SILVERADO
POLICY ACCELERATOR

Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience

Written Testimony of Dmitri Alperovitch
Executive Chairman, Silverado Policy Accelerator

Before the U.S. House Committee on Homeland Security
February 10, 2021

Chairman Thompson, Ranking Member Katko, Members of the Committee:

Thank you for inviting me to testify at today's hearing on cybersecurity. This is the policy arena I have spent my 25-year career in the technology industry exploring as a senior executive working with and advising some of the largest private sector companies and most sensitive government agencies in the country. Now, as the founder of the Silverado Policy Accelerator, a new bipartisan public policy organization focused on national security, foreign policy, and cybersecurity, I am looking at ways to build upon my experience in the private sector to work with policymakers and strengthen our approach to new challenges that threaten our critical infrastructure and the backbone of our economy.

Most recently as the co-founder and Chief Technology Officer of CrowdStrike, which I helped to grow from an idea into the world's largest cybersecurity firm, I witnessed the complexity and scope of the challenges that the U.S. government and businesses face in the cyber domain. Our adversaries in cyberspace are sophisticated and numerous, ranging from global criminal groups conducting ransomware attacks and stealing financial and personal data, to nation-states executing complex espionage campaigns, stealing intellectual property and launching highly destructive and disruptive attacks.

Throughout my years at CrowdStrike, I saw firsthand that cybersecurity represents a growing part of a broader geopolitical struggle between the U.S. and its adversaries and competitors. This inspired my decision to retire from CrowdStrike last February to launch Silverado to advance American prosperity and global competitiveness in a new era of great power competition. Silverado will use a venture capital approach to accelerate bipartisan policy solutions to pressing challenges in critical areas of economic, strategic, and technological competition. We are set to officially launch next week, and I hope this will just be the first of many occasions for Silverado to engage with this Committee to support your important work for the nation.

As the U.S. enters a new era of competition, on battlefields old and new, modernizing and further resourcing America's cyber strategy is a necessary precondition for achieving any number of other critical government objectives. In my testimony today, I will outline a conceptual framework for understanding cybersecurity. I offer five recommendations that I believe will meaningfully improve our ability to anticipate and prevent cyber threats and fortify our cyber defenses, building on the recommendations and critical work undertaken by the Cyberspace Solarium Commission:

1. Providing the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. Department of Homeland Security with the authorities and resources to one day become an operational federal CISO, or Chief Information Security Officer, for the civilian federal government;
2. Adopting speed-based metrics to measure agencies' response to cyber threats;
3. Passing a comprehensive federal breach notification law;
4. Increasing security standards for vendors supplying high-risk software through government acquisition processes; and
5. Targeting the business model of ransomware criminals with mandatory "Know Your Customers" rules in cryptocurrency payment systems.

Threat Landscape

Almost half a decade ago, I coined the phrase: "We do not have a cyber problem, we have a China, Russia, Iran and North Korea problem."

Cyberspace is not a separate virtual world, immune from the forces that shape the broader geopolitical landscape. Instead, it is an extension of that landscape, and the threats we face in cyberspace are not fundamentally different from the threats we face in the non-cyber realm.

China, Russia, Iran and North Korea are the four primary strategic adversaries whose malignant activities in cyberspace we try to counter on a daily basis, as we do their more traditional tactics in the physical world. Oftentimes, these battle lines extend to non-state actors, such as the most well-organized cybercriminals. These actors inflict enormous damage on our economy by launching ransomware attacks and stealing financial data from our businesses and citizens, and it is no coincidence that they operate with impunity from the safety of their homes in these very same countries.

These countries conduct a variety of cyber operations against us on a daily basis, ranging from cyber-enabled espionage against our government to the theft of intellectual property from our companies to destructive attacks that shutdown business operations to the interference in the foundation of our democracy: our elections.

The challenges we face were highlighted just over a month ago, in December of 2020, when we learned that multiple customers of SolarWinds, a network management company, had been compromised by a sophisticated supply chain attack by a nation-state adversary believed to be affiliated with one of Russia's intelligence services.

The latest supply chain attack has drawn attention to serious gaps in the U.S. cybersecurity strategy. As a threshold matter, I believe that it is misleading to refer to this most recent breach as "the SolarWinds hack." Although SolarWinds was a prominent attack vector that received early attention in the press, we now know that it was only one of many supply chain vectors that the adversary used to gain access to private networks. Because investigations into the scope of the attack are still ongoing, we cannot even say with confidence that SolarWinds was one of the largest or most significant vectors. Continuing to refer to the breach as "the SolarWinds attack" distracts from the reality that the breach went far, far beyond a single company. As a result, I, along with other security practitioners, have begun referring to this hack as the "Holiday Bear" operation.

Additionally, as we have learned more about the breach over the past two months, I've come to believe that it is also misleading to refer to this incident as a singular attack, or even as a coordinated campaign with a defined end date. Simply put, the sort of sophisticated, long-term cyber-espionage enabled by supply chain vulnerabilities that came to light through this breach is not a discrete or self-contained occurrence; it is the new normal.

