ENHANCING RESILIENCE THROUGH CYBER INCIDENT DATA SHARING AND ANALYSIS

The Value Proposition for a Cyber Incident Data Repository

June 2015

This document outlines the benefits of a trusted cyber incident data repository that enterprise risk owners and insurers could use to anonymously share sensitive cyber incident data and is the first in a series of white papers.

Table of Contents

Executive Summary

This paper outlines the potential benefits of a trusted cyber incident data repository that enterprise risk owners and insurers could use to anonymously share, store, aggregate, and analyze sensitive cyber incident data. Optimally, such a repository could enable a novel information sharing capability among the Federal government, enterprise risk owners, and insurers that increases shared awareness about current and historical cyber risk conditions and helps identify longer-term cyber risk trends. This information sharing approach could help not only enhance existing cyber risk mitigation strategies but also improve and expand upon existing cybersecurity insurance offerings. Rooted in rich repository data, new analytics products could help inform more effective private and public sector investment in these complementary cyber risk management categories. Specifically, such products could help promote greater understanding about the financial and operational impacts of cyber events, the effectiveness of existing cyber risk controls in addressing them, and the new kinds of products and services that cybersecurity solutions providers should develop to meet the evolving risk mitigation needs of their customers. These developments, in turn, could help drive the critical infrastructure protection and national resilience goals outlined in White House Executive Orders 13636 and 13691 and advance the risk-based approach of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.

To develop the repository concept more fully – and to assess the challenges and opportunities that the concept entails – the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) established the Cyber Incident Data and Analysis Working Group (CIDAWG) under Critical infrastructure Partnership Advisory Council (CIPAC) auspices. The CIDAWG aims to generate key findings and conclusions about the following issues: (1) the value proposition of a repository; (2) the type and scope of non-personally identifiable cyber incident data that should be shared into a repository; (3) how repository participation should be incentivized; and (4) how a repository should be structured. The CIDAWG is comprised of cyber risk mitigation experts (chief information security officers (CISOs), cybersecurity solutions providers, and other cybersecurity professionals), cyber risk transfer experts (insurers), and other cybersecurity subject matter experts from the academic and scientific communities.

During the first stage of their work, the CIDAWG participants agreed that an ideal repository would successfully store and analyze the specific types, quality, and quantity of data necessary to facilitate and incentivize more affordable and effective cyber risk management practices across multiple industry sectors. The CIDAWG participants likewise concluded that with appropriate and sufficient stakeholder input, an ideal repository would be designed to adequately address the privacy, security, and legal needs of organizations that choose to contribute that data. Finally, the CIDAWG participants concurred that an ideal repository would help empower insurers to provide more and new kinds of coverage at lower rates to clients that invest in cyber risk controls best suited to their particular cyber risk situations, as identified through repository-supported analytics.

By establishing the CIDAWG and partnering with its participants, NPPD's ultimate goal is to contribute to the relevant knowledge base about the potential benefits of a repository through the capture of

in-depth cross-sector expertise provided by the CIDAWG participants themselves. NPPD hopes to inform thinking about the needs and requirements for such a repository, whether such thinking involves (1) existing or planned repository efforts; (2) a consolidation of independent tools; or (3) a newly developed and implemented information sharing space.

The CIDAWG's deliberations about the value proposition of a trusted cyber incident data repository culminated in the identification of several core benefits likely to arise from the legally-appropriate, voluntary sharing of data about both intentional and accidental cyber incidents. Specifically, an ideal repository could help with the following tasks:

1. ***Identifying Top Risks and Effective Controls*** – A repository could provide the basis for analysis and assessments of adversary tactics, techniques, and procedures (TTPs), the effectiveness of various "in place" controls, and (potentially) attribution that could link attacks to their respective sources. A repository could also help with supply chain risk management by highlighting common supply chain cybersecurity weaknesses that merit supplier and vendor attention.

2. ***Informing Peer-to-Peer Benchmarking*** – A repository could enable companies to assess their cybersecurity postures against those of their peers and help establish a baseline for reasonable cybersecurity best practices. Among other benefits, organizations could learn about the effectiveness of methods that similar organizations have employed to avoid or remediate particular kinds of cyber incidents.

