TO: Ms. Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

DATE: September 9, 2016

SUBJECT: Input to the Commission on Enhancing National Cybersecurity

---

The Chertoff Group (TCG) appreciates the opportunity to provide comments to the Commission on Enhancing National Cybersecurity ("the Commission"). TCG works with clients across critical infrastructure sectors to help them assess, mitigate and monitor security risks. We also work with the providers of security products, services and solutions to grow their enterprise through business strategy and mergers and acquisitions services.

We applaud the establishment of the Commission through Executive Order 13718. While the targeting of commercial enterprises by malicious actors is not new, the ubiquitous nature of networked technology and the proliferation and evolution of threat actor tactics, techniques and procedures leaves organizations increasingly vulnerable to attack. Attempting to eliminate cyber risks is futile. Nevertheless, based on our cybersecurity risk management experience, we believe that it is both possible and essential for organizations to build a cybersecurity program that provides the organization with reasonable, risk-based security controls to secure sensitive technology assets notwithstanding the threat.

The U.S. Government can, working in partnership with State and local governments, the international community, the private sector and academia, help advance understanding and action toward managing and monitoring cyber risk. The information the Commission collects and communicates to the next administration will greatly assist in addressing this topic. Through our risk management experience and engagements, we have identified several areas the Commission may wish to consider as it develops its findings and recommendations:

**Information security guidance should be more tightly focused on actual effectiveness**

There is no shortage of guidance on what controls should comprise a cybersecurity program. The difficulty lies in the fact such controls must be applied in the context of a busy and sometimes messy legacy information technology environment. Indeed, numerous incidents have occurred notwithstanding an organization's ostensible compliance with an information security standard.

One key long-term answer lies in a "security by design" approach to hardware and software design and production, but this approach does not address "hear and now" realities of legacy infrastructure in place and likely to remain in place for some period of time. Given this scenario, in our view, organizations should realistically manage risk through a greater focus on actual effectiveness. Key elements of an effectiveness-oriented approach include a cycle of rigorous threat and business-impact-informed planning (that balances risk and ease of implementation), training and evaluation for personnel based on role, tracking measures of effectiveness and independent evaluation.

For example, we believe there is a need to link training and evaluation of security operations and related personnel more closely to ensure that they are effective in their roles. Building a 24x7 Security Operations Center is of little value – except to the plaintiffs' bar – if personnel cannot effectively manage it. Conversely, a continuous cycle of training and evaluation hones and validates skills against adaptive adversary techniques.

We believe there is a need for additional focus around sharing of threat information that underpins planning efforts (see below) as well as effectiveness measures that organizations can realistically apply within their own environments.[1] We also believe that, as organizations increasingly rely on outsourced IT services and managed security service providers, there is also a need for guidance and validation around assessing effectiveness of these critical outsourced services.

**Threat information sharing capability development should be prioritized based on the ability to generate effective outcomes in client organizations**

Over the last several years, there has been a significantly increased emphasis on the need to share threat information. Although an increase in the exchange of structured and unstructured threat data can theoretically help thwart potential attacks, it can also overwhelm even the most sophisticated, mature and resourced organization. A blind focus on information, without a linkage to how such information generates action or impacts overall security effectiveness, risks causing information overwhelm, false positive fatigue and overweighting of certain information types at the expense of other more impactful forms of information.

Indeed, greater discipline around the type of information being shared – i.e., distinguishing between cyber threat indicators and other forms of threat information, such as reporting around tactics, techniques and procedures used by malicious actors – is a precondition to considering how that information can be most effectively leveraged. For example, much discussion around cyber threat information sharing has focused on cyber threat indicators, such as IP addresses or MD5 hashes. We are concerned that this focus could deemphasize the importance of sharing around tactics, techniques and procedures (TTPs) used by adversaries,

[1] *See* The Chertoff Group, Views on the Framework for Improving Critical Infrastructure Cybersecurity, Feb. 23, 2016, *available at* http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160223_The_Chertoff_Group.pdf.

or IT assets likely to be targeted (e.g., Active Directory) – critical information for network defenders in prioritizing implementation or modification of security controls.

Recommendations:

1. ***Encourage greater interoperability for automated information sharing initiatives, which should also incorporate confidence levels for cyber threat indicators.*** For cyber threat indicators (IP addresses, MD5 hashes), current efforts to automate the exchange of such information should be encouraged, ideally also with greater emphasis around interoperability with existing tools as well as the incorporation of confidence levels in such indicators.

2. ***Prioritize identification and sharing of TTPs and exploit targets.*** That said, given the extremely rapid adaptation in IP addresses and MD5 hashes used by adversaries, it is also critical to apply greater priorities around the identification and sharing of tactics, techniques and procedures utilized by adversaries, as well as IT resources particularly likely to be targeted. TTPs represent "the behavior of an actor" and therefore provide richer detail into historic and potential patterns of attack and actor operating methods.[2] Understanding TTPs allows security professionals to focus network hardening and detection efforts more surgically to address risks more relevant to their environment – in other words, it helps match control prioritization to likely threat actor TTPs, thereby reducing risk and increasing effectiveness.

   So while file hashes, signatures and more commoditized threat indicator data can support immediate blocking and tackling, a dearth of TTP data prevents security teams from rapidly translating threat intelligence into prioritized implementation and auditing of security controls, identification of security requirements in a system development lifecycle, remediation of vulnerabilities, monitoring around certain assets. As a next step, we believe that prioritized development and distribution of TTP and related intelligence will facilitate that decision making.

