Date: September 8, 2016

To: The Commission on Enhancing National Cybersecurity

Changing the Direction of Cyber Security Will Require a Bold Security Vision

When the President established the Commission on Enhancing National Cybersecurity, he did it in response to a significant threat to our national and economic security, both of which are inextricably entwined. Coming off the theft of 22 million records of Federal employees, Federal contractors, and their families in the OPM breach, the compromises of networks at the White House, the State Department, and the Joint Chiefs of Staff, among many, many other Federal agencies, the President no doubt understood that if we are to change the trajectory in cybersecurity, we will need to embrace radical change in how we approach cybersecurity.

Among many headlines of commercial sector breaches, the heist of Bangladesh Central Bank ($81M), which compromised the integrity of the global SWIFT financial network, nearly netted hackers $1B in a single hack, if not foiled by an observant Fed bank employee due to a spelling error in a wiring order. As we now know, the recent DNC hack and hacks of members of Congress and Congressional committees are now attributed to Russian hacking elements and were likely part of a larger information ops campaign to influence US elections. On the back of these high profile hacks, we must re-think how we do cybersecurity not only because it is clearly failing, but also because the consequences from these failures pose a clear and present danger to National security and economic stability.

My statement to the Commission is to think boldly, not incrementally. Producing a report from another Commission (of which there is a long and distinguished history of Cybersecurity Commissions that have advised USG and Presidents) that urges better cybersecurity hygiene practices will be a wasted opportunity from a Presidential directive. Urging more or better vulnerability management and user training will not produce the changes desperately needed in our Nation's networks. With an upcoming election and a new Administration coming in, the Commission has an opportunity to capture the mindshare of a new President and Administration who will likely understand the importance of cybersecurity and why fundamental change is necessary. This will mean having the courage to take on sacred cows – vulnerability centric security and user training -- and check-box security, which while good for management, have proven ineffective after decades of failure.

A Failed Industry

I speak to you as a practitioner, innovator, and entrepreneur in cybersecurity. Post 9-11, I spent four years at DARPA in classified cyber programs understanding at a deep level the capabilities of our adversaries while developing techniques to counter these adversaries. Post DARPA, I continued my quest to strengthen our Nation's defenses by starting an R&D firm to develop non-signature based cybersecurity capabilities including isolating untrusted content via containerization and mapping the malware genome using machine learning algorithms and big data architectures. To bring these innovations to market, I founded Invincea, a next generation endpoint security company, to challenge behemoth endpoint security companies that have failed to stop cybersecurity attacks on a massive scale. I can say with confidence from my years of experience inside of Government and in the private sector that in order to change the current trajectory of a failing cybersecurity strategy, change must come from leadership and must start with a bold vision.

In response to the Request for Information on Current and Future States of Cybersecurity in the Digital Economy, I'd like to focus on the most common and addressable vector of attack today: spear-phishing.

Spearphishing: A Solvable Problem

According to the 2015 Verizon Data Breach Investigations Report, as much as 80% of all malware infections originate as spear-phishing attacks. Mandiant reports 95% of all breaches they investigate begin as a spear-phish attack. The high profile attacks mentioned in the opening paragraph all began with a spear-phishing attack. Put simply, the attack preferred by adversaries is spear-phishing because it costs very little, does not require much skill, it always works, and there is low likelihood of getting caught.

Since we know definitively that 95% of all consequential attacks begin as spear-phishes, it is obvious that by solving this one issue – users clicking on malicious links and attachments – we can achieve significant gains in driving down incidents while increasing cost to the adversary.

This problem suffers not from a lack of awareness – almost every large enterprise has some sort of spear-phish training program – but from a lack of solution engineering matched to business needs. The market response to spear-phishing has been user training and user shaming. Security professionals have in essence abdicated their responsibility for stopping spear-phishing attacks by placing it squarely on employee users. In a nutshell, the spear-phish defense strategy espoused by most organizations is that it is up to every user to determine which emails are malicious and which are benign and not click on the malicious ones, while being shamed if you do. By extension, the security of the entire network depends on every user to make the correct decision on every email.

The Verizon Data Breach and Incident Response (DBIR) Report for 2016 did a meta-study of spear-phish training for over 8 million users across multiple industries and by multiple training firms. Their results show that on average 30% of users were opened by recipients and 12% of users went on to click on the link or attachment, thus launching a potential malicious payload. The median time for the first user to open a malicious email was 1 minute and 40 seconds, while the median time to opening the first malicious attachment was 3 minutes and 45 seconds. This was backed up by another study showing click rates on spear-phish testing to be on average 31%[1]. Other studies have shown not only is spear-phish training not working, but it also has negative effects on business because "employees become more suspicious and mistrustful, and that's not conducive to good work"[2] It is fair to say the evidence for spear-phish training's ineffectiveness is conclusive – it is just not working and today represents a misallocation of time and money that could be better spent on effective measures.

