BEACON
GLOBAL STRATEGIES

MEMORANDUM

Date: **February 22, 2016**
From: **Beacon Global Strategies (BGS)**
Re: **Cybersecurity in 2016**

The current landscape of cyber threats is dominated by criminals, nations, and other hackers seeking to exploit vulnerabilities in systems, networks, and individuals. Their objectives include:

- theft of personal and corporate data;
- manipulation of corporate data and processes; and,
- achieving persistent access in sensitive systems for future exploitation.

The challenges businesses and consumers face today are more complex than ever:

- individuals are far more aware of risks of their personal information being exposed by hacks on the companies with which they transact. Individuals' expectations for better protections is increasing;
- cybersecurity is becoming a crucial variable alongside cost, performance, and schedule for deals. Yet measuring cybersecurity remains more art than science.
- businesses now acknowledge the importance of cybersecurity, but most still struggle to convert that acknowledgment to improved security practices.
- they confront a dizzying variety of off-the-shelf "solutions" without meaningful mechanisms to compare and tailor solutions to their particular needs.
- as the Internet of Things proliferates, new attack vectors are being created into existing networks that will require even more after-the-fact security solutions since security continues to be an afterthought in these products.

From defense to resiliency: For years, businesses sought products and services to keep hackers out of their systems. Defense was the call. Now, one innocent but accidental click on a malicious attachment can grant unauthorized access to an attacker. Businesses now find themselves alongside governments, operating under a presumption of breach. Resiliency in the face of compromise has now become the focus.

Growth Areas for 2016: In February 2016, the Obama Administration rolled-out several initiatives as part of a Cybersecurity National Action Plan, including:

1. A $19 billion investment in cybersecurity for FY2017, representing a 35% increase in cybersecurity spending. While this dramatic increase represents an important focus of attention for the administration, the risk continues to be throwing too much money too quickly at the wrong problems. Ultimately, skill and training are the top commodities for government and business alike. Over the long term, resources need to reduce the national attack surface, moving beyond "security as an afterthought" and moving towards "security by design."

2. A $3.1 billion Information Technology Modernization Fund that will phase-out obsolete systems across the federal government. This is a long-overdue investment. If married with timely, smart, and security-minded replacements, informed by the work of the U.S. digital services, this fund could go a long way towards reducing the vulnerabilities of federal systems. Next steps include how to measure if and how modernization is and is not improving security, the standardization of authentication and encryption practices, and which steps states can apply to modernize their own systems.
3. A new Federal Chief Information Security Officer to encourage security-minded practices and reforms across the federal government. This too is a long-overdue step in the evolution of how government organizes itself for cybersecurity. As always, the challenge will be for this new individual to build alliances throughout the federal government and to build consensus as to how the IT modernization funds are spent. Next steps will be for White House leadership to decide how much of a role this individual will play in the development of broader cybersecurity policy and the authorities this individual will possess to drive change across government as a whole.
4. A new Commission on Enhancing National Cybersecurity, led by former National Security Adviser Tom Donilon, to provide recommendations about how to improve cybersecurity over a 10-year horizon. Contrary to some arguments that technology changes too fast to think long-term, this commission has an important opportunity to chart a road-ahead for the technology, business, privacy, and government communities. Because so many hacks continue to be the result of exploiting known vulnerabilities, an emphasis on reducing vulnerabilities in software should be a key priority.
5. A new Federal Privacy Council will help ensure the government's efforts in the short- and long-term are informed by privacy considerations. That the President issued an executive order to create this council shows just how critical the privacy community's voice remains to the national dialogue about cybersecurity. The opportunity for businesses to explain how new products increase the protections over a user's private data will be significant. The challenge will be not to oversell these protections in the face of inevitable vulnerabilities that will continue to be discovered in new software.

The federal government has taken steps to improve the cybersecurity of the nation, but ultimately, most businesses most of the time will need to do more to protect themselves, relying on outside service providers to help them get ahead of the threat.

1. *Cyber Command*: Four years ago, the military began to create a 6,000-person strong Cyber Mission Force with three missions: to defense Department of Defense networks and platforms; provide commanders with integrated cyberspace capabilities to support their operations; and to defend the nation from a cyberattack of significant consequence. This force helps the military address sophisticated threats to its systems and ultimately its readiness to respond in a crisis. However, a senior Department official acknowledged in

testimony last year that only the top two percent of threats would be sufficiently serious to prompt the military to respond. While Admiral Rogers, Commander of the Cyber Command, is expected to provide an update on development of this force at an upcoming posture hearing, businesses should neither wait for nor expect the armed forces to come to the rescue of their corporate networks.

