recognize that blanket approaches fail to provide sufficient nuance in implementation and appropriate focus, stifling innovation and fostering inefficiency. Limiting regulations to high-risk areas avoids unnecessary bureaucracy and permits sufficient enforcement resources to be dedicated. High-risk areas and systems should be carefully identified and appropriate standards established to guide, rather than force, the implementation of a stable set of fundamental security practices. No regulatory guidance or set of requirements can themselves establish a network or system which is impervious to attack, but they can provide solid guidance and expertise to inform users and businesses. I urge policy makers to consider the following three principles when considering regulatory or policy action.

Responsible Information Sharing

With appropriate safeguards, increased cyber security collaboration can help prevent denial-of-service attacks, thefts of sensitive information and attacks on the nation's infrastructure. Private industry currently engages in widespread, but often very inefficient, dissemination of security threat information, often limited to a couple of parties or through the security professional community.

As each entity is capable of identifying unique trends and attacks relating to its specific infrastructure, collaboration most often results when one entity's infrastructure is used (after being compromised by a malicious party) to attack another company. Similarly, federal law enforcement agencies track complex international cyber-criminal organizations, but often share that information only with victims, meaning, after the fact. It is critical to establish a clear flow of cyber-threat information from all stakeholders and ensure its widespread accessibility.

But any cyber security bill that is designed to encourage and protect information sharing must recognize the complexities created by shared computing infrastructure environments which are at the heart of cloud computing. Selective information sharing, in the name of stopping cyber threats, can have the unintended consequence of magnifying a security risk. A user of public cloud computing services should not be permitted to disclose information about any vulnerability in that cloud without first disclosing the vulnerability to the cloud provider. This approach would give the provider an opportunity to resolve the vulnerability as quickly and simply as is possible — or to limit or block disclosure in cases where the disclosure would pose a threat to other users served by that provider.

A careful balance must be struck to promote responsible disclosure of vulnerability and threat information without creating additional risk to users of shared computing environments,

and useable, actionable information must be timely disseminated to infrastructure operators and stakeholders.

A Light Touch – Flexible Approaches Which Reflect New Realities

Cyber-security legislation should reflect the new realities of how IT works in the cloud. Any new law should be tailored to fit the way that individuals and companies today use shared computing resources, which are available on demand, across the globe.

Regulations should avoid a reliance on particular or specific technological solutions. These can only stifle innovation by mandating a reliance on a particular technology. Security requirements should be addressable through a reasonable mix of administrative, physical, and technical controls which are evaluated in light of a party's utilization of computing resources.

Likewise while it is critical to allow companies the flexibility to implement to address control requirements, those requirements must avoid excessive vagueness and especially avoid retrospective analysis or results-determined compliance. While regulations should seek to provide controls in appropriate contexts which aim to ensure the security of sensitive data, simply mandating that entities commit to implement controls to 'ensure' security is ineffectual. What controls are sufficient to ensure security? One can only identify gaps after a breach – meaning the ones that were not in place when a compromise happened. The introduction of vagueness or uncertainty into security or privacy regulations can undermine the effectiveness of otherwise well designed approaches, and risk heightening liability for business which are otherwise acting in good faith but find themselves the victim of a malicious third party.

It is also critical to compliment, not contradict, the internet's enabling technologies. Manipulation of fundamental and shared communication systems, such as the Domain Naming System (DNS), are fraught with dangerous consequences and should be avoided without a clear and broad consensus from all stakeholders that such approaches are net-positive for the internet as a whole. Damaging the underlying technologies which enable the internet to be a self-healing, globally effective communications system will only stifle innovation and develop new, unforeseen security risks.

Respect for International Competitiveness & Consistent Regulatory Regimes

Especially when it comes to data privacy and disclosure policies, it is essential at all levels to recognize the impact that data-privacy laws of other countries, particularly in Europe, have on U.S. technology companies — and on U.S. competitiveness. Some European officials, along with European companies that compete against U.S. Internet firms, are actively spreading misinformation about U.S. law.

We continually hear the canard that it is "unsafe" to host data with U.S.-based cloud-computing companies in their European data centers because the U.S. government can access customers' data easily, without due process. While that's simply not true (there is no U.S. law that overrides the data-privacy laws of European nations and The Patriot Act does not allow U.S. law enforcement agencies to access data in overseas data centers) policies which permit information disclosure in the name of law enforcement or security concerns routinely re-ignite

this issue, to the detriment of U.S. companies and the competitiveness of one of America's fastest growing industries.

Congress should provide specific assurances that the data privacy laws of our trading partners will be respected. It is essential that our security and privacy policy regime move towards a consistent international privacy and data transfer framework, while simultaneously providing clear interpretations of U.S. laws which may impact the obligations of U.S. companies serving international customers.



