CCTI Center on Cyber and Technology Innovation
LOCKTON

The Time for Cyber Insurance: Coverage Improves Supply Chain Resiliency

Rapporteur Summary of FDD-Lockton Companies Tabletop Exercise

By Trevor Logan

September 2, 2020

Introduction

Insurance has a long and proven history of helping insured parties reconstitute and recover from an unforeseen incident. In the digital age, insurance can help firms overcome the financial burdens of a significant cyber disruption. Yet experts continue to debate whether modern insurance can improve corporate cybersecurity, and if it can, what practical mechanisms would be needed to do so.

On March 11, 2020, the congressionally mandated Cyberspace Solarium Commission (CSC) published a report aimed at answering these and other critical questions.[1] The product of nearly a year of careful study by experts from across the U.S. government (USG) and private sector, the CSC report concluded that a "robust and functioning market for cyber insurance could play a … role in identifying and regulating behavior to improve cyber risk management." As the report notes, however, "the market for cyber insurance is failing to deliver on this potential." The CSC identified various reasons for this failure, ranging from a lack of "underwriters and claims adjusters … who understand cyber risk," to "insufficient or inconsistent models" for measuring cyber risk, to "the notion of silent cyber risk—the cyber risk inherited from other insurance offerings, such as general corporate liability or property and casualty coverage."[2]

In January 2020, to help identify ways to improve the cyber insurance market and support the CSC's work, FDD's Center on Cyber and Technology Innovation (CCTI) hosted a tabletop exercise in conjunction with Lockton Companies' Critical Infrastructure and Global Cyber & Technology practices.[3] The exercise's participants included former senior government officials as well as private sector leaders from the insurance industry and defense industrial base (DIB) companies, which are among the most in need of cyber insurance.

1. The CSC was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences." For more information, visit the CSC website: U.S. Cyberspace Solarium Commission, "United States of America Cyberspace Solarium Commission," accessed August 5, 2020. (https://www.solarium.gov/)

2. U.S. Cyberspace Solarium Commission, "United States of America Cyberspace Solarium Commission Report," March 11, 2020, page 81. (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view)

3. Prior to the exercise, CCTI published a study examining cyber insurance as a solution to address private sector resilience against cyberattacks. See: Nour Aburish, Annie Fixler, and Michael Hsieh, "The Role of Cyber Insurance in Securing the Private Sector," *Foundation for Defense of Democracies*, September 13, 2019. (https://www.fdd.org/analysis/2019/09/11/cyber-insurance/)

Rather than explore hypothetical scenarios, the exercise worked through case studies of actual cyber events that have affected the DIB. The exercise examined the benefits, limitations, and costs of cyber insurance in these scenarios in light of the range of cyber threats facing the private sector.

The following memo highlights the recommendations for the USG, private sector, and insurance industry that flowed from the expert discussion during the exercise. Where these recommendations map onto CSC recommendations, the memo notes this overlap.

The most important finding from the exercise was that ubiquitous application of cyber business interruption (cyber BI) coverage across the Department of Defense's (DoD's) supply chain would materially improve supply chain resiliency and reduce unwanted supply chain behaviors throughout the DIB.

While its likely effects are difficult to measure in their totality, the application of this type of insurance would materially reduce the likelihood of bankruptcies or cash-flow constraints resulting from a systemic cyberattack or from a typical ransomware attack that freezes a contractor's operations. Furthermore, the insurance reimbursement for a covered cyber disruption would reduce financial pressure on the affected contractor to find product substitutions from what may be an unvetted supplier in order to meet contractual terms. Cyber BI coverage is widely available in today's cyber marketplace. Yet due to a lack of Defense Federal Acquisition Regulation Supplement requirements, many critical DIB businesses still lack this important coverage.

Cyber insurance is no longer a discretionary purchase as it was years ago. With more buyers and policyholders, more underwriting data from applications, and more claims, insurers can more realistically price around exposures and controls and can better reward those companies with better controls.

Scene Setter: The Current Marketplace for Cyber Insurance and What Is Insurable

Cyber insurance is a $4.5 billion market and is expected to grow to $21.4 billion by 2025,[4] making it the fastest-growing business segment in the insurance industry. The proliferation of insurance technology companies entering the market, along with competition for market share between long-established insurers, continues to widen the availability of coverage and keep premium prices relatively low.

