Statement of

Nicholas A. Oldham

Counsel

King & Spalding LLP

before the

U.S. House of Representatives

Small Business Committee

April 20, 2016

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for the opportunity to appear before you today.[1]

I have been involved in cyber issues for many years—as a former federal prosecutor at the U.S. Department of Justice and now as an attorney with King & Spalding. In my practice, I counsel clients, both large and small, on the legal aspects of cybersecurity risk management.

Today, I focus my testimony on the cybersecurity landscape for small businesses, and on three areas of particular concern—the cybersecurity education gap, the need for cybersecurity initiatives to be calibrated for small businesses, and the need to clarify and simplify the current regulatory environment.

Background

We are living in exciting times. Digital assets and connected systems have generated new products and services, redefining how business is conducted and services delivered. But the truth is that we are only at the beginning of the beginning when it comes to understanding the implications of our reliance on this interconnectivity and the dangers that cyber threats present.

Our *interconnectivity* is growing at an astonishing rate, with some estimates that there will be as many as 50 billion devices connected to the Internet by 2020. As a result, we are marching toward an infinitely connected world: always online, our information moving from network to network and device to device.

Partly as a result of this interconnectivity, businesses are gathering and utilizing an ever-growing amount of information to improve their business practices and better serve their customers. Today, every online communication, transaction, and anything else you can think of can be captured and stored, and then transmitted electronically anywhere and at anytime. This

[1] The views and opinions expressed in this statement are mine and do not necessarily reflect the views or opinions of King & Spalding or any of its clients.

interconnectivity, especially including the Internet of Things, holds tremendous promise for consumers and companies.

It also creates new challenges in terms of *cybersecurity* because anything connected to the Internet can be hacked. Cyber threats vary from the technologically sophisticated to the surprisingly low tech methods such as “social engineering” and spear phishing. A recent RAND Corporation study found that over a quarter of American consumers received a notice that their data was stolen within the past year alone. Forbes recently reported that cyber-attacks cost businesses an estimated $400-500 billion per year, and because many cyber-attacks are not reported, it is believed that the real number is significantly higher. These reports underscore the significant costs of preparing for, responding to, and recovering from cyber incidents.

Where do small businesses fit in this landscape? The interconnected world enables small businesses to develop new products and services and compete across the globe. However, growing cyber threats present greater challenges to the same small businesses, which can lack the tools needed to effectively cope with the growing danger.

Small businesses are appealing targets. Small businesses often have more digital assets than individual consumers, but their resources may not allow for the same level of focus on cybersecurity as large companies.

Businesses of all sizes need adequate cybersecurity education, but it can be difficult for small businesses to find the right information and training.

Small businesses also often feel the impact of cyber threats differently than large companies. Establishing effective cybersecurity and incident response mechanisms is complicated and can be expensive. When any business implements mitigation measures or responds to a cyber incident, it can lose significant time and money. The costs can sink a small

business. Small businesses get burned at both ends—they are less likely to have the resources to prevent breaches and they also may have fewer resources to respond to those breaches.

From Cyber Threat Awareness to Cyber Risk Management

In June 2011, various Committees in both the House and Senate held hearings regarding data breaches at Sony and Epsilon Data Management. In March 2012, then-FBI Director Mueller gave a now famous speech at the RSA Conference in San Francisco. His oft repeated quote is that "there are only two types of companies: those that have been hacked and those that will be." These events were key, early moments that helped raise awareness of cyber threats. We have much farther to go in terms of awareness and, perhaps more importantly, companies need to move from awareness to expertise in managing the new normal of cyber threats.

As a lawyer, I do not manage corporate networks or conduct vulnerability testing. Rather, I believe that cybersecurity is as much a people and process issue as it is a technical issue. I focus on the people and process side of the equation, addressing the legal and business cybersecurity risks faced by companies including cybersecurity risk governance, compliance, and incident response processes. I also help companies comply with breach notification obligations, interact with various regulators, and manage their responses to regulatory actions or litigation. The legal and business costs, including compliance costs, drain on employee time and morale, and reputational damage, can be significant.

The Cybersecurity Education Gap

Before spending precious resources on increasing cybersecurity measures, it is natural for small businesses to carefully weigh the cost of putting new measures into place versus the cost to the company of the inevitable cyber incident if it does not take action. Because of the enormous potential costs of a cyber incident, which is difficult to quantify, companies may find that it is far

more expensive to not implement basic security measures. The problem here is that there is a cybersecurity education gap: small businesses may not be able to get the information they need to properly assess and mitigate these costs.