**“Protecting Small Businesses Against
Emerging and Complex Cyber-Attacks”
House Small Business Subcommittee on Health and
Technology**

March 21, 2013

Submitted by:

**The Computing Technology Industry Association
(CompTIA)
515 2nd Street, NE
Washington, DC 20001**

Computing Technology Industry Association (CompTIA)
Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624

Introduction

Good afternoon, Chairman Collins, Ranking Member Hahn, and distinguished members of the House Subcommittee on Health and Technology. This testimony is submitted on behalf of the Computing Technology Industry Association (CompTIA).

My name is Dan Shapero, I am a CompTIA member and the Founder of KlikCloud, a company I launched in 2010 focused on offering a variety of IT services, such as Digital Marketing, Website hosting, SEO (Search Engine Optimization) blogging, email newsletters, and other business advisory services.

I am a California native and graduated from the University of California, San Diego. Prior to KlikCloud I spent 20 years working as a technology executive, including at Ernst and Young, a professional services organization, and at Kaseya, an IT automation and cloud services based business. I have launched or helped other entrepreneurs launch several IT startup companies. For instance, my past clients include Vincinity which is now Microsoft Maps, and Avamar which is now EMC2.

In short, I have 25 years of experience in the IT sector as an executive and entrepreneur. I have worked on cybersecurity issues for 8 years and have looked at the issue as a user and a service provider.

I want to thank Chairman Collins, Ranking Member Hahn, and Members of this Subcommittee for holding this important hearing to “examine the increased volume and complexity of cyber-attacks as it affects emerging technologies utilized by small businesses, such as cloud computing and mobile technology.”

From the perspective of a small tech business, cybersecurity is among the most important issues facing small and medium size companies. We will highlight this point shortly, but first some background on CompTIA.

About CompTIA

The Computing Technology Industry Association (CompTIA) is the voice of the world's \$3 trillion information technology industry. CompTIA membership extends to more than 100 countries. Membership includes companies at the forefront of innovation along with the channel partners and solution providers they rely on to bring their products to market and the professionals responsible for maximizing the benefits that organizations receive from their technology investments. The promotion of policies that enhance growth and competition within the computing world is central to CompTIA's core functions. Further, CompTIA's mission is to facilitate the development of vendor-neutral standards in e-commerce, customer service, workforce development, and ICT (Information and Communications Technology) workforce certification. CompTIA is also the leading

Computing Technology Industry Association (CompTIA)
Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624

global provider of IT workforce certifications. Currently there are over 1.4 million CompTIA IT certification holders worldwide, and many of those are for IT security

CompTIA's members include thousands of small computer services businesses called Value Added Resellers (VARs), as well as nearly every major computer hardware manufacturer, software publisher and services provider. Our membership also includes thousands of individuals who are members of our "IT Pro" and our "TechVoice" groups. Further, we are proud to represent a wide array of entities including those that are highly innovative and entrepreneurial, develop software, and hold patents. Likewise, we are proud to represent the American IT worker who relies on this technology to enhance the lives and productivity of our nation. Based upon a recent CompTIA survey, we estimate that one in twelve (or about 12 million American adults) considers him or herself to be an IT worker. This is larger than the number of American adults classified by the Bureau of Labor Statistics (BLS) as employed in farming, mining, and construction combined. This is also close to the number of adults classified by BLS as working in manufacturing or transportation. CompTIA has concluded that the IT workforce is now one of the largest and most important parts of the American political community.

Overview of the IT SMB Sector

As a baseline, the IT security infrastructure for SMB's is as vulnerable to cyber attacks and threats as large companies and firms. Unfortunately, SMB's are less resilient than larger companies because they have fewer IT resources in terms of personnel, hardware and software to combat the onslaught of daily cyber threats and attacks that many SMB's encounter on a daily basis.

Some SMB's are comprised of 5 to 20 employees, so resources come at a premium. As a small business owner I have to rely on my own expertise to implement adequate measures to ensure that the IT infrastructure that supports my business is secure. I also have to make sure that my clients understand the cybersecurity risks and threats to their businesses, and I advise them on the type of cybersecurity compliance measures that they must implement to keep their IT systems secure.

Opportunities for SMB's from Emerging Technologies

In the last five years, we have seen a steady transition from a server environment to a cloud-based one. This has created a tremendous opportunity and boost to the SMB sector. For SMB's, cloud computing services have been a huge equalizer in the marketplace. In the 1990's and early 2000's a new company had to invest considerable resources in IT infrastructure, including mainframes, servers, routers and other IT products and services to satisfy their computing needs. Today, with the advent of the cloud, SMB's can economically subscribe to cloud and virtual computing services from a third party for (literally) pennies on the dollar compared to the cost of building out the infrastructure that would offer comparable services. The emergence of cloud

Computing Technology Industry Association (CompTIA)
Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624

technologies is now allowing SMB firms affordable access to IT infrastructure, including software, that was financially beyond reach only a few years ago. This is an exciting time in the IT SMB sector, and it is even more critical now that we ensure there are adequate measures and controls in place to protect SMB's from cybersecurity threats and attacks.

