STATEMENT FOR THE RECORD

STEVE GROBMAN, SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, MCAFEE, LLC

BEFORE THE U.S. HOUSE OF REPRESENTATIVES TASKFORCE ON ARTIFICIAL INTELLIGENCE, FINANCIAL SERVICES COMMITTEE

ARTIFICIAL INTELLIGENCE AND THE EVOLUTION OF CLOUD COMPUTING: EVALUATING HOW FINANCIAL DATA IS STORED, PROTECTED AND MAINTAINED BY CLOUD PROVIDERS

OCTOBER 18, 2019, 9:30 AM | 2128 RAYBURN HOUSE OFFICE BUILDING

Chairman Foster and Ranking Member Hill, it is an honor to take part in this hearing on the evolution of cloud computing and its implications for securing the financial services sector from cyberattacks. Along with governments, telecommunications, and energy and water resources, the financial services sector is critical to the daily functioning of our economy and our overall security. Thank you for investigating ways to better protect this vital segment of our digital economy as such innovations as cloud computing and artificial intelligence change the way the financial services sector manages its information technology systems.

As McAfee's Senior Vice President and Chief Technology Officer, I set the technical strategy and direction to create technologies that protect smart, connected computing devices and infrastructure worldwide. I lead McAfee's development of next-generation cyber defense and data science technologies, threat and vulnerability research, and internal CISO and IT organizations. Prior to joining McAfee, I dedicated more than two decades to senior technical leadership positions related to cybersecurity at Intel Corporation, where I was an Intel Fellow. Participating in the public policy debate on how the public and private sectors can work together to protect our nation's critical infrastructures has and continues to be a professional and personal passion of mine.

MCAFEE'S COMMITMENT TO CYBERSECURITY

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates enterprise and consumer solutions that make our world a safer place for the benefit of all. Our holistic, automated, open security platform and cloud-first approach to building security solutions allow all security products to coexist, communicate, and share threat intelligence with each other anywhere in the digital landscape. Our customers range from government agencies to all sizes of businesses and millions of home users.

We are committed to solving the most challenging cybersecurity challenges in our industry, particularly the interoperability challenge. For too long, organizations have not been able to reap the full value of the cybersecurity tools they have purchased from vendors because of the lack of interoperability, the expense of integration, and the potentially valuable data locked

away from sight in proprietary silos. According to the industry analyst firm Enterprise Strategy Group, organizations use, on average, 25 to 49 different security tools from up to 10 vendors, each of which generates siloed data. Today, integrating security products into an established operational environment can be extremely resource-intensive, time-consuming and costly, all at the expense of hours that could be better spent hunting and responding to threats. What's needed is for cybersecurity companies to share "the plumbing" – the foundation, or common platform, upon which cybersecurity tools are built.

At McAfee, we're leading the drive toward interoperability and data sharing across the cybersecurity landscape. Together with IBM Security, McAfee recently launched the Open Cybersecurity Alliance (OCA) to bring together a large number of like-minded global cybersecurity vendors, end users, thought leaders, and individuals interested in fostering an open cybersecurity ecosystem, where products from all vendors and software publishers can freely exchange information, insights, analytics, and orchestrated response. OCA's purpose is to develop and promote sets of open source common content, code, tooling, patterns, and practices for interoperability and sharing data among cybersecurity tools. This partnership will enhance the ability of both the public and private sectors to keep up with and overtake cyber hackers, who are also leveraging such innovations as cloud computing and artificial intelligence to improve their own capabilities.

To solve the industry's most challenging issues and achieve interoperability across the cybersecurity landscape, we also must employ the best and the brightest in the field. This means developing and retaining a diverse and inclusive workforce.