   US government analysis resources (e.g., DHS NCCIC, US-CERT, ICS-CERT; FBI NCIJTF; etc.) can, working in conjunction with experts from Information Sharing & Analysis Organizations and industry, identify, evaluate and communicate actionable TTP insights out to relevant communities. Timely receipt of TTP information would enable organizations to apply security resources around focused, mitigation efforts, thereby increasing security effectiveness.

3. ***Foster collection and categorization of incident data to identify TTPs and other relevant information.*** A key source of TTP information lies information collected as part of an incident response effort. Greater focus is thus required around "reverse engineering" incidents to identify TTPs utilized and

[2] Tactics, Techniques and Procedures are "The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique." NIST Special Publication 800-150 (2nd Draft), April 2016.

corresponding courses of action that could mitigate such TTPs. The Department of Homeland Security is currently sponsoring a Cyber Incident Data & Analysis Repository (CIDAR) initiative to define the architecture for an incident repository (which would also provide important information for cyber insurance underwriting efforts). Discussions are also under way in other fora to achieve similar ends. A key precondition is willingness of organizations to contribute such data. Thus specific focus should be applied around how to incentivize organizations to contribute incident data to appropriate repositories, consistent with legitimate legal concerns.

4. ***Encourage development of common language for exchange of threat information.*** As organizations around the country and world develop information sharing capabilities, we see shadows of some of the same challenges that arose in the context of post-September 11th terrorism information sharing efforts. It is important to nip this risk in the bud by fostering a common language to describe the key attributes of cyber threat information.

   For data to be useful beyond an immediate context, it has to be searchable. In other words, for data to be useful in a longer term – particularly data around TTPs, Threat Actors and Incidents – it should ideally be standardized at collection. The Markle Foundation Task Force on National Security in the Information Age calls this concept "discoverability" – the "who, what, where, when" values – and analogizes to a card catalogue in a library.[3] Without standardization, it can be impossible to draw actionable information out of the data being shared.

   In a terrorism context, the National Information Exchange Model (NIEM) was developed and has formed the foundation for such capabilities as the National Data Exchange (N-DEx) system utilized by state and location law enforcement, as well as the National Suspicious Activity Reporting Initiative. In other words, these systems entail "semantic interoperability" so we can understand that what one system calls a "car" and another calls a "vehicle" is in fact the same thing.

   In the cyber context, we welcome the focus around the Structured Threat Information Expression (STIX) framework. That said, at an operational level, many practitioners today leverage the Vocabulary for Event Recording and Incident Sharing (VERIS) to manage threat TTP and incident information. VERIS includes schema for a number of aspects of cyber threat activity, including detailed categorizations for Actors, Actions, Assets and Attributes. Without resolving the issue, we recommend specific focus around defining a common language for sharing.

**Third party risk evaluation programs require greater alignment and focus around effectiveness**

While most information security guidance is focused on controls an organization should implement to secure its own environment, the reality is that most organizations operate in a much more complex ecosystem, where numerous third parties have access to each other's network and sensitive data. Managing third party risk is a

[3] *See* Markle Foundation Brief, "Meeting the Threat of Terrorism: Discoverability," available at http://www.markle.org/downloadable_assets/20090825_discoverability.pdf

significant challenge even for the most mature organizations. Likewise, third parties must also manage multiple differing requirements across customer sets. In fact, in today's complex, highly interdependent economy, many organizations – including almost all service-oriented organizations – are themselves third parties in specific business contexts, and a certain amount of schizophrenia sometimes exists between frameworks organizations would apply to themselves versus their third parties.

Approaches to managing third party risk vary widely between sectors, but even in sectors with detailed requirements, the focus can too often revolve around compliance activities instead of actual risk reduction.

We are not suggesting a single, uniform standard – requirements should vary based on level of risk. That said, we do suggest that greater attention is required across sectors on how to assess security *effectiveness* for third parties with access to critical business information and processes. Likewise, we believe a focused conversation is required around harmonizing the varied existing approaches toward consistent, risk-reducing approaches that include elements of independent validation, continuous monitoring and adaptation based on changes in threat and technology.

**Governments should cooperate to minimize the proliferation of multiple, conflicting security-related regulatory expectations**

The information security regulatory environment is becoming increasingly complex. The role of regulation should be to provide a level of assurance that reasonable risk-based controls are in place, but the proliferation of regulatory expectations across jurisdictions risks diverting valuable information security resources away from impactful risk reducing action to process-focused compliance cross-checking activities.

Organizations are already wrestling with how best to manage multiple competing state-level data breach notification requirements. Likewise, from a privacy perspective, a huge amount of compliance activity went into complying with the recently invalidated US-EU Safe Harbor framework. The recent promulgation of the EU Network Information Security Directive – which must now be implemented across multiple EU member state jurisdictions – risks adding another layer of potential conflicting information security requirements on organizations unless governments and industry collaborate quickly to harmonize approaches.

The US Government is itself in the midst of considering updates the NIST Framework for Improving Critical Infrastructure Cybersecurity.[4] It should work with industry and likeminded governments to work to harmonize expectations and guidance as much as possible around a common set of risk-based expectations.

[4] *See* "NIST Seeks Comments on Cybersecurity Framework Use, Potential Updates and Future Management, Dec. 10, 2015, *available at* https://www.nist.gov/node/771991.

Thank you for the opportunity to provide these comments. TCG welcomes any questions you may have regarding these comments.

For further information please contact:
Chris Duvall
The Chertoff Group
202-552-5280
chris.duvall@chertoffgroup.com