As an IT professional, entrepreneur, and CompTIA member I would like to highlight two policy issues that have a significant ongoing impact on the IT SMB sector.

Data Breach Notification Reform

First, the majority of cyber attacks create exposure across state lines. For this reason data breaches are an area of serious concern. There are currently 47 state data breach notification (DBN) laws in place. These laws establish the circumstances under which a consumer must be notified when a breach of their personally identifying information (PII) has occurred. We think that consumer notice is a fundamental consumer right and we fully support it.

The issue for the SMB sector is that ongoing compliance with the patchwork of 47 different data breach laws across the country are an unnecessary burden, and in some instances, an insurmountable regulatory hurdle for an SMB to overcome. For example, state DBN laws vary as to when a consumer notice should be provided. Some state DBN laws require consumer notice when a company is made aware of a breach. Other state laws require consumer notice only if the breached data has the likelihood of resulting in consumer harm to the consumer. Moreover, all state DBN's differ on the type of penalties and fines that can be imposed and whether a consumer can file a private right of action against a company that has suffered a breach of consumer PII. These issues are compounded in the context of the cloud due to the mobility of data. In a cloud environment data travels across multiple jurisdictions adding more uncertainty for SMB's who may not have the resources to understand their DBN compliance obligations.

As mentioned earlier, SMB's tend to be very small with only a few employees. An annual report by the Ponemon Institute found that the average cost to a business for one incident of data breach to be \$6.75M and \$214.00 per customer record compromised.¹ A contributor to these costs arises from legal compliance and related expenses. For many SMB's an exposure of \$6M is enough to send an SMB into bankruptcy.

To be clear, CompTIA supports data breach notification laws, but again, the issue is that the current patchwork of state data breach laws imposes duplicative costs and undue burden on SMB's. SMB's must hire lawyers and expend other resources simply to track down the various compliance obligations. With our increasingly mobile economy these laws are getting even more complicated to understand since it is not always clear what

¹ <http://www.ponemon.org/news-2/23>
 Computing Technology Industry Association (CompTIA)
 Public Advocacy
 515 2nd St NE
 Washington, DC 20002
 202-503-3624

state a data breach may have actually occurred in which can be different from where a consumer may reside.

Therefore, CompTIA believes that the creation of a national framework for data breach notification can go along ways towards reducing costs and eliminating barriers to entry for SMB firms. A national framework for data breach notification will serve as an incentive toward the expansion of IT services across state lines.

Workforce Development

Another issue that we face as small and medium size businesses is the ability to recruit and retain in-house talent to help protect ourselves from cyber attacks. As Advanced Persistent Threats (APT) become more advanced and more persistent, all of our employees have a responsibility in keeping us secure; especially those in IT related roles. However, there is a skills-gap issue that is affecting the IT community as a whole. There are approximately 250,000 open IT jobs in the U.S. at any given time. As the SMB community, not only are we competing with the rest of the world for this talent, we are competing against other larger U.S. companies with big names. If the ecosystem were better saturated with the necessary skills, it would be significantly easier for us to attract candidates to our open positions. There are a lot of great opportunities that come with working for small and medium size companies that you cannot get in a larger institution, but we simply cannot compete with the recruitment dollars that are spent by the bigger names.

Certifications play an important role in this conversation. It is not the magic bullet, but it is a critical part of the solution. It is a way for us as employers to know that an applicant knows what they say they do and to have a professionalized IT workforce. The government should lead by example by hiring individuals who have earned industry-recognized certifications and by encouraging their existing IT employees to earn certifications. This will encourage others looking to enter the cyber workforce to focus on certifications as an entry point and help close the skills gap. Having access to a plentiful and skilled workforce will help companies like mine protect themselves from cyber attacks.

Finally, we believe that education about the steps SMB's should take to protect their IT infrastructure goes a long way toward making the overall US IT ecosystem more secure. Many of the IT vulnerabilities come from human error and negligence. For example, failure to implement security passwords or failure to keep the passwords secure with certainly reduce the overall threat of cybersecurity. Also, sharing information about how to safely share and exchange, information on the Internet can also help the overall ecosystem.

In closing, I would like to share for the record with this Subcommittee CompTIA's Information Security Trends report (<https://comptia.box.com/s/f2pob0gz7rl6hj5tdg9e>), and a link to a recent blog which I have highlighted below: (<http://clikcloud.com/blog/2013/03/07/cyber-security-threat-to-small-business/>).