MCAFEE'S COMMITMENT TO DIVERSITY AND INCLUSION

While we recognize there is still more to do, we're proud to describe the strides we're making at McAfee to promote diversity and inclusion. We believe we have a responsibility to our employees, customers, and communities to ensure our workplace reflects the world in which we live, and we're implementing programs to increase diversity and inclusion among our ranks. This business model is essential to the cybersecurity industry's success. Studies show time and again that diverse perspectives and human experiences lead to more creative approaches to solving challenges, and we know that inclusive teams deliver the best results.

Our most recent accomplishment was to audit our global employee base to examine pay parity. In April 2019, we achieved pay parity, making McAfee the first pureplay cybersecurity company to do so. It required an investment of $4 million to make salary adjustments on April 1. We'll continue to adjust the pay gap and uphold pay parity with annual analysis.

In 2018, our first year as an independent company, we released our first Inclusion and Diversity Report, which demonstrated our commitment to building a better workplace and community. In 2018, 27.1% of all global hires were women, and 13% of all U.S. hires were underrepresented minorities. In June 2018, we launched our "Return to Workplace" program for men and women who have paused their career to raise children, care for loved ones, or serve their country. This

12-week program offers the opportunity to reenter the tech space with the support and resources needed to successfully relaunch careers. As a result, 80% of program participants were offered a full-time position at McAfee.

Now, I'd like to address the Committee's central concerns: the effects of cloud computing and artificial intelligence (AI) on the security and integrity of the financial services sector.

THE FINANCIAL SERVICES SECTOR'S MIGRATION TO THE CLOUD

Financial services organizations are migrating to the cloud to reduce complexity, cut costs, and focus their capabilities on delivering financial services to their customers. According to the research firm MarketsandMarkets, the finance cloud market will grow at a compound annual growth rate (CAGR) of 24.4% to $29.47 billion by 2021.

Cloud adoption is ultimately about delegating certain functions to allow enterprises to focus on their core competencies. This includes:

- Infrastructure as a service (IaaS), delegating capabilities that would traditionally be run in a private datacenter
- Platform as a service (PaaS), delegating the technology building blocks and services that can be used to build solutions, and
- Software as a service (SaaS), delegating a complete application stack

With these "as-a-service" offerings, cloud providers usually take on the implementation of the service, which provides unique advantages, including:

- Faster innovation cycles
- The ability to optimize cost structure by having the opportunity to evolve and optimize an implementation of technology, as long as customer interfaces remain consistent
- Enhanced supportability of sophisticated solutions, as implementation and operational complexity is assumed and abstracted by their cloud providers

The technology at scale delivered to customers by cloud providers allows for very specific expertise that would not "scale down" to smaller organizations. This allows smaller organizations, including small businesses and organizations outside the technology industry, to access advanced technology that traditionally would be available only to large organizations or organizations that invest heavily in a highly technical employee base.

Cloud providers generally practice strong cyber hygiene, as they are executing at scale. For instance, all public cloud providers patched for the Spectre Meltdown vulnerability within days, while private datacenters had significant variability and, in many cases, did not have patches applied months after the vulnerability was disclosed. For example, AWS quickly disabled CPU microcode for the vulnerability.

Despite the benefits to organizations of moving to the cloud, there are also challenges. Organizations that transfer their IT capabilities to cloud providers have less visibility into their architecture and operations, given the delegation of "trust" to the provider. Any cyber vulnerabilities can impact multiple tenants. For example, a breach in a cloud provider's architecture can place multiple organizations' data at risk. An analogy I like to use is that traditional, on-premise computing is a lot like an automobile, and cloud computing is a lot like an airplane. While an airplane is safer than an automobile given its more advanced technology, when a failure does occur, the impact can be catastrophic.

Today, almost all organizations use multiple cloud providers. This trend is becoming the norm in the financial services industry, as it is in virtually all industries. Because of this, organizations need scalable monitoring and management solutions that allow common policies and operational capabilities to be applied to their multiple providers. In order to facilitate this, it is critical that programmatic interfaces are made available from the cloud provider or service to monitor solutions that can enable abstraction of monitoring, vulnerability detection, and management. This functionality is known as a Cloud Access Security Broker (CASB) and is a critical new class of application that is rapidly being adopted as a means to manage and secure diverse cloud environments.