In 2018, there were 528 U.S. insurers writing cyber insurance policies, up from 471 in 2017.[5] When analyzing cyber insurance pricing for the government and defense contracting industries, Lockton's proprietary analytics show a median price of $10,000 per $1,000,000 of coverage, a rate of 1 percent. While prices can vary depending on a company's particular circumstances and needs, this 1 percent median rate provides a solid indicator of cyber

4. Laura Wood, "Global Cyber Insurance Market Report 2019-2025: Market Size is Expected to Reach $21.4 Billion - ResearchAndMarkets.com," *Businesswire*, December 13, 2019. (https://www.businesswire.com/news/home/20191213005215/en/Global-Cyber-Insurance-Market-Report-2019-2025-Market)

5. "State of the Cyber Insurance Market— Top Trends, Insurers and Challenges: A.M. Best," *Insurance Journal*, June 18, 2019. (https://www.insurancejournal.com/news/national/2019/06/18/529747.htm)

insurance pricing in the industry class. Given the average cost of an uninsured data breach, which IBM cites as $8.19 million in the United States, the risk is difficult for companies to bear alone.[6]

For DIB, cyber disruptions can result in:

- Failure to perform under contract
- Delay to overall production schedule
- The need to find replacement parts from third party that may not be certified by DoD
- Potential bankruptcy (which, in turn, can cripple supply chains or create national security concerns by exposing sensitive assets to purchase by a foreign adversary)

According to Lockton's proprietary DIB and government contractor benchmarking, the average contractor is purchasing $10 million in limits, with an average of $5 million in limits for companies generating under $100 million in annual revenue, and an average of $30 million in limits for companies generating between $1 billion and $2 billion in revenue. These relatively low limits suggest companies are purchasing the minimum amount of insurance necessary to satisfy contractual requirements, without regard for their actual risk exposure. For comparison, according to Lockton's experts, the insurance industry has recorded cyber insurance limits of up to $700 million.

Finally, traditional cyber insurance models are based largely on handling Personally Identifiable Information or Personal Health Information, of which a manufacturer or technology company may have little. Models based on outage times calculated in business continuity and disaster recovery plans provide a superior method of estimating cyber BI risk and the amount of coverage businesses should purchase.

Instead, the following cyber risks are most relevant to DIB companies:

- Breach of any kind (insurable)
- Supply chain disruption to a company, its suppliers, and/or its customers (insurable)
- Cyberattack with kinetic outcome, such as an explosion (insurable)
- Altering manufacturing specifications or data (uninsurable)
- Theft of intellectual property (partially insurable)
- Act of war with kinetic impact (uninsurable)

Having proper cyber insurance reduces risk both for individual companies and for the DIB supply chain overall. Figure 1 shows the coverages and services currently available through cyber insurance providers. Oftentimes, companies base their decisions to procure cyber insurance as much on the services provided as on the size of the payouts.

6. "How much would a data breach cost your business?" *IBM Security*, April 2019. (https://www.ibm.com/security/data-breach). For small businesses without insurance, the average direct cost of an uninsured data breach exceeds $36,000. While that number may appear low, it does not include the cost of lost productivity from having to divert resources from regular business activities toward clean-up and recovery. For small businesses that operate with a small profit margin, these out-of-pocket costs may be too much to bear. "Small Businesses: The Cost of a Data Breach Is Higher Than You Think," *First Data*, 2014. (https://www.firstdata.com/downloads/thought-leadership/Small_Businesses_Cost_of_a_Data_Breach_Article.pdf).