3. ***Showing Return on Investment*** – A repository could support cost-benefit analyses and budget justifications for cybersecurity investments and could help quantify risks and losses to improve cybersecurity insurance pricing and availability.

4. ***Allowing for Sector Differentiation*** – Analyses of industry-segregated and cross-industry data stored by a repository could provide insight into which kinds of cyber risks are typical within a particular sector; highlight which other sectors face similar risks; and inform which sectors could benefit most from appropriate cyber risk management investments.

5. ***Supporting Forecasting, Trending, and Modeling*** – A repository could support analyses about specific threat actors and their likely attack methods as a predicate to developing loss estimates for related cyber incidents. Such analyses could include consequence models that demonstrate the short-, mid-, and long-term cascading impacts of those incidents.

6. ***Advancing Risk Management Culture*** – A repository could help propel internal discussions about an organization's cyber risk that could improve cybersecurity governance through the promotion of more holistic, cyber risk-inclusive approaches to Enterprise Risk Management (ERM). The more widespread this development, the more it could both enhance the maturity of existing cybersecurity insurance policies and boost dynamic cybersecurity insurance models and the diverse policies they could support.

In the coming months, the CIDAWG will continue to contribute to the discussion about improving the nation's cybersecurity posture through better cyber incident information sharing. It will next tackle the challenging topics of which specific cyber incident data points should be shared into a repository to deliver on the aforementioned value propositions; the privacy protections and other characteristics that a "trusted" repository must have to make it a safe information sharing space; and how a repository should be scoped and structured during an initial operating stage in order to support the kinds of analyses that cybersecurity stakeholders require to improve their cyber risk management practices.

Introduction

The probability of cyber incidents happening – and happening frequently – has become more widely accepted in the wake of recent large-scale and highly publicized cyber attacks on several well-known retailers and industry sector giants. Repeated cyber intrusions into companies around the world, moreover, demonstrate the need for improved cybersecurity not only by holders of sensitive personally identifiable information (PII) and by owners and operators of industrial control systems (ICS) but also by all actors who use cyberspace to transact business and offer services.

The Department of Commerce Internet Policy Task Force has described cybersecurity insurance as a potentially "effective, market-driven way of increasing cybersecurity" in the private sector.[1] Despite growing interest in this market, it remains underdeveloped given a persistent lack of real-world cyber incident data needed to inform actuarial calculations and related underwriting considerations by insurers. This dearth of actionable cyber incident data has similarly stymied efforts by CISOs and other cybersecurity professionals to identify and fund the most cost-effective cyber risk mitigation investments appropriate for their organizations. Moreover, it has limited the ability of cybersecurity companies to more effectively forecast and develop the next generation of responsive technologies and other needed cybersecurity solutions.

NPPD is charged both with securing the federal .gov domain of civilian government networks from cyber attacks and with assisting private organizations in taking steps to help improve the Nation's overall cybersecurity posture. As part of those efforts, NPPD provides capabilities that are essential for the timely sharing of cyber threat and vulnerability information with stakeholders across the public and private sectors. NPPD accordingly believes that it is well-positioned to help address the increasing call for a trusted cyber incident data repository by both the risk transfer and risk mitigation communities given its overarching critical infrastructure protection and partnership mission. The development of the repository concept – in strict accordance with all applicable legal and privacy requirements – could foster the creation of a novel information sharing capability among the Federal government, enterprise risk owners, and insurers that increases shared awareness about current cyber risk conditions and longer-term cyber risk trends. This information sharing approach, stemming from analysis of data stored in a repository, could help not only enhance existing cyber risk mitigation strategies but also

[1] Department of Commerce Internet Policy Task Force, Cybersecurity, Innovation and the Internet Economy (2011) at 23-24, *available at* http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

improve and expand upon existing cybersecurity insurance offerings. Analysis that provides a better understanding of the financial and operational consequences of cyber incidents, and the cyber risk controls best-suited to address those consequences, could be a particularly valuable contribution.