Unfortunately, the adversaries understand this well, which is why even the most sophisticated nation state actors use spear-phishing as the go-to method for getting access onto a network. To address this problem, we need to take responsibility for stopping spear-phish attacks from succeeding rather than blaming users when it does. While spear-phish awareness is beneficial, as are awareness training around other types of threats, we know conclusively it is not a viable strategy for tackling spear-phish attacks.

Isolating Untrusted Content

Having spent years at DARPA studying adversarial methods and common defenses, one approach to changing the game on adversaries became apparent: isolate untrusted content users interact with from the core systems and data on which they run. In the extreme case to illustrate, computers are relatively safe from Internet based attacks so long as they aren't connected to the Internet. However, this is not a feasible strategy. Likewise running separate computers – one for Internet, one for business applications – has proven too cumbersome particularly as most business applications have migrated to the cloud. The balance between security and usability is a critical one to get right. Any security solution that inconveniences the user is

[1] "Nearly a Third of Users Fall for Phishing" online in *eWeek*. http://www.eweek.com/blogs/security-watch/nearly-a-third-of-users-fall-for-phishing.html

[2] "Security Awareness or No, Users Will Keep Clicking on Dodgy Links" online in *Helpnet Security*. https://www.helpnetsecurity.com/2016/08/04/security-awareness-training/

likely to be bypassed or removed altogether. For example, putting browsers in the cloud and using terminal services to remotely browse has proven too cumbersome for many real-world applications, in spite of the apparent gains in security from isolation.

To this end, Invincea has brought to market sandboxing software that runs on the endpoint with negligible footprint and performance overhead. The approach is simple – anytime a user clicks on a link or opens an attachment from an email, the content (e.g., a web page or an Office document) is automatically opened in a sandbox that remains invisible to the user. No special browsers or applications are needed. Invincea accomplishes this by isolating the application and providing it its own file system. This approach maximizes the benefits of isolation while not being cumbersome to the user nor introducing a noticeable performance penalty on the endpoint. The approach categorically eliminates spear-phishing as a threat without asking users to open a sandbox or login to remote servers or changing their normal workflow.

This approach has achieved remarkable market penetration as well. Dell sells this spearphish isolation approach as Dell Protected Workspace on all of its enterprise laptops and desktops. The Department of Homeland Security as well as the United States Postal Service – both large departments with over 200,000 employees – have recently acquired and are deploying this technology to all of their desktops and laptops. In other words, the technology has proven itself in commercial and Federal environments in scale. It is not an academic idea or suggestion. It is a real world technology that daily is stopping 0-day attacks and previously unknown malware and ransomware in large numbers. And most tellingly, the original technology was built under DARPA funding to Invincea Labs. This is an example of true DARPA innovation that crossed the chasm to commercial markets. You can read more about this and the performance of the machine learning algorithms in this separate blog.

Call to Action

As is often the case, leadership typically determines outcomes. A recent Congressional report on the OPM incident showed that the most significant reason for the breach was a failure in leadership. Leadership that did not treat the threat seriously when they were informed, nor employ a security strategy to address the type of threat they faced. In terms of cybersecurity spending, not only were they underfunded, but they also misallocated security investments. Even prior to the breach in 2015, OPM heavily allocated budget to post-breach detection and response tools at the expense of prevention tools in a 70/30 ratio respectively. The results were a self-fulfilling prophecy. The lack of prevention tools enabled Chinese adversaries to get into the network and steal 22 million employee records with national security significance. The post-breach detection and response tools told them what happened.

Failure to learn from history is a recipe for continued failure. Doing the same thing over and again and expecting a different result is Einstein's definition of insanity. The opportunity for the panel is to take advantage of the Presidential visibility on cybersecurity given massive cybersecurity failures and make recommendations that are more than incremental iterations of the same old strategy that is failing.

With next generation security tools in machine learning, behavioral monitoring, and isolation now available in market, only a lack of vision and leadership holds the Federal Government back from making serious strides in cybersecurity. It is not for lack of innovation we can't do better. My call to action for the Committee is to make strong recommendation for enterprise wide adoption of solutions that can categorically take threats like spear-phishing off the table to make a meaningful impact in cyber security.

Thank you for your attention and consideration.

Very respectfully,

Anup K. Ghosh

Anup K. Ghosh
Founder & CEO
Invincea, Inc