Beef up your Network Security to Avoid Cyber Security Threats

Your network is only as strong as the weakest point. To avoid threats from Cybersecurity make sure you have a Firewall in place and keep all connected devices have up to date firmware, operating system patches and keep the latest anti-virus and anti-malware definitions current.

Cyber Security Education and Training

Educate your employees and staff on the threats of cybersecurity. Make sure they are aware of the threats of Phishing schemes and are able to identify and avoid these dubious attacks. Train all employees on the risk of sharing privacy data such as name, email, birthdays and financial information on social media networks.

CyberSecurity Policies and Procedures

Establish clear procedures on notification and escalation of a data leak or data breach. Ensure your team knows how to escalate a concern within your company. It is more important to raise the issues quickly rather than cover up a Cyber Security breach. Ensure you have clear policies on how to coordinate notifications outside of your company, should an attack occur.

CyberSecurity Insurance

Cybersecurity insurance is designed to help mitigate the loss of data leaks, network damage and other financial exposure of a Cyber Security attack. Your business may be eligible for affordable insurance to cover costs associated with CyberSecurity attacks.

There is no way to totally eliminate the risk of a Cyber Security attack, however, there are steps you may take to prevent attacks and be prepared on what to do in case your business is victimized. Contact your IT Support organization for a complete IT Security Assessment.

Closing

Thank you again for the opportunity to share our perspective on the issue of cybersecurity, and I would be happy to answer any questions.

Computing Technology Industry Association (CompTIA)
Public Advocacy
515 2nd St NE
Washington, DC 20002
202-503-3624

**STATEMENT OF DR. PHYLLIS SCHNECK, VICE
PRESIDENT AND CHIEF
TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR**

McAFEE, Inc.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON SMALL BUSINESS

SUBCOMMITTEE ON HEALTH AND TECHNOLOGY

***“PROTECTING SMALL BUSINESS AGAINST COMPLEX
AND EMERGING CYBER-THREATS”***

MARCH 21, 2013

Good morning Chairman Collins, Ranking Member Hahn, and other members of the Subcommittee. I am Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector for McAfee, Inc. We appreciate the Subcommittee’s interest in cyber security as it affects small business, and I’m pleased to be addressing the Subcommittee once again.

My testimony will focus on the following areas:

- The threat landscape and its implications for small business
- Recommended best practices for small businesses to protect themselves
- What the private sector can do to help small business
- What government can do to help small business

First I would like to provide some background on my experience and on McAfee.

I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to my role with McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance (NCFTA), a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 400 cyber criminals worldwide. Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee’s™ Internet reputation intelligence. I am the Vice Chair of the Information Security and Privacy Advisory Board (ISPAB) and have also served as a commissioner and working group co-chair on the public-private partnership for the Center for Strategic and International Studies (CSIS) Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2000 to over 33,000 members nationwide. Prior to joining McAfee, I was Vice President of Research Integration at Secure Computing. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

McAfee's Role in Cyber Security

McAfee, Inc. protects businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology company and is a proven force in combating the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers, who can now snap into our extensible management platform. Today, more than 160 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

The Threat Landscape and its Implications for Small Business

Since I last testified before the Subcommittee the cyber threat has only intensified. I want to focus on two areas where information technology is helping small business be more efficient but where caution is also necessary. These are the areas of mobile communications and the cloud.

Mobile Threats

It should come as no surprise that cyber criminals follow the latest technology trends because that's where the targets are the most promising. The growth in mobile communications is staggering, and the U.S. leads the world in mobility. Globally, mobile data traffic grew 70% in 2012, and by the end of this year the number of mobile-connected devices is expected to exceed the world's population, according to the Cisco Visual Networking Index.

Small businesses, as others, are relying more on mobile devices not only for communication but also for business processes, and there's every reason to believe this trend will continue. When I last appeared before the subcommittee, in December of 2011, mobile threats had begun to appear on the radar screen. Now they are front and center.

According to McAfee Labs, the growth in mobile malware almost doubled in each of the last two quarters of 2012. At the beginning of this year, the total number of samples in our mobile malware "zoo" reached almost 37,000—with 95% of those having arrived in 2012. To put this in perspective, in all of 2011 we gathered only 792 samples. The Android platform is the lead target of mobile malware, with 97% of last quarter's (4th Q 2012) being directed there.

One of the most volatile and worrisome areas of threats today is some new functionality in malware. A scam known as Android/MarketPay is a Trojan horse program that buys apps from an app store without a user's permission. We're likely to see crooks take this malware's app-buying payload and add it to a mobile worm. With such a mobile worm, attackers will no longer need victims to install a piece of malware. And if user interaction isn't needed, there will be nothing to prevent a mobile worm from going on a shopping spree.