It is clear to me that the Russians have learned from their past operations. Throughout 2014-2015, SVR, the Russian foreign intelligence agency believed to be responsible for this most recent activity, launched a broad campaign which gave them access to the networks of the White House, the Joint Chiefs of Staff and the State Department, among others. The success, however, was short-lived, as U.S. defenders quickly detected the noisy campaign and ejected the adversary within weeks. I believe that those original mistakes led the SVR to reevaluate how they conduct new cyber operations and focus on compromising software supply chains in order to gain access to target networks in a much stealthier fashion and to remain in them for weeks, if not years. In some ways, this tradecraft is the cyber equivalent of the Russian illegals program, long practiced in human espionage operations: an extremely patient and long-term effort to gain maximum access to high-value U.S. targets. Since the 1930s, Russia has been sending covert sleeper operatives into our countries under non-official cover to live and work amongst Americans and over years get close to powerful officials in order to steal our secrets. Unlike the Illegals program, however, supply-chain based cyber intrusions are much easier and cheaper to scale to hundreds of high profile victims, all without putting their human intelligence officers at risk.

I believe that this is the Russians' new way of doing business in cyber operations, and I suspect we will continue to see this new approach for years to come. We have also seen China's intelligence services leverage supply chain attacks in the past, and we can expect them to incorporate valuable lessons from this latest Russian action into their own operations.

Recommendations

This Holiday Bear operation further highlights the need for a broader paradigm shift in both the private sector's and the government's approach to cyber strategy. Across the board, organizations should adopt what we in the cybersecurity industry call an "assumption of breach" approach, where defenders operate on the basis that an adversary has already gained access to their sensitive networks. The premise is simple:

- No cyberdefense system is 100-percent effective at preventing breaches;
- Even with the best training, human error will inevitably foil the smartest defense strategies; and
- Adversaries are constantly adapting to existing defense mechanisms and designing new ways to circumvent them without being detected.

The only safe assumption in the cyber battlespace is to assume that networks are never safe.

The assumption of breach approach is the only appropriate paradigm to govern cybersecurity strategy in this new era of great power competition. Our competitors in this contest are highly-sophisticated, well-resourced nation-state actors. We underestimate their capabilities at our own peril.

Incidentally, this is not any different from the approach we already take in the physical world. As a matter of practice, we assume that at any given moment there are people inside our sensitive government agencies who have been recruited by foreign intelligence services. Our counterintelligence approach is not merely focused on preventing such recruitment. Instead, we explicitly undertake significant efforts to identify spies and limit the damage they may be able to do to our national security. We need to adopt this same approach in cyberspace.

This shift in strategic paradigm necessitates a shift in practice. This Committee should be commended for its strong leadership in pushing for new and significant resources to support the federal government's cyber strategy, most notably by creating CISA in 2018 and strengthening CISA's authorities under the FY21 National Defense Authorization Act (NDAA). But, more needs to happen to capitalize on this momentum and deepen these commitments, and in particular, I have five recommendations for this Committee's consideration:

1. **Congress should take steps to set CISA on a path to becoming the operational CISO, or Chief Information Security Officer, of the civilian federal government.** The majority of the 137 Executive agencies lack the personnel, the knowhow, and the resources to execute a comprehensive cybersecurity strategy. Congress took an important step toward centralizing federal cybersecurity strategy by creating CISA in DHS in 2018, but the next step is to give CISA both the authority and the resources that it needs to effectively execute its mission.

Ultimately, CISA should have the operational responsibility for defending civilian government networks, just as Cyber Command does for DoD networks. The recent NDAA, which vested CISA with the authority to hunt on agencies' networks without the explicit permission of those agencies, was a critical move in that direction. CISA will now need additional funding to build a 24/7 threat hunting operations center to fulfill the requirements of that mission. Another important step would be to create incentives for federal agencies to outsource their cybersecurity operations to CISA, turning it into a cybersecurity Shared Service Provider. Such incentives may include exceptions for agency heads from FISMA compliance and turning that responsibility over to CISA, if it is actually being given the authority to secure that agency's network.

2. **Congress should make agencies adopt speed-based metrics to measure their response to cyber threats**. In cyberspace, the only way to reliably defeat an adversary is to be faster than they are. Under an assumption of breach approach, the question is not, "Can we prevent an initial compromise?" The much better question is, "How long does it take us to find and eject them?" Central to detecting adversaries is the speed with which they leverage the initial resource they have established as their beachhead within the network, move laterally across the environment, and gain access to other sensitive resources. Once adversaries are able to do that, what would have been a minor security event turns into a full breach that requires a lengthy and complex incident response process and that puts defenders' data and operations at risk. Stop the adversary quickly, and you have prevented them from accomplishing their objectives.