Cybersecurity Insurance Workshops

NPPD has conducted several cybersecurity insurance workshops since October 2012, which have brought together diverse groups of private and public sector stakeholders, including insurers, risk managers, CISOs, critical infrastructure owners, and social scientists. Those stakeholders have examined the current state of the cybersecurity insurance market and how to best advance its capacity. During the workshops, participants:

- Identified challenges and opportunities facing the cybersecurity insurance market;
- Highlighted the importance of input from CISOs to the cybersecurity insurance discussion;
- Outlined the value of discussing the concept of a trusted cyber incident data repository; and
- Recommended continued discussion of a repository among insurers, CISOs, and other cybersecurity stakeholders.

As envisioned during the workshops, an ideal repository would store, aggregate, and analyze non-personally identifiable cyber incident data relevant to the cyber risk management community, which includes risk mitigation experts (CISOs, cybersecurity solutions providers, and other cybersecurity professionals), risk transfer experts (insurers), and other cybersecurity subject matter experts from the academic, government, and scientific communities.[2]

The Cyber Incident Data and Analysis Working Group

Following the cybersecurity insurance workshops, NPPD established the Cyber Incident Data and Analysis Working Group (CIDAWG), comprised of insurers, CISOs from various critical infrastructure sectors, and other cybersecurity professionals, under CIPAC auspices to deliberate and generate key findings and conclusions about the following topics:

1. The value proposition of a trusted cyber incident data repository, including the different types of cyber risk analysis a repository should support;
2. The type and scope of appropriate data that should be shared into a repository to realize that value;
3. How to incentivize the voluntary sharing of that data with a trusted and independently managed repository; and,
4. How a repository should be structured to function effectively during any future "alpha" stage of operations.

[2] *See* U.S. Department of Homeland Security Cybersecurity Insurance webpage and Cybersecurity Insurance Workshop Readout Reports, *available at* http://www.dhs.gov/publication/cybersecurity-insurance.

Approach

NPPD is following a three-phase approach in its effort to facilitate the conversation about how a trusted cyber incident data repository could be leveraged to improve the overall cyber hygiene of private and public sector organizations and to create the conditions necessary for a more robust cybersecurity insurance market. It is now engaged in phase two of the approach.

1. Phase 1: Engage insurers, risk managers, CISOs and other cybersecurity professionals, critical infrastructure owners, and social scientists to determine if the cybersecurity insurance market could help incentivize better cyber risk management by offering more coverage at affordable prices to companies that manage their cyber risk well.

2. Phase 2: Focus the dialogue on the concept of a trusted cyber incident data repository and how it could help meet the data and analysis needs of both the cyber risk mitigation (CISOs and other cybersecurity professionals) and cyber risk transfer (insurers) communities. Validate the outcomes of Phase 1 regarding the repository concept. Identify a full range of repository value propositions, identify and refine required cyber incident data points, and determine characteristics that would make a repository a trusted information sharing space that safeguards personal privacy.

3. Phase 3: Develop recommendations for how a cyber incident data repository notionally should be scoped and structured during an initial operating stage, desired initial outputs for cyber risk transfer and cyber risk mitigation audiences, and initial performance metrics for future iterations of a repository.

Assumptions

- This paper does not address the type or scope of cyber incident data that should be shared with a cyber incident data repository. The CIDAWG will address the question of cyber incident "data points" in its next paper.
- For ease of organization and understanding, each specific repository value proposition described in this paper is contained within one of six overarching value proposition categories. In reality, many of the specific propositions overlap with one or more of the overarching categories.
- The cyber incident data repository concept described in this paper involves a mechanism to incentivize the voluntary sharing of anonymized, non-personally identifiable cyber incident data over time among a broad array of cybersecurity stakeholders to inform cyber risk management practice generally. It is not concerned with prescribing a specific course of action in response to a specific cyber incident.
- There are currently no plans for DHS or other Federal departments or agencies to build or manage such a repository. A resulting repository could potentially be managed by a private organization.