Another developing area for mobile threats is in phones or other devices with near-field communications (NFC), which are becoming more common. As users are able to make "tap and pay" purchases in more locations, they'll carry their digital wallets everywhere. That flexibility will, unfortunately, also be a boon to thieves. Attackers will create mobile worms with NFC capabilities to propagate (via the "bump and infect" method) and to steal money. Malware writers will thrive in areas with dense populations (airports, malls, theme parks, etc.). An NFC-enable worm would run rampant through a large crowd, infecting victims and potentially stealing from their wallet accounts.

Attackers love it when users install malicious apps that let the bad guys gain complete control of victims' phones; it's no wonder that mobile backdoors remain popular with attackers. Android/FakeLookout.A is a mobile backdoor that pretends to be an update to antivirus software. In reality it hands control of a phone to an attacker. It's designed to steal and upload text messages and other files to the attacker's server. Another one of these is Android/GinMaster.A, a mobile backdoor that uses a root exploit to gain further access to a user's phone. It posts a number of pieces of identifying information to the attacker's server and accepts commands from the attacker.

As you can see, innovation is thriving in mobile malware development and needs to thrive even more strongly in our small businesses. Faced with the challenges of "Bring your own device," sometimes known as "BYOD," many small businesses will struggle with maintaining security and management control over a wide spectrum of devices that consumers increasingly want to use for their work.

Migration to the Cloud

Another IT trend that serves small business particularly well is migration to the cloud. Small businesses, in particular, can find real efficiencies in outsourcing their IT and communications systems to the cloud. They can reduce costs, improve offerings, eliminate complexity and have less need for onsite IT staff. These are great objectives—as long as security is not sacrificed.

I won't go into detail here, but not surprisingly, we are seeing bad actors target cloud providers. Most cloud providers do not offer a forensics capability as part of their base offering. This means that if a company's data stored in the cloud is breached, it will cost the company extra to provide forensic data to either law enforcement or a security firm so that the breach can be traced and remediated. Small business owners should address this need up front with cloud providers so they are not surprised if a breach occurs.

This is especially important at this time, when companies of all sizes are being encouraged to report breaches or suspected events to 1) protect victims, and 2) use the behavior intelligence and forensics around the event to help protect others. There has never been a more important time for a security provider—cloud or otherwise—to enable easy, sound, connected intelligence and behavioral analysis at a price point that is a worthy investment. This helps small businesses individually and collectively.

What Can Small Businesses Do to Protect Themselves?

Mobility and the cloud are here to stay, and it makes sense for small business to embrace these trends. They shouldn't do so without protections, however; this, too, makes good business sense.

Here are some recommendations for small businesses to protect themselves:

In General

At McAfee, we believe in “Security Connected,” from the chip to the cloud. As a part of the Intel Corporation, we explore behaviors from hardware to software and specialize in recognizing malicious intent before it can cause irrevocable harm. The keys are ensuring that cyber security is a boardroom issue of risk—even in the smallest of companies—and enabling companies to implement a connected, holistic approach that considers their networks an ecosystem of traditional, mobile and cloud devices and services.

This ecosystem concept is well described in the white paper from the National Protection and Programs Directorate within the Department of Homeland Security. Done correctly, networks can detect behaviors over time and begin to recognize, almost biologically, threats before those threats can overtake network functionality. Maturity models have shown that for any size organization, a wise design up-front leads to increasing security and decreasing cost over time. A connected, behavior-based approach enables network components such as phones, laptops and servers to communicate observed behavior amongst each other. Security can thus be man-

aged in real-time based on policy that adapts to current threats and provides resilience: the ability to run while under attack.

These intelligent systems are the result of innovation, and we need to help small business make wise—not expensive—choices to create a connected security foundation. As I mentioned in my prior testimony to this Committee, small business comprises over 95% of the U.S. business fabric. Small businesses have personal information stored, operational requirements and valuable intellectual property, and they need strong cyber security as much as large enterprises. Budget constraints in smaller businesses accentuate the need for a connected, ecosystem-based strategy in planning in security investment.

For Mobility

Like laptop and desktop PCs, today's mobile devices are complex platforms with multiple modes of communication, significant processing power and large storage capabilities. This by itself would make today's mobile devices subject to the same risks as business laptops; however, mobile devices have certain characteristics that make them even more vulnerable than PCs. Thus we recommend contracting with reputable service providers who take security seriously.