Even with the addition of these types of advanced cloud cybersecurity tools, there are other cybersecurity issues related to the cloud, such as when an organization moves traditional computing to IaaS. Cloud environments add new complexity that a new workforce will need to understand in order to secure. As these public clouds are often accessible via public or private networks, organizations need to ensure that access is not accidentally granted to unauthorized entities via misconfigurations. Additionally, the control and configuration paradigms in cloud environments differ from traditional computing, and this could require the retraining of the existing IT workforce.

Another security issue with cloud is the use of unauthorized cloud applications, or Shadow IT, which often results when employees or small teams within a business attempt to work more efficiently by using IT resources outside of those sanctioned by the IT department. They run capabilities in a public cloud without IT controls, creating severe security risks and leading to exposure of an organization's technology and data. Shadow IT includes execution of rogue virtual machines in public IaaS as well as unsanctioned use of SaaS applications such as Microsoft 365, Gmail, GitHub and Source Forge (the top 4 according to McAfee's cloud team analysis). Given that a typical organization will access on average 120 such services, it is critical to understand and control legitimate, or sanctioned, applications from the unsanctioned applications. One of the challenges is that not all SaaS applications, including storage or collaboration services, are created equally, and without guidance from the chief information officer (CIO) or IT team, employees might opt for an application that has comparatively lax security controls, claims ownership of users' data, or is hosted in a country that tolerates, or even encourages, cyber-crime directed toward Western allied companies, particularly those in the financial services sector.

In sum, the financial services sector's use of cloud can provide many advantages – as long as security concerns continue to be top of mind, as they have been all along for this sector.

THE FINANCIAL SERVICES SECTOR'S USE OF ARTIFICIAL INTELLIGENCE

Financial services firms are using AI and machine learning to enable advanced analytics to better serve and protect customers. According to a study by Autonomous in an 84-page report on AI in the financial industry, the industry's slice of this massive AI pie represents upwards of $1 trillion in projected cost savings. By 2030, traditional financial institutions can save 22% in overall costs with AI: $490 billion in front office (retail functions), $350 billion in middle office (risk management and profit/loss calculations), and $200 billion in back office (settlements, regulatory compliance, and accounting).

For cybersecurity, artificial Intelligence is without doubt the new foundation for cyber defense. The entire industry is tapping into the tremendous power this field offers to better defend our environments. AI enables better detection of threats beyond what we've seen in the past. It helps us out-innovate our cyber adversaries. The powerful ability of AI-based automation is key to addressing our talent shortage. AI means we can now delegate many tasks to free up our human security professionals to focus on the most critical and complex aspects of defending our organizations. AI enables us to evaluate data "at scale," and it enables us to find the so-called "needle in a haystack of needles" that has challenged our field for the last decade.

Yet it's important to understand that the cybersecurity industry is very different from other sectors that use AI and machine learning. To start, in many other industries, there isn't an adversary trying to confuse the models. AI is extremely fragile; therefore, one focus area at McAfee is Adversarial Machine Learning, where we're working to better understand how attackers could try to evade or poison machine learning models. We are developing models that are more resilient to attacks using AI techniques. As an industry, we need to be realistic about the immense power of AI-based technology. While it solves a host of problems for us – including making our defenses stronger – AI also intensifies the capabilities of our adversaries.

Bad actors can use AI to identify the most vulnerable victims, automate phishing, and evade detection. AI improves their ability to execute their attack and enables the creation of content to be used in social engineering and information warfare, as occurred in the 2016 election. One of the most troubling evolutions of AI-based information warfare technology is deep fake video generation, which can create realistic video of events that did not occur. These and many other adversarial uses of the technology can and will occur, putting our democracy and civil society at increased risk.