2. *Federal Bureau of Investigation*: The FBI has evolved into an organization with sophisticated capabilities to tackle malicious cyber activity. By some accounts the FBI aims to hire more than 2,000 analysts and agents specifically to combat cyber crime. Companies need to establish relationships with local FBI field offices and representatives. The FBI can provide early (though often incomplete) warning of a compromise, and, in some situations, be a useful partner in the aftermath of a hack. Especially as the number of technically-trained agents increases, the FBI should be in a position to provide more substantive assistance in the years ahead.

3. *Department of Homeland Security*: For years, DHS has struggled to organize itself to accomplish its cyberspace mission: to secure non-military federal systems, to protect critical infrastructure across the nation, and to disseminate cyber threat information and analyses. Last fall, Congress questioned DHS's efforts to reorganize its National Protection and Programs Directorate but ultimately acknowledged a need to empower the National Cybersecurity and Communications Integration Center to be a true 24/7/365 hub for information sharing and analysis. Analysts expect DHS to assume greater prominence in national cybersecurity efforts over the course of 2016. First, last year's passage of the Cyber Information Sharing Act (CISA) granted liability protection to companies who share cyber threat information, but this protection is mostly conferred when the information is shared through DHS. Second, as threats to national critical infrastructure grow, DHS's Industrial Control System response teams will become much more in demand.

4. *Future Legislation*: Ultimately, CISA passed last year due to a belief that doing something was better than nothing. In the wake of the Apple encryption case, Congress will continue to debate encryption legislative proposals, but with the privacy and technology communities still leery of the government's motives, analysts do not expect any further meaningful cybersecurity legislation for the rest of the Obama Administration. Instead, effort will shift to implementing CISA, specifically the speed at which information can be disseminated.

5. *NIST Framework*: Over the last several years, the National Institute of Standards and Technology has developed a framework of best practices for improving critical infrastructure cybersecurity. Initial efforts to impose such standards on companies ran into fierce opposition, so NIST's framework remains voluntary. NIST completed an initial framework in 2014, but they continue to convene workshops to examine the framework's effectiveness and consider avenues for improvement.

5. *International Norms*: Another federal government priority is to reduce malicious cyber activity by promoting international norms of peacetime behavior in cyberspace. An

agreement last year between Presidents Obama and Xi marks an aspiration to reduce state-sponsored theft of intellectual property for private economic gain, but White House officials still say it's too soon to tell if the Chinese are living up to the agreement. Generating international consensus around peacetime norms in cyberspace is a key diplomatic priority, but rigorous monitoring by potential victims themselves will be the source of metrics to know if and by how much this hacking has decreased. Companies need to work with security advisors to detect recidivist hackers, and the government needs to provide indicators to help companies better protect themselves from such repeat offenders and to close-off repeat intrusion points.

Wyndham Fallout: Perhaps the most watched case of federal government regulation and enforcement in the cybersecurity arena settled last year: the FTC's investigation of Wyndham's security of its networks concluded with a settlement under which Wyndham will establish a comprehensive information security program. Although such information security programs are becoming more commonplace, companies should not view the Wyndham case as a rebuke to the government's ability to investigate and regulate how businesses handle data privacy. To the contrary, as the scope and scale of data breaches continues to grow, more pressure – especially under a new administration – will fall on regulatory bodies to probe the practices of how companies secure data. The more attention companies devote up-front to designing thorough and transparent plans, and then having those plans independently red-teamed, the better chances they have to work through a future breach and investigation.

Public-Private Partnerships: A cornerstone of federal cybersecurity policy has been that cyber threats cannot be solved by the government alone. Working together with the private sector is not just crucial, it is required. Since the vast majority of telecommunication and information infrastructure is owned and operated by the private sector, the government has little ability on its own to dictate protective measures. Information sharing provides one avenue for such public-private cooperation.

- *Information Sharing and Analysis Centers (ISACs)* have emerged in recent years as member-driven non-profits to facilitate sharing of information within particular sectors. The financial and electricity sectors are two examples.
- *Information Sharing and Analysis Organizations (ISAOs)* have similar goals but are not sector-specific. Promoting these organizations became a key objective of President Obama's Executive Order 13691, which sought to improve cybersecurity across the country. The Northeast's Advanced Cyber Security Center (ACSC) is an example of a regional ISAO, comprised of banks, law firms, and universities.

The key issues for 2016 are: whether these information sharing organizations will actually benefit from more relevant and timely information from the federal government; and if so, how quickly these organizations can push *operational* information to their members.