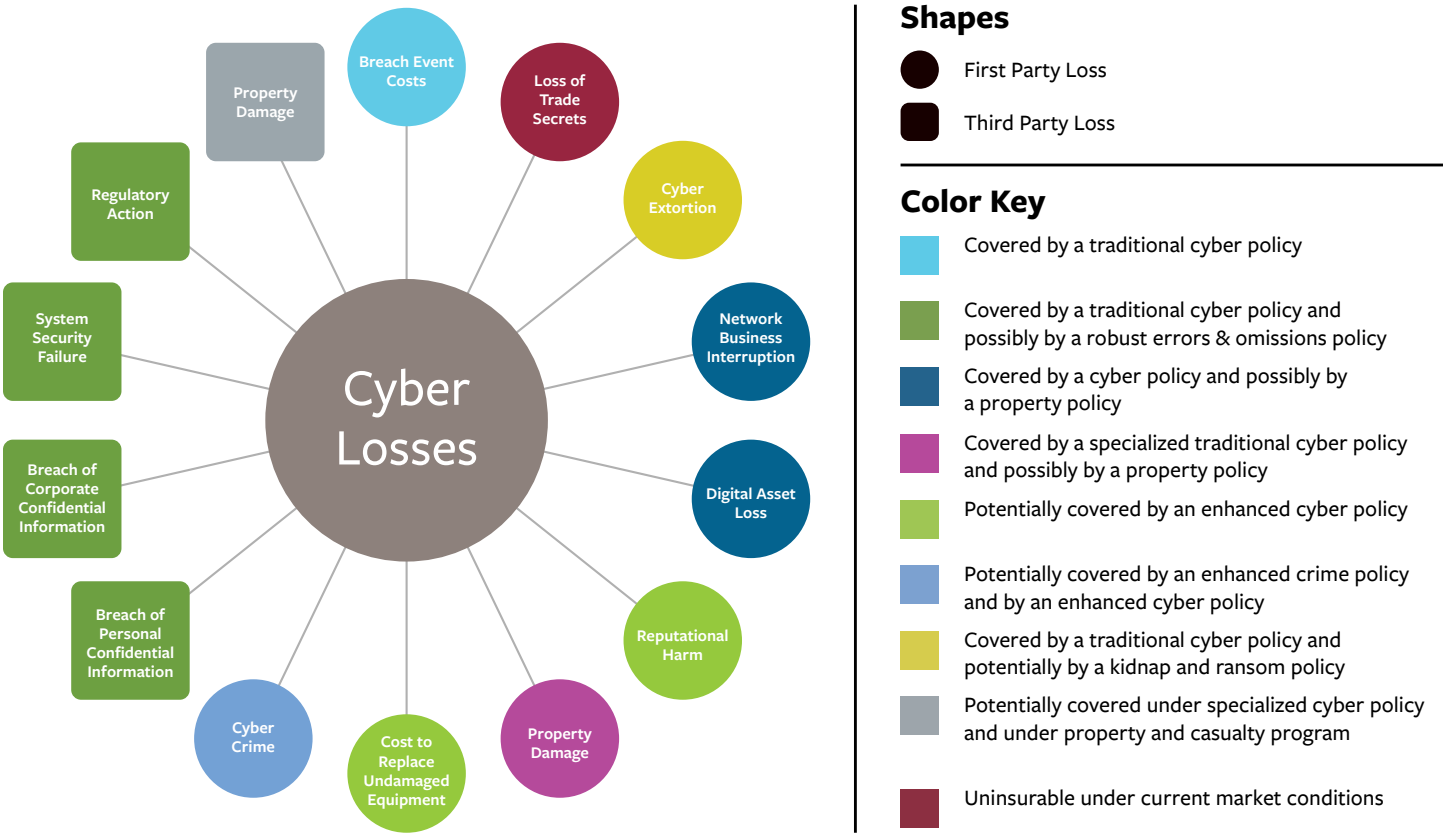

Figure 1: Coverage for Cyber Risk

Risk mitigation services provided by insurers

- Risk assessment tools
  - Written self-assessments
  - Technological solutions to rate companies
  - Limited consultations with risk assessment professionals
- Employee training materials and courses (phishing, etc.)
- Tabletop exercises
- Sample policies and procedures for cyber risk management and information governance
- Access to web portals providing cyber risk information and risk management information
- Risk management budget (for large companies)

Response services provided by insurers

- Breach coach
- Cyber forensics
- Breach notification vendor
- Public relations assistance
- Attorneys
- Loss adjuster/forensic accountant
- Ransom negotiator (ransomware)
- Data restoration services
- ID & credit monitoring for individuals

As the CSC report notes, the "lack of clarity about what security measures are effective in reducing risk,"[7] along with the rapid and continuous evolution of the threat, has created difficulties for the insurance industry given its longstanding practice of building models based on historical data. The industry's approach to addressing the lack of data required for effective modeling has been to invest in, or partner with, cyber-risk scanning and cyber-data aggregating companies. While still relatively ineffective at accurately pricing exposure, the industry has grown increasingly comfortable with the current coverages provided.