There are also precautions that small business owners can take to make sure their employees' devices are secure. Here's a partial list:

- Track and adaptively manage the devices that access your corporate network
 - Educate employees on their role in protecting the organization, its data, and brand against theft, loss or malicious use
 - Use passwords
 - Encrypt on-device data and email, and ensure mobile device data and email remote “wipe” capabilities
 - Have policy controls over memory card usage and encrypt that data.
 - Implement Bluetooth controls, such as installing firewalls and pairing with only known, trusted devices
 - Protect against Trojans with blacklisting and whitelisting applications
 - Have policy controls over web browser use and website access
 - Install a firewall on the mobile device to restrict inbound connections and prevent use of the mobile device as a bridge

The best security providers offer both targeted and comprehensive protections for the leading mobile device platforms. As mentioned earlier, Android devices are attacked much more than others. As an example of emerging mobile security software, McAfee last week announced an embedded control solution that is the industry's first to reside in the Android kernel. The control is embedded in the operating system rather than sitting at the user level, which is what makes it unique. As businesses depend more on mo-

mobile devices, security vendors will continue to innovate in the mobile space.

For the Cloud

Nine out of 10 businesses cite security as the top obstacle to cloud adoption, according to International Data Corporation (IDC). Yet small businesses can take advantage of cloud computing safely with some precautions upfront. These include making sure they are outsourcing to a cloud provider that can ensure robust security. We recommend that cloud providers contract with a third-party security vendor, offering the most up-to-date protections for the most recent—and emerging—threats.

But there are steps small business owners can take before even getting data to the cloud provider. You can think of these practices as building a secure bridge to the cloud. Here are a few recommendations:

Discover and classify data in the organization before it even leaves to go to the cloud

Before even beginning to consider what type of data should or should not be moved to the cloud, a business must first understand what data it has, where it resides—and more importantly—the value or sensitivity of the data. Only when there is a complete inventory of the data can an organization begin to classify the data to build the appropriate policies to protect it and then enforce policies while data travels both within and outside the organization.

These policies can be kept simple, but they should be in place to enable cyber security to be managed as a risk mitigation tool and business enabler for small business.

Secure the primary channels of traffic that move data to and from the cloud

These channels include email traffic, web traffic (including mobile), and authentication traffic (making sure users are who they say they are, and that they are authorized to access the data).

McAfee and other comprehensive security vendors offer cloud security platforms that are very effective at managing these tasks.

It's also possible for small businesses to get their security virtually—whether or not they are outsourcing their IT. Again, we and other security vendors offer security via a third party, or “the cloud,” and this can be a cost-effective way for small businesses to get optimum security without having to manage everything themselves.

What the Private Sector Can Do to Help Small Businesses

In addition to providing security for mobility and the cloud, the security and IT industries need to keep their focus on innovation in order to help small business and other organizations. At McAfee we feel strongly that the path forward is for security to be integrated into products at the beginning, for disparate islands of secu-

urity to be connected, and for security vendors to offer real-time situational awareness of threats.

Security features are not as effective when they are glued onto systems as an afterthought. Rather, cyber security must be integrated into equipment, systems and networks at the very start of the design process. Security must be embedded in a product or network element so that it becomes an integral part of the product's or element's functioning. Products must also be built to communicate with each other—exchanging information in real-time about what each product is seeing on the network to create the behavioural knowledge throughout the network ecosystem. This design-level approach is not only more effective; it is less cumbersome and less expensive than trying to lock down systems that are inherently insecure. This approach also provides tremendous cost savings for small businesses, because the products and services that enable the business have more native security and lead to a safer infrastructure with less need for additional expenditures.

McAfee and Intel create and support these Security by Design and Security Connected approaches. Today's attackers now can be stopped below the machine's applications layer—and even below the operating system. McAfee and Intel are working together to change the security paradigm to dynamically and adaptively protect systems against attacks at the core of computing, and to provide proactive defenses in real-time, making networks intelligent enough to prevent malicious instructions from reaching their targets—instead of requiring those targets to be vaccinated using signatures.

We also believe that as a security industry we must unify, simplify, and strengthen the way we provide security. We need to provide a framework for integrating potentially disparate technologies—building bridges between security islands to close coverage and technology gaps. This is the rationale for McAfee's Security Connected platform. With cyber security integration, security companies and their small business customers will be able to quickly and comprehensively detect and deter threats.

And having real-time visibility into emerging threats and a comprehensive view across the threat landscape is a powerful means of defeating cyber incursions. One robust technology that enables this real-time global visibility is called Global Threat Intelligence. With Global Threat Intelligence, millions of sensors scan the Internet across the globe and feed back real-time data on threats. This data is instantaneously correlated and fed back into security products, delivering real-time protection to customers, as we identify and block malicious files, Internet protocols and web addresses. With even more threat data from more security organizations fed into this network, customers would get even more comprehensive visibility into the quickly changing patterns of infestations and could take immediate steps to counter them.