Value Proposition Discussion

NPPD facilitated two meetings about the value proposition of a trusted cyber incident data repository in order to capture the perspectives and goals of cybersecurity insurers, CISOs, and other cybersecurity professionals. The CIDAWG participants deliberated on the following questions:

- What value might a repository provide to the insurance industry, CISOs and other cybersecurity professionals, and other stakeholders?
- What kinds of cyber risk analysis – based on what data shared with a repository – would be most useful? Why?
- What current cyber risk data and analysis gaps might a repository help fill?
    - What kinds of cyber risk analytics products already exist that repository-informed products could complement and/or supplement?
    - What new information should such new cyber risk analytics products convey?
- How could repository-informed cyber risk analysis products assist with peer-to-peer benchmarking?
- What other value might a cyber incident data repository provide?

Value Proposition #1: Identifying Top Risks and Effective Controls

The CIDAWG participants cited the identification of top cyber risks and the security controls that are most effective in addressing them as one of the major potential benefits of a repository. A repository could provide assessments of adversary TTPs, the effectiveness of various "in place" controls, and (potential) attribution that could link attacks to their respective sources. It likewise could inform stakeholders about which root causes and vulnerabilities have been exploited during a cyber incident and illuminate any common underlying strengths and weaknesses within industry sectors or sub-sectors – information that would help companies establish and prioritize effective standards for protective measures. By showing the relationship between the presence (or lack) of certain controls and cyber incident losses, moreover, repository users could gain needed insight into control "gaps" and associated costs (damages and remediation), how best to mitigate future incidents, and how to reduce incident response and recovery times.

The CIDAWG participants agreed that a repository also could benefit supply chain risk management efforts by supporting analysis that allows companies to identify the impact and/or role of a vendor's security product or service during an incident. Leveraging such analytic products, they noted, would allow companies to develop cybersecurity statements, policies, and procedures for their vendors on a much shorter turnaround time than currently is possible.

Value Proposition #2: Informing Peer-to-Peer Benchmarking

The CIDAWG participants concurred that repository-supported analysis could help organizations conduct peer-to-peer benchmarking and provide greater knowledge about their peers' actual cybersecurity

practices. Several asserted that if a company discovers that it falls in the bottom fifty percent as compared to its peers when it comes to cyber risk preparedness, that knowledge could motivate the company to increase its cybersecurity budget and related mitigation efforts. They reported, however, that most companies today have almost no insight into how they "rank" against their peers when it comes to such preparedness and/or performance. Other participants asserted that they have only limited knowledge about what their peers are doing regarding the implementation of cyber risk controls, their scope, and how those controls fit within overall cybersecurity strategies.

Repository-supported analysis could help address these shortcomings by enabling organizations to measure cybersecurity preparedness and/or performance as something other than a percentage of the information technology (IT) budget. Specifically, such analysis could provide insight into what steps their peers have taken to avoid or remediate particular kinds of cyber incidents, at what cost, and with what effect. Such insight could help CISOs and other cybersecurity professionals make the case for their cybersecurity budgets to boards of directors and other senior leaders. That case would be strengthened to the extent that such analysis (1) facilitates more accurate assessments of a company's exposure to known cyber risks; and (2) enables a company to compare its actual cyber incident experiences against those of its peers.

As technology evolves, analysis of repository data likewise could help establish a cybersecurity preparedness and performance "floor" when it comes to meeting applicable industry standards of care and/or best practices (e.g., the NIST Cybersecurity Framework). Among other things, such analysis could establish a post-breach understanding of the "reasonableness" and "cost-benefit" of commonly implemented controls in place at the time of a breach. Such knowledge could help organizations better respond to negligence claims, help them eliminate redundant controls, and facilitate lower audit costs.

Value Proposition #3: Showing Return on Investment

Various CIDAWG participants asserted that trusted repository-supported analysis could help them tie specific cybersecurity controls and their associated successes and failures to the level of losses resulting from a particular cyber incident. For example, such analysis could help identify which controls had the most success in reducing incident response times and the overall magnitude of harm. That information, in turn, could help improve the ability of insurers to price policies by enabling comparisons between similar cyber incidents – i.e., comparing the costs of incidents experienced by companies that had specific cyber risk mitigation measures in place against others that did not have those same measures in place.