7. U.S. Cyberspace Solarium Commission, "United States of America Cyberspace Solarium Commission Report," March 11, 2020, page 78. (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view).

Key Findings and Recommendations

***Key Finding 1*: No amount of money spent on cyber defense will make a company 100 percent un-hackable, so companies should prepare for the worst. Cyber BI coverage is widely available and is now almost always excluded from traditional property insurance policies.**

The safe course for any company is to assume it will suffer a cyber breach and that its "traditional" policies will not cover this costly event. After initial investments in cybersecurity and cyber hygiene, there is a point at which additional investment in preventive measures is no longer cost-effective. The next dollar spent in those areas will reduce cyber risk by only a marginal amount.

Cyber insurance, on the other hand, can shift the entire risk curve (as shown in Figure 2) and thus provide a cost-effective way to capitalize risk mitigation and optimize recovery. For example, investing an additional $1 million in security technology may yield a 0.1 percent improvement in security posture. An investment of $1 million in cyber insurance, however, may provide $100 million in risk capital to efficiently and effectively capitalize risk mitigation, response, and recovery resources. In short, cyber insurance (with cyber BI coverage) will reduce a company's exposure to losses from a cyber event and significantly improve the resiliency of the insured company by strengthening its ability to protect critical assets during a breach and to expedite response and recovery. This is relevant for small, medium, and large companies alike, as all companies seek to avoid unbudgeted earnings losses. These unbudgeted losses can hurt the share prices of even the largest publicly traded companies.

- Cyber insurance significantly shifts the security curve with minimal investment.
  - Ex: $1M for $100M in risk mitigation, response, and recovery capitalization
  - The law of diminishing marginal returns makes insurance the more effective use of residual risk capital after appropriate investments in security have been made.
  - Capitalization of business disruption in the supply chain
- A single cybersecurity event can be significantly disruptive to the DIB as a whole and may put smaller and less profitable contractors out of business.
- Capitalization of world-class cyber-risk service providers strengthens a contractor's ability to protect critical assets during a breach and expedite response and recovery.
- Risk assessment is an inherent part of insurance underwriting and can provide valuable information to DIB contractors about their security posture.
  - Lockton believes that an 800.171(B) compliance assessment can become part of the built-in risk assessment process for contractors. Zurich Insurance is currently working on a solution.
- More and more insurers are including cybersecurity scanning and measurement as part of their underwriting process.

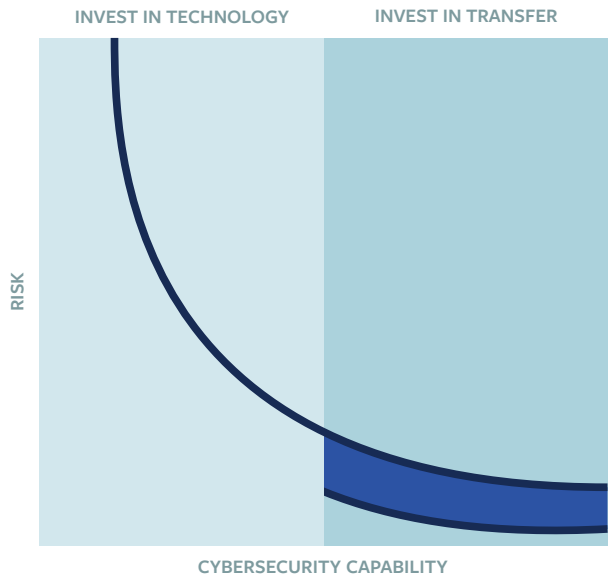

Figure 2: Purchasing Cyber Insurance Decreases Cyber Risk

Notably, however, the risk curve for government contractors looks slightly different because the USG requires contractors to comply with cybersecurity standards. The USG evaluates compliance on a binary scale: companies are either in compliance or not.