What Government Can Do to Help Small Business: Enable Information Sharing

It's hard to overstate the importance of being able to share threat information between the private sector and the government. There

are several initiatives that can facilitate this process, and I'll discuss two of them: an information sharing bill and an information sharing mechanism available to large business known as ISACs, or Information Sharing and Analysis Centers.

An Information Sharing Bill - Rogers/Ruppersberger

During the last Congress and again this year, House Intelligence Chairman Mike Rogers (R-Michigan) and Ranking Member Dutch Ruppersberger (D-Maryland) introduced the *Cyber Intelligence Sharing and Protection Act*, also known as CISPA. The bill would facilitate the sharing of cyber intelligence between the government and the private sector. Significantly, the bill would offer liability protections for private entities sharing cyber threat information in good faith. Ensuring that sufficient privacy protections are baked into this bill will help cement the broad consensus necessary to make this proposal a legal reality.

An Information Sharing Construct - ISACs

While we definitely need legislation for robust information sharing, the government has endorsed and the private sector has put in place several Information Sharing and Analysis Centers, or ISACS. These ISACS, which are organized by sector, provide a specific mechanism for sharing cyber threat data.

Small businesses have neither the budgets nor the cyber experts to participate in a traditional ISAC. Indeed this Committee might consider the merits of conducting a study or holding a hearing on this matter to develop policy proposals to enable deeper small business community participation in the ISAC community. As we know, small businesses represent 99.7% of all employer firms and employ about half of all private sector employees, according to the Small Business Administration. We need to find a way to include small business in our nation's security paradigm—and that includes information sharing.

The National Cyber Forensics and Training Alliance (NCFTA) is one example of successful information sharing. Small businesses need the intelligence that such collaborations provide, and perhaps the small business community could leverage the information sharing agreements in the NCFTA so that collectively they could better protect the U.S. small business fabric, and thus our economy.

Thank you for the opportunity to address the subcommittee. I will be happy to answer any questions.



March 20, 2013

Honorable Sam Graves
Chairman
U. S. House of Representatives
Committee on Small Business
Washington, D. C. 20515

Dear Mr. Chairman:

Secure networks are crucial to America's national security and economic development. Your interest in ensuring that America's small businesses are protected from cyber attacks is timely and appreciated.

NTCA–The Rural Broadband Association (NTCA) represents rural community-based telecommunications providers. As you know, our members help put rural Americans on an equal footing with their urban neighbors by providing broadband and other telecom services in areas that large companies will not serve. Rural telecom providers are a critical link in the nation's telecommunications network, serving 40% of America's land mass containing approximately 7% of its population. Rural providers have relied on the Universal Service Fund (USF), intercarrier compensation (ICC) and Rural Utilities Service (RUS) loans to accomplish this mission, and they have an admirable track record of efficiently leveraging every resource available to them. Rural carriers are small businesses that help other small businesses startup and grow by providing broadband and other advanced telecommunications services that are essential to doing business today.

While it is essential that the public and private sectors work together on securing America's critical infrastructure, we are very concerned with the prospect of new unfunded mandates on our sector, which already faces significant uncertainty as the Federal Communications Commission imposes new cuts, caps, and constraints on USF and ICC cost recovery mechanisms that are essential to investment and operations in rural areas. The protracted climate of uncertainty surrounding the USF and ICC mechanisms has ground rural telecommunications infrastructure investment to a halt, meaning many Americans will not receive the robust and affordable broadband service that is essential to their safety and economic livelihood. When rural telecom investment is sidelined, this will undermine small businesses in rural areas that leverage these critical connections to share ideas and reach new markets. It is crucial that any new cybersecurity initiatives not further burden rural telecom providers at a time when they already face significant challenges in the form of regulatory uncertainty.

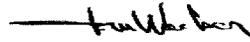
America's small rural communications providers have always displayed a strong commitment to the interests and needs of the consumers and communities they serve, while simultaneously

planning for, and appropriately reacting to, both potential and actual emergencies and threats involving their infrastructure and services. Our members are deploying all manner of cyber defenses according to the needs and vulnerabilities of their various networks, and NTCA is encouraging and assisting them in this effort through training and development. Rural providers are experts at “doing a lot with a little,” and many already employ personnel with cyber expertise who handle other duties as well.

We can achieve the twin aims of secure networks and robust economic growth if government and industry work toward a solution that helps make businesses aware of the range of cyber threats they face and the options available for defending their assets so each business can tailor a solution that best fits their unique situation. Rural, community-based telecommunications providers are eager to work with fellow providers, other small businesses, and the government to share threat information and develop cybersecurity best practices that ensure that Americans can confidently rely on stable and secure networks. Indeed, NTCA is already partnering with industry and government through the Communications Sector Coordinating Council, which facilitates the coordination of telecommunications sector activities and initiatives designed to improve physical and cyber security of the critical infrastructures and related information flow within the sector, cross-sector and with DHS.