Various CIDAWG participants emphasized the need to frame cyber risks and corresponding controls to support cost-benefit analyses that help prioritize and advocate cybersecurity investments in ways that are meaningful to boards of directors and other senior business leaders. Insurers, for example, could help CISOs frame their cyber risk management requirements in business terms by telling companies that they are not insurable, or that their insurance liability will increase, unless they meet certain cybersecurity requirements that repository-supported analysis could help identify. CISOs, in turn, could use such analysis to better support their cybersecurity budget justifications by showing how particular

investments could help avoid significant cyber incident costs over time. According to one participant, the ability to provide this insight, as informed by actual but anonymized cyber incident data, represents the biggest potential value of a repository.

Value Proposition #4: Allowing for Sector Differentiation

The CIDAWG participants concurred that aggregated cross-sector cyber incident data could offer the "best bang for the buck" when it comes to understanding cyber risk at a high level. They emphasized, however, that differentiation of cyber incident data by industry sector also has benefits that a repository should pursue. For example, they explained that for companies, such industry-segregated data – coupled with more general cross-industry data – would allow for the determination of which kinds of cyber risks are typical within a particular industry sector, while at the same time highlighting not only which other sectors face similar risks, but also what those sectors have done to address them.

The CIDAWG participants noted that different industries tend to experience different cyber incidents and risks – for example, routine credit card hacks or hacktivist denial of service attacks for some and sophisticated attacks aimed at sabotage, large-scale theft, or espionage for others. They observed, however, that particular attack vectors often are used during cyber incidents against multiple industry sectors. Given this dynamic, companies increasingly need to know not only what is happening to their most immediate industry peers, but also to other companies across the entire cybersecurity ecosystem. Through repository-supported analytics that provide this knowledge – supported, for example, by the proper use of metadata and a good data search and selection capability – companies would be better positioned to tailor cybersecurity approaches to the cyber risks most relevant to their industry sector while learning from the experiences of companies in multiple other sectors.

Several CIDAWG insurance participants concluded that a company that uses certain best practices appropriate to its industry sector, as informed by both sector-specific and complementary cross-sector cyber risk analyses, would be a more attractive client to insure.

Value of Industry-Specific Data

The CIDAWG conversation revealed that insurers, CISOs, and other cybersecurity professionals are interested in industry-specific data – not only in terms of threat (who is being targeted and how), but also in terms of effective (and ineffective) cyber risk mitigation approaches. For insurers, industry sector differentiation would provide insight into which industries are at higher cyber risk – knowledge that, in turn, would help them not only differentiate insurance pricing terms and conditions but also offer more cost-effective insurance policies in response. Repository-supported analysis could help identify, for example, which cybersecurity best practices industrial control systems (ICS) operators should implement as a prerequisite to obtaining cybersecurity insurance. Anonymized data shared into a repository about an ICS operator's cybersecurity practices at the time of a cyber incident likewise could inform trend analysis that could correlate best practices with the amount of loss – e.g., which practices identified in the NIST Cybersecurity Framework most effectively prevent or mitigate losses and which practices meet with less success?

Value of Regional Data

According to the CIDAWG participants, another argument for industry sector differentiation is the fact that multinational organizations often experience regional differences in their "cybersecurity context" across their various operating locations worldwide. European countries have different standards for privacy protections that can affect what controls a company can or cannot deploy in its network architecture. Other countries, moreover, value different types of data differently. For instance, PII and intellectual property (IP) data are valued differently in various countries with very different legal regimes. Having servers in countries without strong legal IP protection, for example, could increase the risk of attack on those systems given potentially insufficient law enforcement mechanisms and/or lenient criminal penalties that a malicious hacker might face. In addition, international subsidiaries of the same company may face different legal and regulatory regimes depending upon their locations, adding further complexity into the cyber risk management mix. Regional differences, if better understood through repository-supported analytics, therefore could significantly affect how cyber risks are most effectively prioritized, mitigated, and/or transferred through insurance.