As noted by one tabletop participant: "I would encourage the government to begin to think more about this continuum and making that decision of where do you want to sit on that curve. This is the broader set of how much you want to invest in security and how much of that is for cybersecurity itself versus risk transfer."

Recommendations

1. The USG and DoD should undertake studies to gain a quantitative understanding of how the ubiquitous deployment of cyber insurance across the DIB and government contractor industries will shift the security and resiliency of the industries' supply chains.

2. The USG, including DoD, should thoughtfully determine cyber coverage standards, including but not limited to: underwriting, policy coverage, and insurer education certifications. Cyber insurance standards, however, must not become another bureaucratic rubber stamp. Therefore, the USG should implement a process for regular reevaluation of coverage standards and the metrics for judging companies' compliance with these standards, based on evolving cyber-threat data gathering and risk assessments.

3. The USG should require first-party cyber BI coverage throughout the DIB by defining "cyber insurance" coverages in the Defense Federal Acquisition Regulation/Federal Acquisition Regulation to include cyber BI coverage. This would significantly reduce the complexities and costs of third-party supply chain coverage for any one vendor.

4. Insurance providers should specify whether a given policy covers direct and/or indirect attacks, whether physical damage occurs or not.

5. When calculating the appropriate limits, the insurance industry should take into account the given firm's business continuity and disaster recovery plan information, along with Property Business Interruption/ Contingent Business Interruption values. By applying loss-of-income calculations associated with an operation or many operations to the technology infrastructure that supports those operations, the industry can improve the accuracy of the probabilistic models used to develop cyber BI insurance limit recommendations. Over time, this will allow limit benchmarking to become a more useful tool.

6. As the CSC noted in its report, "Congress should resource and direct the Department of Homeland Security [DHS] to fund a federally funded research and development center to work with state-level regulators to develop certifications for cyber insurance products."[8]

7. Additionally, as the CSC urged, "The executive branch should establish a public-private working group at DHS to convene insurance companies and cyber risk modeling companies to collaborate in pooling and leveraging available statistics and data that can inform innovations in cyber risk modeling … particularly with regard to dependency mapping and the consequences of cyber disruptions."[9]

8. Ibid., page 80.
9. Ibid.

***Key Finding 2*: When done correctly, the process of acquiring cyber insurance helps companies understand the overall threat environment and identify their at-risk assets. If cyber insurance is to be mandated for the DIB, it should be done in a manner aligned with business operations.**

A growing number of insurers are providing meaningful pre-attack services, including risk assessments (that is, do-it-yourself questionnaires or outside assessments measured against peer companies), technology (such as hardware) to repel attacks, employee training (such as anti-phishing), and tabletop exercises. When done well, the process of acquiring cyber insurance can help companies understand the overall cyber threat environment and identify at-risk assets.

Too often, the relevant corporate departments – general counsel, chief security officer, chief financial officer, and chief revenue officer – are siloed, with each department incorrectly believing it understands the company's assets. Only when a company brings those people together for a tabletop exercise does the company get a full picture of the enterprise-wide risk. In some larger companies, chief information security officers (CISOs) are taking an active role in defining cyber insurance coverage terms that are an extension of the CISO's overall security platform. This includes defining service providers as well as insurance coverage terms and limits to match exposure basis.

The efficacy of the services provided by insurers can vary depending on how the findings are used by the provider and by the company itself. Nevertheless, as one participant emphasized, "It could be great even just going through the process. [That experience] could provide tremendous educational benefits to a potential insured… [Additionally, the experience] will allow a deep look at the systems, to assess [them] for insurability… [Y]ou're going to learn a lot from this."

Recommendations

8. The cyber insurance industry should require tabletop exercises as part of the underwriting process so that clients understands which assets are at-risk and need to be insured. Property insurers ask whether a company has and exercises business continuity plans. Whether self-administered by the company or led by the insurance broker, cyber tabletops – complete with documented evidence and results from the company – must become a routine and widely accepted practice.

