Proactive Public Policy per Cybersecurity

I) .US---The US has lost millions of technology jobs in the past 10 years due to inexpensive outsourcing operations overseas which have exacerbated cybercrime.

The infamous breach of DHS 3 years ago was due to a lack of standard of care and due diligence by a third-party data storage company. The 2008 Verizon Data Breach Report noted that 39% of breaches were a result of hackers transiting/island hopping through strategic partner networks. It is imperative that we grapple with the systemic risk from outsourcing which permeates our digital ecosystem.

The reason why global businesses open offices in New York City and pay astronomical rents is because they have trust and confidence in the safety and soundness of the USA. These businesses have faith in the rule of law and the enforcement of contracts and the security of the marketplace. This real world phenomenon can manifest in cyberspace given political leadership to challenge the webhosting, data warehousing and managed service providers to improve their standard of care per cybersecurity. .US being realized would improve US comparative advantage per data hosting, improve cybersecurity and reestablish technological hegemony.

1. Promote a secure .US ecosystem
2. Mandate that all entities who provide data services of any sort to the United States Government or the big 4 Critical Infrastructures sign Information Security Service Level Agreements which include at a minimum:
    A. Verify that the legal requirements to which the service provider is contractually obligated are compatible with your organization's definition of adequate security e.g. NIST 800-53
    B. Identify who in the service provider organization is responsible for security oversight (e.g., CSO or CISO) and their Information Systems Security Policy and incident response plan must be reviewed prior to movement of data or provision of service.
    C. Confirm that their policies and agreements regarding security breaches include customer notification on a timely basis (within one hour). Maintain the right to test their incident response plan on an annual basis.
    D. Confirm that the service provider has adequate backup facilities which are regularly tested for vulnerabilities.
    E. On a quarterly basis conduct red-teaming of their network security posture, and verify whether they have layered security beyond firewalls, virus scanners and encryption. (NIST 800-53A Appendix G serves as excellent guidance on this matter). Note: These audits should be conducted after security breaches as well.

The administration might consider giving tax credits to all commercial entities that currently are FISMA compliant as well as tax credits to those who maintain ISSLAs with third parties and strategic partners in 2009.

II) Cyber-Risk Assessments of Critical Infrastructures-- As evidenced by specific campaigns carried out against federal agencies in recent years, and further illustrated by trends emerging on the larger cybercrime landscape, a lack of situational awareness and an inability to predict the specific methods being utilized by electronic assailants of all archetypes has been one of the most significant failures in stemming the tide of successful attacks.

While organizations across the federal space, as well as the private sector, have gone to great lengths to employ layered defensive mechanisms aimed at preventing specific classes of threats from infiltrating their IT systems, clearly, based on the successful campaigns that we know of – such as the set of coordinated cyber-attacks emanating out of China beginning in 2003 and labeled "Titan Rain" which compromised assets at the DoD, NASA and Sandia National Laboratories, as well as those of federal contractors– these defenses have been proven vastly insufficient. And as we know there are likely many more incidents along these lines that have not been reported publicly than those we can already cite here today.

To address this dire reality, which has been highlighted most recently by widely publicized electronic data theft carried out against private merchants such as Heartland Payment Systems, which saw thieves make off with millions of its sensitive customer payment card records, your committee could compel all corporations which maintain critical infrastructures to undergo more frequent internal assessments to gauge their risk to cyber attacks.Specifically, corporations which maintain critical infrastructures must be required to conduct security audits using Red Team penetration testing methodologies on at least a quarterly basis to gain a more precise fix on where their most significant weaknesses lie by emulating the same tactics as those being employed by cyber criminals as closely as possible.

These quarterly security and IT systems penetration tests (as defined by NIST special document 800-53A Appendix G) must be applied to all federal networks and computing assets, as well as those of critical infrastructures providers across energy, finance and health sectors, among others, to empower these organizations to gain better a better understanding of where they are most vulnerable to potential attacks. Using classic risk management practices, those critical vulnerabilities that are identified via this process must then be remediated, and we must also create additional systems of accountability for those organizations found to be unable to properly address their critical vulnerabilities.

By compelling federal agencies and their business partners to engage in this proactive security testing, and specifically conduct regular internal assessments mimicking hacker activities, these organizations will be able not only to identify their most pressing instances of IT risk and ward off more attacks, but also to create effective benchmarks that they can refer to frequently over time to mark their progress in improving their security posture, and to channel spending into the most effective resources for doing so.

III. International-- The globalized nature of the Internet is creating systemic risk to the US economy and national security. The World Bank for years has spent billions connecting the developing world t the internet through ICT projects and E-finance projects. At issue is that US telecommunication infrastructure and financial infrastructures are directly intertwined with the developing worlds. Much of the cyber threat originated from the developing worlds IT infrastructures and weak enforcement regimes can be remedied. It is paramount to the success of our international effort that we provide financial incentives and to the developing world so that they create a more secure

cyberspace and assist in managing the systemic risks associated with the widespread compromise of those developing countries networks. The development of more secure telecommunications infrastructure and financial systems as well as capacity building per cybercrime enforcement is critical and can be achieved through World Bank programs.

Mitigating the systemic risk that occurs when foreign telecommunications and financial systems are compromised by hacker syndicates must be a priority. The hacker havens which exist in the developing world need to be eradicated. Promoting global development of secure, sustainable information communications technology (Sustainable ICT) is fundamental to ensuring US economic and national security. Therefore, this Committee should make this a top priority, including the following:

Congress should:

- Instruct all Departments and Agencies to incorporate cyber security standards and measures into all bilateral and multilateral projects, and report to _____ on these cyber security elements. Examples of bilateral or multilateral ICT opportunities include
    a. DOD: Strategic Defense installations in Poland.
    b. Treasury: Financial payments systems in developing economies.
    c. HHS and CDC: Health information systems with foreign partners.
    d. Transportation and FAA: Transportation control systems.
    e. Energy: Secure control access device systems for power.
    f. DOJ: Rule of Law work and anti-money-laundering enforcement
- Direct the Secretary of the Treasury to instruct the US Executive Director of the World Bank[1] to make Sustainable ICT development a top priority of all Bank development projects.
    g. Allocate 20% of project funds for telecommunications and finance projects to Sustainable ICT
    h. Direct the Bank of International Settlements and the Electronic Banking Group to develop and implement secure electronic controls to ensure the confidentiality, integrity, and availability of electronic banking systems, including all alternative payment channels not yet regulated by national legislation of many countries.
- Urge the G-8 to create a Cyber Action Task Force along the lines of the Financial Action Task Force to promote the development of Sustainable ICT and to combat attacks against the confidentiality, integrity, and availability of information systems.
- Urge all foreign partners to meet the criminal enforcement standards of the Council of Europe's Cybercrime Convention and apply for membership in the Convention.
- Urge regional multi-national bodies, such as OAS and APEC, to make Sustainable ICT a top priority in all programs and initiatives.

Tom Kellermann, MA, CISM

Vice President of Security Awareness

Core Security Technologies