Impact of Seasonal Conditions on Cybersecurity

The CIDAWG participants likewise commented that local conditions (i.e., seasonality) can affect the "rhythm" of a company's cybersecurity operations. For instance, heavy shopping periods in a particular country may increase the likelihood of attempted retail attacks, while significant religious, historical, or political dates, and ongoing social issues, may inspire hacktivists and other cyber criminals to action. A trusted cyber incident data repository that facilitates analyses of these factors could be used to better plan for non-technical cybersecurity measures such as increased analyst coverage or timely training materials alerting company personnel to the increased likelihood of phishing attempts or other attacks.

Value Proposition #5: Supporting Forecasting, Trending, and Modeling

Various CIDAWG participants commented that a well-designed repository could offer value beyond the mere aggregation of data by supporting analyses aimed at closing gaps in cyber risk management, situational awareness, prediction, and response and recovery activities. For instance, more information on insider threats and the frequency of various types of attacks could be helpful in informing cybersecurity investments. This would enable companies to focus on a particular subset or family of controls that have the greatest effect against the most common types of attacks. Over time, the ability to progress from descriptions of incidents that occurred, to inferential analyses, to predictive analyses, would promote the establishment of ranges of cyber incident costs – including minimum-maximum loss estimates. Moreover, repository data could enable analyses of various data point combinations such as threat actors by industry, attacks associated with the highest losses, types of attacks compared to targets, or trends in attack motivation. Such analyses could identify, for example, gradual or sudden changes in likely threat actors and consequently the TTPs for which companies should be on guard.

Analysis of Long-Term Impacts and Cascading Effects

Another area of considerable interest to the CIDAWG participants was the extent to which a repository could enhance their understanding of both the immediate and long-term impacts and consequences of

cyber incidents. Several noted that a repository could help shed light on cascading effects by supporting the modeling of real-world cyber events. Critical interdependencies that such models might reveal are of particular concern to insurers because their interest in a cyber event may extend to more than one insured party. This may be the case, for example, among partnering (and insured) companies across multiple supply chains. Repository-enabled analyses that show the cascading effects from a particular kind of cyber incident to be a frequent and/or likely occurrence could be used to boost the insurer case for addressing supplier and vendor cybersecurity as a condition for insurance coverage.

Correlation with Government Data Sources

Another input to a repository that could help insurers and industry conduct more accurate risk assessments would be the inclusion of government-derived threat information. Ideally, sanitized repository information shared by NPPD, law enforcement, and other government threat information sources – in strict accordance with all applicable legal and privacy requirements – could be triangulated against data from commercial cybersecurity providers, as well as observations from the companies themselves, to add insight into the sophistication of various actors and attacks. This would help inform how responsive risk mitigation steps should be prioritized and executed and what investments insurance companies should insist upon as a condition for initial and continuing coverage.

Value Proposition #6: Advancing Risk Management Culture

Rapid Adaptation to Evolving Cyber Risks

The CIDAWG participants observed that the cyber risk landscape is inherently unpredictable due to the constant change of attack vectors, a characteristic that requires a unique risk management approach that addresses both the virtual and physical dimensions of effective cybersecurity. Unlike patrolling night guards or sprinkler systems for fire risk mitigation, no hard and fast set of cybersecurity controls exists that will work consistently over time in protecting against the "next" cyber incident. Several CIDAWG participants commented, however, that the combination of a rapidly evolving risk management environment and the availability of large amounts of near real-time cyber incident data through a repository could shift industry's relationship to the insurance community by making both stakeholders more dynamic and adaptive. Specifically, a repository that regularly captures and analyzes legally-appropriate cyber incident data as incidents evolve could enable more rapid adaptation in both the risk assumptions and mitigation approaches that undergird current "defense in depth" strategies. Such progress, in turn, could lead to the development of new cybersecurity insurance policies that prompt insurers and insureds to be in regular communication about changing risks and what steps insureds should take to address them. This more interactive approach, they asserted, could incentivize better cyber risk mitigation investments by insureds over more relevant timeframes. Specifically, insureds who quickly and effectively address changed cyber risk circumstances could be "rewarded" with meaningful (and continued) coverage at affordable rates. In the process, the risk of cyber losses to both insureds and insurers could be lowered.