***Key finding 3*: At present, there are unclear and sometimes conflicting standards and models for cybersecurity, leaving companies – especially the small- and medium-sized enterprises critical to the DIB – confused and uncertain. Some insurance companies are seeking to underwrite to Cybersecurity Maturity Model Certification (CMMC) guidelines. DoD could advocate for this approach (or others) to be included in cyber insurance underwriting and could help socialize these guidelines to the broader DIB.**

One participant lamented, "What the DoD has said publicly and privately is that they are not doing anything other than a checklist. If you get hacked, we're going to dump on you like a ton of bricks because clearly compliance doesn't mean protection. So this has left companies in a bit of a bind. [On top of that, all companies that want to be part of a] defense contract will have to have a certificate at some level. Interestingly enough, this is only for protection of unclassified but sensitive data, controller classified information, the definition of which is arbitrary, non-consistent and different from contract to contract or office to office."

By enabling contractors for the USG, including DoD, to carry policies underwritten in part to the CMMC standard, the USG can shift the cost-burden of compliance assessment away from the contractor and toward the insurance company. As one participant noted, "I think the way to get to the heart of it is… If contractor X can't meet your contractual obligation, insurance can help or we can incentivize them. The government has to incentivize them to find ways of having backups and hardening those backups." This strategy would reduce a contractor's overall cost of compliance and insurance, perhaps even providing a net benefit to the contractor, depending on the cost of assessment against the amount of insurance purchased. And, at the same time, because every insurance company has an underwriting assessment process, including the CMMC assessment in underwriting would not have a direct negative cost impact on insurance companies.

Recommendations

9. DoD should require that "cyber policies" issued to any defense contractor be underwritten to at least CMMC standards and any additional criteria suitable to the insurance company. Doing so will efficiently satisfy CMMC compliance and promote adoption of cyber insurance in the DIB.

10. The USG and insurance industry should encourage insurers and insurance brokers to offer CMMC as a consultative service offering, thereby eliminating cost redundancies for the DIB and USG contractors.

11. The USG should permit certifying bodies to include as evidence of compliance cyber insurance underwriting in which CMMC guidelines are followed.

12. At the same time, deeming insurance companies "certified assessors" introduces errors & omissions risk that may pose a new burden for an industry that is used to underwriting to, but not certifying, the insured's compliance. The USG, including DoD, should explore ways to accept the insurance company's assessment as evidence of compliance.

13. As the CSC recommended, Federal Acquisition Regulation should be updated such that "upon the development of cyber insurance policy certifications," USG "contractors maintain a certified level of cybersecurity insurance and explore whether the Cybersecurity Maturity Model Certification should be updated to require cybersecurity insurance."[10]

14. As the CSC recommended, the executive branch should establish a public-private working group to "conduct research on the applicability and utility of common frameworks, controls, and 'essentials' as baseline requirements for reducing premiums in pricing insurance risk, such as the NIST [National Institute for Standards and Technology] Cybersecurity Framework and the International Organization for Standardization/ International Electrotechnical Commission (ISO/EIC) 27000 standards family."[11]

***Key finding 4*: Without more robust and expansive data gathering and risk assessment, the cyber insurance industry – and the DIB it serves – will not mature as quickly as needed.**

During the exercise, a participant highlighted the current "dearth of data." This participant noted that there is "no way to correlate breaches to claims to cyber posture across an industry." This participant noted that legislation

10. Ibid., page 83.
11. Ibid., page 81.

could force broader sharing of data. Legal protections would also enable companies to share breach data without the risk of legal exposure.

Part of the reason for this lack of data is that no regulatory regime exists that penalizes and rewards companies for their investments in cybersecurity. The Occupational Safety and Health Administration's (OSHA's) Experience Modification Rate, for example, determines the price of workers' compensation insurance based on companies' safety practices. This regulatory body collects data on workplace injuries and illnesses, and in turn, this data helps OSHA better understand how to protect the health and safety of the American workforce. The regulations pertaining to this program require employers to record and report workplace injuries, illnesses, and fatalities.