NTCA is available to provide information and insight to ensure that any new cybersecurity law or policy enhances the online experience for all Americans. Thank you for your thoughtful deliberation on this important matter.

Sincerely,



Tom Wacker
NTCA–The Rural Broadband Association
Vice President of Government Affairs



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

National Association of Federal Credit Unions | www.nafcu.org

March 20, 2013

The Honorable Chris Collins
Chairman
Subcommittee on Health and Technology
Committee on Small Business
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Janice Hahn
Ranking Member
Subcommittee on Health and Technology
Committee on Small Business
U.S. House of Representatives
Washington, D.C. 20515

Re: Tomorrow's Hearing on Protection from Cyber-Attacks

Dear Chairman Collins and Ranking Member Hahn:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing our nation's federal credit unions, I am writing in regards to tomorrow's hearing entitled "*Protecting Small Businesses Against Emerging and Complex Cyber-Attacks*." As the Subcommittee addresses this important issue, we urge you to not overlook the significance of securing personal and financial data from cyber-attacks.

As small businesses themselves, credit unions are acutely aware of the value of reputation in the marketplace. With so many options available to consumers, a small business's reputation can be its greatest asset. Now more than ever it is important for small businesses to take proper action to ensure that their reputations remain intact. One of the best ways they can do so is by gaining and maintaining the trust of their clientele. A breach from a cyber-attack resulting in the compromise of consumer data is a growing threat and can devastate a business's reputation.

The risk of a data breach is serious problem for both consumers and businesses. Every time a consumer chooses to use a plastic card for payment at a register or the accounts attached to them for online payments, they are unwittingly put at risk. Many are not aware that their financial and personal identities could be stolen, or that fraudulent charges could appear on their account, damaging their credit scores and reputations. These consumers trust that entities collecting this type of information will at the very least make a minimal effort to protect them from such risks. Unfortunately, this is not always true.

As you may be aware, financial institutions, including credit unions, bear a significant burden as the issuers of payment cards used by millions of consumers. Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud related losses, many of which stem from a negligent entities failure to protect sensitive

financial and personal information, or the illegal maintenance of such information in their systems. Moreover, as many identity thefts have been attributed to data breaches and identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to a minimum standard for protecting such data.

There have recently been several large-scale data breaches, such as the ones at Sony and Michael's Inc. The aftermath of these breaches demonstrates what we have been communicating to Congress all along: credit unions and other financial institutions, not retailers or other entities, are out front protecting their members and consumers in picking up the pieces after a data breach occurs. It is the credit union or other financial institution that must notify their account holders, issue new cards, replenish stolen funds, change account numbers, and accommodate increased customer service demands that inevitably follow a major data breach. The negligent entity that caused these expenses by failing to protect consumer data loses nothing, and is often undisclosed to the consumer.

NAFCU is pleased to see the Subcommittee begin to debate cybersecurity, and urge you to consider efforts to protect consumers from cyber-attacks that compromise their financial and personally identifiable information as part of this debate. The issue of data security is one of the priorities outlined in NAFCU's five-point plan for credit union regulatory relief, and recommend examination of the following issues for inclusion in any bill that seeks to address cybersecurity and data security issues:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.
- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to Gramm-Leach-Bliley that covers retailers, merchants, and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the Gramm-Leach-Bliley Act.
- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to by providing their personal information. NAFCU believes that this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant, but would provide an important benefit to the public at large.
- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent

transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions to the list of those to be informed of any compromised personally identifiable information when, associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated, so consumers are aware of those that place their personal information at risk.
- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.
- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the merchant or retailer who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information, but sustained a violation regardless. The law is currently vague on this issue, and NAFCU therefore asks that this burden of proof be clarified in statute.

NAFCU would also note that there are critical homeland security considerations at stake when deliberating data safety issues. Weaknesses in the protection of consumer information can and have helped terrorist networks and organized crime groups fund their operations. NAFCU believes it is critical that these simple changes be enacted so as not to facilitate the financing of operations that threaten not only the financial stability, but also the livelihood of millions of Americans.

Thank you for your kind attention to this important matter. We appreciate this opportunity to voice our concerns, and look forward to working with you as you examine this issue. Should you have any questions or need additional information, please do not hesitate to contact myself or NAFCU's Associate Director of Legislative Affairs, Chad Adams, at 703-842-2265 or cadams@nafcu.org.

Sincerely,



Brad Thaler
Vice President, Legislative Affairs

cc: Members of the Subcommittee on Health and Technology