Bridging this education gap can be difficult for small businesses, especially those that lack the resources to hire specialized employees or cybersecurity experts. Basic resources are available online, but even where they provide crucial information, they can be difficult to find, are rarely updated, or are inadequate.

On the legal compliance front, the Federal Trade Commission recently released a new web-based tool for developers who make health-related apps. The tool asks developers a series of 10 high-level, yes or no questions related to their apps covering topics such as the apps' functions, data they collect, and the services they provide. Then, based on the answers to the high-level questions, the tool identifies four potentially applicable federal laws. While useful as a starting point for introducing and orienting developers and other healthcare industry players to the legal thicket affecting health apps, the tool provides high-level guidance on the basics of only a few relevant laws.

The FTC's tool is one example of an approach geared toward educating the public on legal compliance. The tool is somewhat promising, but does not cover all relevant laws and does little more than point the developers to summaries of the relevant language. This approach, however, could go a long way toward helping small businesses stay informed on cybersecurity legal best practices, provided such tools are expanded to cover a broader set of laws and give more specific, timely information.

In many ways, cyber threats have analogs to traditional crime. Ransomware is cyber extortion, spear phishing is nothing more than a con artist taking advantage of the ubiquity of e-

mail. Hackers, moreover, are like burglars. They use their “gloves,” “dark clothes,” and “tools” to get inside a network, stealing digital loot along the way. In the traditional crime scenarios, small businesses would likely call the local police department for best practices in preventing these crimes or responding to them. In the digital crime scenarios, there is no one logical place to call. The government may have a role in bridging the cybersecurity education gap by encouraging the development of cybersecurity education resources and connecting them to those who need them in the private sector.

Existing Programs Are Not Geared Toward Small Businesses

Many of the cybersecurity initiatives receiving the most attention are not necessarily tailored to take into account the realities of small business owners. Standards seem to be coalescing around the NIST Cybersecurity Framework in some areas, for example, which is a promising development. This has the potential for simplifying the landscape for small and large businesses alike.

The current iteration of the NIST Framework, however, is not particularly geared toward the needs of small businesses. The Framework itself can be difficult and expensive to understand and implement regardless of business size, and until it is better tailored to small businesses, for some of them it may just be one more program that they cannot afford to keep up with. Perhaps more importantly, a small business might become subject to a cybersecurity framework by virtue of its contractual relationship with a partner that passes its cybersecurity obligations through its supply chain. In this case, the small business might agree to obligations under the cybersecurity framework without the same level of vetting it might undertake if it were adopting the framework from scratch, and thereby inadvertently expose itself to significant liabilities and expose itself and its partners to significant cyber risks.

While good cyber hygiene is important, to improve the NIST Framework, and similar programs and policies, the government should make a serious effort to increase the involvement of small business owners in all phases of the legislative and rule-making process. Until small business concerns are fully baked into these standards, they could face serious challenges of adoption.

The Current Regulatory Regime Is Difficult to Navigate

The current regulatory regime for cybersecurity presents additional difficulties for small businesses, who will inevitably struggle to determine both (1) what cybersecurity measures they are required to enact, and (2) when a breach or attack does occur, what procedure the law requires them to follow.

There are currently 51 different state or territory laws that pertain to the notifications a company that has been the victim of a data breach must provide to its customers. They are inconsistent with each other in a variety of ways. Additionally, several states have enacted laws requiring companies to put "reasonable security measures" in place. What "reasonable" means in this context is evolving and can differ by jurisdiction and industry. I have seen a growing number of federal regulatory agencies stepping into the same space.

The cost of ensuring compliance with laws for any company is enormous even before taking into account the cost of litigation and reputation damage if a breach does occur. Small businesses in particular are vulnerable to these costs because they can consume a much larger proportion of their available funds. Small businesses would benefit from a public sector approach that lowers the cost of compliance and the cost of implementing best practices.

In short, there is a need to clarify and simplify what companies must do. Because of the complicated and evolving landscape, the on-the-ground expertise of the private sector must necessarily play an important role in these efforts.

Thank you for the opportunity to testify before you today. I look forward to your questions.