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 here 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 those 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 attacks 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 impeding 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.