SECURE HALO
SECURING THE ENTERPRISE

INSIGHTS ON THE COMMISSION ON ENHANCING NATIONAL CYBERSECURITY REPORT

Natalie Lehr, co-founder and Vice President of Product Development for Secure Halo, shares her thoughts on the Commission on Enhancing National Cybersecurity report. Working for more than 15 years as a national intelligence professional, Lehr has extensive experience supporting federal agencies, as well as an inside view of policy development.

There is nothing unanticipated in the Commission on Enhancing National Cybersecurity's final report. While designed to accelerate the incoming administration's cybersecurity policies (by establishing nonpartisan, industry-focused input), there is no clear signal that the Trump administration intends to take its recommendations (fully or partially) into account. If anything, the president-elect has illustrated a willingness to view policy from a non-traditional perspective, and as a result even the commission's nonpartisan composition may not spare the report from the executive privilege to reimagine cybersecurity policy from its unique perspective.

Much has been stated about the Obama Administration's use of executive orders and presidential policy directives to kick-start federal cybersecurity engagement with private industry. From the foundational executive order 13636 on improving cybersecurity for critical infrastructure and PPD 21 in February of 2013, executive branch agencies have spearheaded cybersecurity policy without corresponding affirmation by the legislative branch. While executive action enabled progress on a variety of related matters, such as the government's role in information sharing and incident response, sustainment of the existing strategies and priorities by the new administration is far from certain.

The six imperatives, or aspirations, of the Commission are:

1. Protect, defend, and secure today's information infrastructure and digital networks

2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy

3. Prepare consumers to thrive in a digital age 4. Build cybersecurity workforce capabilities

5. Better equip government to function effectively and securely in the digital age

6. Ensure an open, fair, competitive and secure global digital economy

It is unlikely that the American public would disagree with the imperatives, as written, because they represent a common-sense ideals. Who doesn't want to "prepare to thrive" in a digital economy? The public and private sectors generally agree, for example, that more incentives and less regulation will produce better outcomes than prescriptive approaches. The real issue has been what is the right blend of market-driven and federal government incentives to accelerate cyber resiliency and investment? Are these incentives highly context-specific, or do general levers shift behaviors and outcomes? On this, there isn't much in the way of specifics.

The commission implicitly acknowledges the current lack of consistent, objective and repeatable cost-benefit analysis conducted against existing data sets.

As the commission considers the short, medium and long-term recommendations for their imperatives, the notable lack of actionable information and resources available to either U.S. businesses or government is acknowledged. Low cost, high yield cybersecurity investments are referenced as elusive due to the lack of foundational data to conduct effective modeling. While the DHS/CIDAR efforts are cited, its shortcomings (to include the lack of incentive to voluntarily share data and dedicated resources to see it realized) will not be resolved with the establishment of a new Cybersecurity Framework Metrics Working Group. Rather, by making this recommendation, the commission implicitly acknowledges the current lack of consistent, objective and repeatable cost-benefit analysis conducted against existing data sets, as well as the lack of progress to achieve that goal with the existing federal government policies and funding. We are no closer to definitively illustrating how we might pivot from the attacker having the advantage to the defender. Despite the $120 billion a year in private sector spending on cybersecurity, and its public sector equivalent of $14 billion, our digital networks are no more secure today from attack. In fact, the defender remains in an economic and technical disadvantage relative to the attacker.

SECURE HALO
SECURING THE ENTERPRISE

INSIGHTS ON THE COMMISSION ON ENHANCING NATIONAL CYBERSECURITY REPORT

Investments in simple, perimeter defense strategies are outmoded as attackers are developing more sophisticated capabilities that target internal identity and authentication systems. The IoT evolution will make the protection of identity and the strengthening of authentication even more necessary, due to the profound impact and exponential scale it adds to our digital ecosystem. Outside in and inside out defenses must be aligned, measured and continuously improved.

Similar to other industry publications, the commission calls out the struggles of small and medium sized business in the face of increasing cybersecurity burdens. In many cases, SMBs have the greatest need, but their engagement with the federal government and the resources at their disposal lag significantly and disproportionately behind large companies. As SMBs are increasingly used as attack vectors on larger corporations, we ignore their interest at our collective peril. Market-based incentives that make cybersecurity measurable and accessible to SMBs must remain a federal and commercial priority. Market forces in the short and medium term will ultimately determine which among the basket of potential incentives drive SMB cyber resiliency.

In the near term, the central judgement remains that the NIST Cybersecurity Framework (2014) and market-based incentives in the form of cyber insurance will form the bridge between the past and the future. The commission opines that NIST Framework and insurance will continue to influence industry decision-making and government engagement in the near and long term. Additionally, the NIST framework, as illustrated in a 2016 Gartner survey, will likely show increased adoption by critical infrastructure (CI) industries and non-CI businesses alike. It is also highly likely that the NIST framework will form the central basis for extension into international cybersecurity engagements, since the underlying framework contains many of the same core industry safeguards, and therefore is globally-relevant and scalable. Harmonization of the NIST Framework with federal and state government initiatives is recommended as an approach to reduce burdens and accelerate conformity.

Criticism of existing public-private sector cooperation is well-known and documented, especially that such engagements need to be actionable and effective. The report highlights the imperative for the federal government to establish repeatable, consistent processes for evaluating and assessing "appropriate deterrence, prevention, response and mitigation...from a legal policy, national security and business process perspective," which in short reveals the seemingly ad hoc nature of its current treatment.

Ultimately, the first 100 days of the incoming administration will define the pace and scope of its cybersecurity strategy. It will also signal how, if at all, the new administration intends to harmonize the cybersecurity efforts of the executive branch agencies with independent commissions. While industry can rely on the federal government sustaining its role in incident response, the first 100 days will also signal whether the incoming administration intends to organize and adequately resource federal policy and processes that are essential to transition from reactive programs to proactive strategies.

As there is no obvious economic or technical silver bullet, complex policy matters will likely remain elusive in the short-term. In the interim, market-based incentives, especially those in tune with global market forces, will have the opportunity to outpace executive action.

Market-based incentives that make cybersecurity measurable and accessible to SMBs must remain a federal and commercial priority.

We are at a critical juncture, where as a nation and as a government we must decide the rules that will govern our transition from an industrial economy to a digital economy. It is in the interest of our national prosperity that our economic and national security strategies balance that transition with concern for near term as well as long term implications. Traditional regulatory authorities and resources cannot keep pace with cyber risk. Market-based incentives such as cyber insurance will ease our transition as the contours of the public-private engagement are formed and cemented.

Please contact us for more information on how Secure Halo can assist your organization to meet and exceed compliance with the SEC's cybersecurity guidance.