Enhanced Discussion of Cyber Risk Management

Many CIDAWG participants agreed that a repository that enables the evaluation of cyber risk trade-offs would enhance corporate discussions about risk and risk tolerance. They noted that such a repository

could help foster these discussions by enabling comparisons – specifically, between: (1) the cost and effectiveness of controls (risk mitigation) and the cost of insurance (risk transfer); and (2) the potential costs of a breach if vulnerabilities are left unmitigated and if a company remains uninsured (risk acceptance). One participant cited the particular value of such comparisons when it comes to accidental cyber incidents. Over time, such incidents could be analyzed to determine whether organizations learn from them and enhance their cyber risk postures accordingly.

The CIDAWG participants emphasized that cyber risk management should not be about "transferring risk from one balance sheet to another." It instead should be viewed as the catalyst for driving an enterprise-wide risk management approach that involves not only the Board of Directors but also relevant stakeholders in IT, legal, acquisition, risk management, R&D, finance, supply chain, human resources and communications. Buy-in from and involvement by all these groups, the CIDAWG participants continued, is ultimately essential for a truly improved cybersecurity posture. Put simply, real-world cyber incident data and analysis that enables companies to more accurately assess their cyber risk profile could help inform and incentivize more effective cyber risk management strategies at every level of an organization.

Conclusion

NPPD is following a three-phase approach in its effort to facilitate conversation about how a trusted cyber incident data repository could be leveraged to improve the overall cyber hygiene of private and public sector organizations in order to create the conditions necessary for a more robust cybersecurity insurance market. The CIDAWG has initiated a dialogue to evaluate the proposition that the voluntary sharing of anonymized, non-personally identifiable cyber incident data through such a repository could support the creation of much desired consequence and other analysis that informs:

- Risk mitigation strategies of CISOs and other cybersecurity professionals on the day-to-day cybersecurity front lines and the investments that their organizations make to address their unique cyber risk profiles;
- Research initiatives and related product and service development plans of forward-looking cybersecurity solutions providers; and
- Insurer efforts to scope, price, and provide existing and new cybersecurity insurance policies that effectively transfer cyber risk by drawing upon new streams of actuarially relevant information.

Over the first several months of this effort, the group has exhaustively debated and ultimately validated the value of this overarching proposition. While not all-inclusive, the following benefits of a repository were identified by insurers, CISOs, other cybersecurity professionals, and outside experts:

1. Identifying Top Risks and Effective Controls
2. Informing Peer-to-Peer Benchmarking
3. Showing Return on Investment

4. Allowing for Sector Differentiation
5. Supporting Forecasting, Trending and Modeling
6. Advancing Risk Management Culture

Executive Orders 13636 and 13691 and the NIST Cybersecurity Framework make clear that enhanced information sharing that facilitates effective cyber risk management across industry sectors is a national (and economic) security imperative. As the CIDAWG's conversation develops through future discussions, NPPD's goal is to answer three key questions:

- Do existing repositories meet the cyber incident data needs of cybersecurity stakeholder groups?
- Are owners and operators of existing repositories open to leveraging the knowledge that the CIDAWG develops – regarding needed cyber incident data and analysis and the best ways of sharing it – and incorporating it into their existing structures?
- If not, should a new cyber incident data repository be developed?

As the number, scale, and sophistication of cyber incidents around the globe continue to mount, the importance of facilitating and incentivizing more informed cyber risk management and investment through enhanced information sharing cannot be over-emphasized. Determining the value of a trusted cyber data incident repository is only the first step in this inquiry. In the coming months, the CIDAWG will continue the discussion by addressing additional topics that are core to the repository concept, including: which specific cyber incident data points should be shared into a repository to deliver on its value propositions; the privacy protection and other characteristics that a "trusted" repository must have in order to make it a safe information sharing space; and how a repository notionally should be scoped and structured during an initial operating stage in order to support the kinds of analyses that cybersecurity stakeholders across every sector require to improve their cyber risk management practices.