FINANCIAL SERVICES AND CLOUD PROVIDER CYBERSECURITY PREPAREDNESS

Our financial services and cloud provider customers and partners tell us the three biggest challenges they have are 1) dealing with conflicting regulations, 2) a constantly changing and

evolving technology landscape, and 3) the growing sophistication of cyber attackers. They also have to deal with cybersecurity tools that often don't work well with each other. The lack of interoperability among cybersecurity solutions limits their ability to exchange threat data on a rapid basis and creates seams of access for hackers.

The National Institute of Science and Technology's (NIST) Cybersecurity Framework provides a valuable roadmap for organizations of all sizes to evaluate their risk, see where their vulnerabilities are, and improve their cybersecurity capabilities. We commend the U.S. government for enabling this partnership that has improved the security posture of many critical infrastructure industries, including financial services and cloud providers. Likewise, compliance with Europe's General Data Protection Regulation (GDPR) is having a real impact on improving both the security and privacy practices of those U.S. companies that collect data from European Economic Area residents. GDPR protects personal data in both administrative and technical manners, requiring anyone handling the data to record their uses and make sure that they are securing the data.

Most major financial institutions are prepared for major cyberattacks with the potential to produce system-wide failure, in part due to the regulatory oversight of both the Bank Service Company Act (BSCA) and Gramm-Leach-Bliley Act (GLBA). Financial services companies have plans in place and are engaging actively in cyber sharing groups, in collaboration with the Department of Homeland Security (DHS), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve. They know what they'll do first to identify and respond to a nation-state attack against economic critical infrastructure.

Overall, third-party cloud providers also have a strong cybersecurity track record, due to their technical expertise and financial resources. These companies have solid plans in place to respond to cyberattacks, as evidenced by their commitment to aligning to the NIST Cybersecurity Framework. Cloud providers are also active in several public-private partnerships, such as the DHS Information Technology Sector Coordinating Council (ITSCC) and the National Telecommunications Advisory Committee (NSTAC), which further buttress their cybersecurity capabilities.

Cloud providers are less regulated than their counterparts in the financial services sector, given the general consensus among policymakers that overly prescriptive cybersecurity regulations would stifle the ability of internet companies to maintain their rapid rates of innovation. However, if service providers perform services for a bank, the BSCA gives federal regulators the ability to examine and regulate third-party vendors, including cloud providers. GLBA enables federal agencies to establish appropriate standards for financial institutions to ensure the security and confidentiality of customer information. Federal regulators have a legitimate interest in seeing that IT and cybersecurity services provided by cloud providers to financial institutions are well done to ensure confidence in our nation's financial services infrastructure.

Due to the increasing role cloud providers are playing in managing the IT capabilities of critical infrastructure companies (financial services, energy, telecommunications), policymakers should be exploring ways they can enhance the cybersecurity readiness of these companies.

CONCLUSION

The largest and most sophisticated companies in the financial services and cloud sectors are at the top of their game in cybersecurity, particularly in comparison to smaller companies and other industry sectors that have lagged in investing in the strategies, processes, people and technology needed to keep up with new threats and attackers. While innovations in both cloud and artificial intelligence are and will continue to enhance the cybersecurity of these sectors, these same innovations will progressively enable cyber hackers.

It is appropriate for policymakers to review the security capabilities of both financial services and third-party cloud providers, as both play vital roles in maintaining the safety and integrity of our nation's economy. However, policymakers should be wary of imposing additional cybersecurity mandates and regulations on the private sector, given the strong possibility that out-of-date, check-the-box compliance rules could be the result. Policymakers should first support voluntary collaboration and the use of industry-supported standards and best practices such as the NIST Cybersecurity Framework. When appropriate, existing cybersecurity rules for highly regulated critical infrastructure industries should be updated to reflect the rapid speed of innovation.

Thank you for the opportunity to discuss these issues with the Committee. I look forward to answering your questions.