STATEMENT OF

GUILLERMO CHRISTENSEN
PARTNER
DATA SECURITY & PRIVACY/GOVERNMENT INVESTIGATIONS
ICE MILLER LLP

before the

SUBCOMMITTEE ON

COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENATIVES

MAY 28, 2020

Chairman Cleaver, Ranking Member Hill, Chairwoman Waters, Ranking Member McHenry, members of the Subcommittee and staff, thank you for inviting me to join you today for this roundtable. As an aside I would note that the COVID-19 pandemic is certainly taking us in interesting directions – the last time I recall being a participant in a Congressional hearing was while still serving in the intelligence community and, as is the norm, it was a closed meeting involving classified matters, where the presence of internet enabled cameras and microphones would have been frowned upon to say the least.

Today, we are having this roundtable in a highly dispersed, appropriately socially distanced setting that relies on the public internet infrastructure.

I confess that like most of you I am still getting used to this!

You have my biography but I'd like to give some additional context that I hope will help guide you in asking questions on issues that I may have insights on to benefit to you and your constituents. Although I am no longer in public service, one of the reasons I love my work is that it still very much involves helping to protect businesses and individuals from threats that we will touch on today.

Currently I am partner at Ice Miller, a law firm with a great history of over 100 years that has its roots in the Midwest. I work out of the firm's DC office, just down the street from the Capitol. Much of what I do as a lawyer is informed by my time as a public servant – I was privileged to serve as a CIA officer for many years and I later returned to public service with the Department of State, focusing on science and technology issues. Please note that my remarks today are my own, the do not necessarily reflect the views of Ice Miller or of any of our clients.

At Ice Miller I am involved in helping our clients deal with cybersecurity risks and protecting their data and their systems. I also assist clients with sensitive government investigations and with national security laws, such as high technology export controls and foreign investment reviews involving the Committee on Foreign Investment in the U.S.

On the data security side of things, our work spans what many of us in the field refer to as "left of boom" to "right of boom." I prefer to do as much as possible "left of boom" – which is the lower stress, less expensive and less damaging part of the spectrum. This means preparing clients for risks that we hope won't materialize, but knowing that being prepared even in that context is well worth doing. To paraphrase General Eisenhower, while plans are generally useless, planning is indispensable.

But, we also spend a lot of time on the "right of boom" dealing with the consequences of incidents, breaches and insider threats, and they are often catastrophic. This is especially so for small- and medium-sized businesses that we all know are so important not only to our economy but to psyche and morale as a country.

In the past decade, we have all become very familiar with cyber-attack headlines – words like ransomware, malware, data breach, phishing, hacking. Those words have a very dramatic meaning to the victims of cyber incidents and breaches. You need only ask a small business owner that is forced to use scarce cash to try to recover their computer system from old backups or to pay the extortion demand by an organized criminal group that is using ransomware with makes like NetWalker or BitPaymer. In many cases, the organized criminal group has developed a sophisticated, scalable business operation with significant revenues.

Tragically, many businesses are typically fighting that battle alone, with no allies, against a dangerous, well equipped enemy. My key point here is to underscore that this is increasingly looking more like a battlefield with no boundaries.

And this is a battlefield where the weapons are increasingly easy to get, develop, steal, share or rent. Earlier this year I was involved in a project sponsored by the Department of Homeland Security and the Director of National Intelligence that looked the proliferation of the tools we had seen emerging from nation states. Our study has many useful conclusions and I encourage you to use it for your benefit. The main take way is captured by a key word in the title – Commodification. A word that we chose after much deliberation to capture the concept that the tools and weapons of cybercrime, cyber espionage and cyber war are now becoming a commodity, not something exotic or hard to develop.

Where does the COVID-19 pandemic fit in all this? A few days ago I spoke to another audience on the question of the impact of the measures we have taken to mitigate the impact of the pandemic on national security.

On the negative side of the ledger is the significant disruption in private sector communications systems, networks, and practices from shifting our workforce overnight to working outside the corporate network. The analogy I drew on is what you might undertake in a military operation when confronted with an enemy that is using very secure communications to operate better than you. Rather than spend time and lots of effort to compromise their system to be able to read their messages, sometimes it is simpler to degrade that link with jamming, cutting fiber optic lines and push the enemy onto a less secure grid.

The real challenge in my view around COVID-19 and cyber is that is what has effectively happened to our entire internet communications. In the span of a few days, we shifted the majority of in-person business and government interactions that take place in offices, hall ways, around the water cooler or ping pong table and put them out on the wild wild web. We've essentially added to the huge trove of daily digital communications via email by digitizing those in-person discussions, using mostly excellent audio and video (all jokes about video conferencing aside). And this is coming from someone who routinely walks over to Alexa or Siri when I see them hiding in an office and unplugs them before I have a conversation involving anything of substance. And we're relying in many cases on home computers, personal laptops, outside the security of corporate networks.

This is far from a gloom and doom story. First, moving to "WFH" has kept a lot of Americans employed and mitigated the impact of the pandemic on our economy. But looking beyond that, it is massively accelerating the transition to a digital economy in the United States. This is a positive development. Humans always innovate more rapidly in times of war. This is not so different.

The challenge that all of us need to focus on is to keep moving toward a digital economy and infrastructure that is not going to be our Achilles heel. A nation that can pivot to "WFH" when needed, and do so seamlessly, has a real competitive advantage.

I look forward to discussing some of the areas where we need to prioritize our efforts on cybersecurity – such as widespread use of encryption, especially promoting end-to-end encryption; improved cooperation between law enforcement and the private sector; regulations that emphasize protecting the victims of digital crime; and programs that help companies to work together and scale the resources to defend themselves.

Thank you for your time.