Foreign Cyber Threats: Small Business, Big Target"

Introduction

Good afternoon and thank you Chairman Chabot and Ranking committee member Velázquez and all Small Business Committee members for the opportunity to testify on foreign cyber threats to American small business.

It is an honor to address members of this distinguished body, both as a small business owner and also as a citizen who notes that small businesses not only employ approximately 50% of the private sector workforce, but they also produce approximately 50% of the non-farming GDP in the United States. They are therefore a vital part economy and their well-being and the need to ensure their ability to operate in a transparent and secure environment is paramount.

My name is Justin Zeefe, and I am co-founder and Chief Strategy Officer of Nisos Group, a cybersecurity firm of former elite cyber operators and Special Forces officers from within the U.S. government. I, and each of my associates, have more than a decade of assessing and mitigating cyber risk to any system which, if compromised, could damage U.S. national security interests. These systems range from critical infrastructure to financial institutions and everything in between. We each observed, over recent years, a significant shift by foreign cyber threats increasingly toward private sector concerns. This evolution, magnified by our observation that the commercial sector is unprepared for the inbound threat, prompted us to bring our capabilities to industry.

It is an honor to speak to you today regarding the most significant present and near-term threat to the national small business economy – foreign cyber threats in the form of cybercrime. There are no shortages of statistics to this end – it is the fastest growing economic crime according to PWC, and is projected to cost the global economy $445 billion by the end of 2016, according to the World Economic Forum. In fact, according to McAfee, the well-renown security company, if cybercrime was a country, its GDP would rank 27th in the world – above Austria, Norway, and Egypt.

How would we collectively react if we knew that the 27th largest economy was absolutely dedicated to attacking our value? What if they were overwhelmingly directing their actions against small businesses? In fact, both of these statements are accurate. Symantec found in June 2015 that 75% of cyberattacks were directed at organizations with fewer than 2,500 employees – a dramatic increase from years prior. Not a week goes by that we don't read of a major data breach in the paper, with mention of what the attackers stole, and often how they managed to gain access.

Most voices and solutions in the field of cybersecurity address the 'what' and 'how' of the threat; yet without an intimate understanding of the threat actors – their motivations, vulnerabilities, capabilities and adaptability – the discussion is incomplete. Never in the history of mankind has there been an industry – illicit or otherwise – which could be addressed strategically without factoring in the players in the game. Cybercrime, and the threat it represents against small businesses and large alike, is no outlier.

This very thing – the 'why' – is a vital part of the equation which requires understanding the humans behind the threat and just as importantly, the vulnerabilities which these threat actors seek to exploit. By understanding the driving forces and motivations behind the threat actors, as well as the evolution of their tools, it is possible to narrow the gap between threat actor capability and the cybersecurity solutions in the marketplace.

Once we understand attacker motivations, it becomes easier to model future behavior from state-sanctioned or state-sponsored activity, and criminal enterprise – the source of almost all cyber incidents. Armed with these insights, only then should we deliberate legislative incentives, penalties, and the appropriate distribution of risk to aid – not hamper – small businesses.

The 'why'

So, why? Why do foreign cyber threats target small businesses? One word and one analogy are sufficient to encapsulate this trend. The word is 'profit' and the analogy is that like water or electricity, malicious hackers follow the path of least resistance. As larger organizations professionalized their defensive and reactive postures to cyber incidents, and as stolen data became less profitable due to a stricter regulatory and law enforcement environment, threat actors – in search of profit – turned their focus to targets which had neither the capacity nor the budget to address cyber threat. A positive feedback loop ensued, in which threat actors only became more dangerous as they adapted to the increasingly sophisticated target set.

The first and most significant evolution was the professionalization of the threat actor. What were only a few years ago best described as small bands of hackers who occasionally work together have, by virtue of their success, drawn the attention of traditional organized criminal elements. These groups, with many years of experience in the conduct of criminal enterprise, accurately assessed that cybercrime represented an opportunity for increased profit and decreased risk. Rather than trafficking in weapons, drugs or other contraband – activities dependent on physical items which thus present a significant risk of detection or interdiction – these groups of experienced criminals increasingly invest in individuals or groups whose cybercrime activities are both wildly successful and stealthy when it comes to attribution.

The second most significant evolution, inextricably linked to the first, has been the dramatically improved defensive posture of larger organizations. These whales were the first to be targeted and given their deep pockets, they were also the first to fund an improved posture informed by a corporate hierarchy which lends itself to coordinated risk mitigation as well as a keen awareness that the regulatory and judicial systems track their behavior. This evolutionary development is in part driven organically within an organization as well as the result of free market products and services which address the technical problem.

A third and critical component, which is less of an evolution than it is a failure to evolve, deserves consideration here. Small businesses underestimate the degree to which they are vulnerable and they often believe – in the face of plain evidence – that they aren't a legitimate target of cybercriminals. A 2015 survey by the National Small Business Association found that

half the respondents had been knowingly targeted, and that the average cost to remediate was more than $20,000. Nevertheless, a report by Travelers Insurance found that only 23% of small businesses "worried a great deal" about cyber risk. In addition to willfully ignoring the first-degree risks, there are often larger secondary risks presented by a vulnerable small business. They are often service providers or vendors to larger businesses and often are, to reuse the analogy, the path of least resistance by which malicious actors can gain unauthorized access to larger organizations.

These two evolutions, along with small business' failure to adapt, readily explains the explosive growth of successful ransomware attacks. If you will permit another analogy, imagine thieves targeting the Louvre museum. Now imagine that a year ago, they could have easily gotten in and stolen the Mona Lisa, which they could have then sold on the black market for millions of dollars. Now consider, much like big business in the United States, that the Louvre has upgraded its security. At the same time, law enforcement has gotten much better at policing the black market. As a consequence, the costs associated with both stealing and reselling the painting exceed the potential benefit. To this, the thieves realize they can simply padlock the entire museum shut, wire all of the art with explosives, and demand payment to disarm the explosives and unlock the doors. Now imagine the costs of conducting this sort of attack were low and could be conducted against thousands of museums in an hour, and that the fee charged to remove the padlock was tens of thousands of dollars - a significant sum but acceptable when compared with the reputational cost of losing revenue or reputation by going public with the incident or by refusing to comply. A dramatic example

perhaps, but considering the havoc that ransomware is, at this very moment, causing predominantly to small business, it is not an ill-fitting example.

Conclusion

While understanding the motivations which drive the threat actors is not on its own sufficient to build an effective framework for deterring or interdicting cyberattacks targeting small business, it is a vital component of the problem which cannot be ignored and which needs to be prioritized alongside other more established business risks. When taken in consideration with other factors – such as the advancement of technical solutions (both offensive and defensive) – the knowledge of the enemy and their tactics, techniques and plans may permit a logical and cohesive approach to the ever-evolving problem.