With this in mind, Congress should require federal agencies to adopt speed-metrics that evaluate agencies' response to cyber threats based on the time it takes to begin and complete fundamental defensive tasks. In the private sector, I developed what I called the "1-10-60 rule" to measure response times to perceived threats: **detect an intrusion on average within one minute, investigate it within 10 minutes, and isolate or remediate the problem within one hour.** Through legislation, Congress could require agencies to adopt speed-based metrics by mandating that they collect data on the average time it takes to perform four fundamental defensive actions: (1) detecting an incident; (2) investigating an incident; (3) responding to an incident; and (4) fully mitigating the risk of high-impact vulnerabilities. Over time, these metrics would provide objective and diachronic measurement of an agencies' threat response capabilities that they could report to CISA, OMB, and the relevant oversight committees in Congress. If the metrics prove effective in decreasing agencies' response time to cyber threats, Congress should also consider models to extend their adoption by the private sector.

3. **Congress should pass a comprehensive breach notification law**. Such a law would require major private companies, such as those in critical infrastructure, to report technical indicators associated with breach attempts to CISA, including for breaches where no personal information is actually compromised. If there is a single overriding lesson from the recent supply chain attacks, it is that the information sharing between government and industry remains a serious challenge. Some victims have shared very little information about what took place inside their networks; others have not even publicly acknowledged that they were targeted.

At present, there is no comprehensive federal breach notification law, and state-level laws are too decentralized, too focused on personal information instead of risk to systemically important critical infrastructure, and sometimes create a perverse incentive for companies not to investigate attacks. In the case of complex supply chain attacks like “Holiday Bear,” one company’s failure to publicly report a breach can have wide-reaching implications. For example, if cybersecurity company FireEye had not voluntarily and publicly shared evidence of their own compromise and that SolarWinds was the attack vector, the public and the government may not have known about this highly impactful attack for many months to come. Yet, FireEye had no legal obligation to report this breach under existing law. They should be praised for their courageous decision, but unfortunately, not all other victims have followed their lead in transparency.

4. **Congress should take steps to increase security standards for vendors supplying high-risk software via government acquisition processes*.*** Government agencies and private-sector businesses currently rely on a number of companies such as SolarWinds whose software runs with high levels of privilege on their networks. Yet these agencies and businesses have little to no sense of the security levels of that software. Borrowing from a widely-used private sector practice, Congress should compel these vendors to undergo annual, independent third-party audits of their source code and penetration exercises of their networks. The government could require that companies provide the results of these stress tests as part of the federal procurement process, or even require companies to publish the results of those audits publicly on their website. Not only would this process increase transparency for their customers, but it would also incentivize companies to quickly and efficiently patch vulnerabilities in their networks or source code and get a clean bill of health, as no one would want to publish a failed audit.

5. **Congress should support stricter “Know Your Customer” (KYC) requirements for worldwide cryptocurrency exchanges to target the business model of ransomware criminals.** Dangerous ransomware attacks pose an existential threat to critical infrastructure and many small and medium businesses in this country. For example, criminal attacks on hospital systems—a favorite target of ransomware attacks—put the lives of American citizens in danger, especially during the pandemic, when hospital beds are already in short supply. Ransomware criminals rely on widely-available and largely anonymous cryptocurrency, such as Bitcoin, to collect hundreds of millions of dollars in ransom payments without risk of disclosing their identities to victims or law enforcement. It is no coincidence that the explosion of ransomware attacks occurred only after the invention of cryptocurrency platforms, which are the oxygen that fuels the fire of these criminal operations. And while it remains very difficult to purchase goods and services, such as real-estate, cars and other luxury items that these criminals may want, with cryptocurrency, it is currently easy to anonymously use cryptocurrency exchanges to convert ransom payments into reserve currency like dollars or euros.

The bottom line is that we need stronger tools to undermine the ability of criminals and nation-states to use cryptocurrency to receive and convert ransom payments and purchase illicit goods. The international community has already taken some steps to strengthen KYC requirements. In June of 2019, the intergovernmental Financial Action Task Force (FATC) issued guidance recommending that virtual asset service providers, including crypto exchanges, share information about their customers with one another when transferring funds between firms. In December 2020, the U.S. Treasury Department published an advance notice of proposed rulemaking that would require cryptocurrency exchanges to perform and store KYC information on their customers, just like we require banks and other players in the global financial system to do. If designed and implemented properly, these types of tools can starve ransomware threat actors of the oxygen they need to operate.

Congress should undertake an evaluation of how stronger KYC requirements and other safeguards can be used to effectively stem ransomware threats and then propose legislation and support agency action that achieves those objectives.

Conclusion

I am grateful for this Committee's leadership on cybersecurity issues, and I believe that these recommendations would further advance America's defense by bringing its cybersecurity strategy in line with an assumption of breach approach. As the recent supply chain breach has made abundantly clear, we cannot afford to delay these actions any longer. Every day we fail to act on them is another day that we leave the American government and our people vulnerable to cyber attacks, intellectual property theft, and espionage.

These new steps would also serve to preserve America's competitiveness in this new era of competition between the U.S. and its adversaries. This contest has reached an inflection point: the nations that present bold, long-term strategies to advance their economic, technological, and strategic interests will shape the future for decades to come, and the nations that fail to act will fall behind. Modernizing America's cyber strategy is a linchpin that makes all other efforts to ensure continued American leadership possible.

Thank you for inviting me to testify before you here today. Silverado is committed to being a long-term partner and resource for this Committee in our shared missions to address these critical challenges facing our nation.

I look forward to your questions.