In the OSHA model, employers with 10 or more workers must report serious work-related injuries and illnesses. There are exceptions to the reporting requirement, but as a general rule, employers must report illnesses and injuries requiring medical treatment beyond routine first aid. Then, a company's number of OSHA "reportables" and its incident rate correlate directly with the company's price of workers' compensation insurance, as determined through a rating index called Experience Modification Rate, or MOD rate. If a company's MOD rate is 1.0, it pays the industry's average rate. However, if the company's MOD rate is .80, it pays 20 percent less than the industry rate; conversely, if the MOD rate is 1.2, the company pays 20 percent more than the industry rate. There is no similar reporting requirement or rating index for cybersecurity.

Another component of the problem is that cyber insurance limits tend to be driven by Personally Identifiable Information or Personal Health Information, but manufacturers and contractors typically do not maintain a significant amount of this type of data. The typical cyber insurance quantitative models used to advise clients do not accurately measure losses associated with an operational or supply chain disruption – the critical driver of loss in the DoD and USG supply chains.

Recommendations

15. Congress should empower the Cybersecurity and Infrastructure Security Agency (CISA) to serve as the cyber equivalent of the Department of Labor's OSHA. Doing so will help the USG both resolve data shortage issues in the cyber arena and efficiently connect cyber insurance prices to company practices. OSHA provides a longstanding precedent and model that the USG can apply to the cyber realm.

    - Like OSHA, a CISA federal-level program would allow for variations among states' statutory requirements. At the same time, the federal program would track companies' cybersecurity performance and enable a central rating function that insurance companies would use to price cyber insurance coverage. This program would ultimately launch a cyber equivalent of the National Council on Compensation Insurance, which collects and analyzes data, provides safety recommendations, and publishes MOD rates that serve as the basis in most states for workers' compensation insurance costs.

16. Without more robust and expansive data gathering and assessment of risk and consequences, the cyber insurance industry and the DIB it must serve will not mature as quickly as needed. Congress should create legal protections enabling insurance companies to share anonymized data within the insurance industry and with an independent central organization, such as NIST.

- A similar framework exists between OSHA, the National Council on Compensation Insurance, and insurance companies with respect to rates for health and injury insurance premiums.

- The combination of 1) insurance-impact data, 2) contextualization of that data by Information Sharing and Analysis Centers, and 3) threat-indicator information from organizations such as the Cyber Threat Alliance will ultimately enable organizations to better calculate the return-on-investment of improving specific cybersecurity behaviors and controls. This is similar to the approach taken by the National Transportation and Safety Board (NTSB) and has been proven to be highly valuable in advancing the cause of transportation safety for every mode of transportation in NTSB's jurisdiction.

17. As the CSC report recommended, the executive branch should establish a public-private working group at DHS to "identify common areas of interest for pooling anonymized data from which to derive better, more accurate risk models."[12]

18. As the CSC report recommended, Congress should establish a Bureau of Cyber Statistics (within the Department of Commerce or another agency) charged with collecting and providing statistical data on cybersecurity and the cyber ecosystem to inform policymaking and government programs.

***Key Finding 5*: The USG, insurance industry, and broader policy community should explore existing models and experiments that create cost-neutral (to government) backstops to a range of systemic risks to determine lessons that can be applied to covering systemic cyber risk in the United States.**

Several countries, including the United Kingdom, France, Germany, and Singapore, have created public-private partnerships ensuring that their governments can backstop catastrophic events such as terrorist attacks in a cost-neutral manner in partnership with their respective national insurance industries. In these models, the government receives premiums for the backstop and is reimbursed by the pool over time should the pool's capital reserves be breached.

This model offers significant advantages over the current methods of managing risk in the United State and has the following benefits:

- Reduces current government spending levels
- De-risks the government in backstopping the U.S. economy
- Creates significant reserve capital for a cyber catastrophe
- Replaces the government as the primary payment obligor in a systemic failure event
- Ensures repayment of the government should the fund's reserves be drained
- Pays the government premiums for temporarily backstopping the pool of reserves
- Proliferates the expansion of insurance coverages for supply chain and systemic failures by removing or reducing the catastrophic exposure
- Fully capitalizes response and recovery, significantly improving the resiliency of U.S. national infrastructure

12. Ibid.

Recommendations

19. Congress should create a Systemic Cyber (and other systemic risk) Risk Pool backstopped by the USG. The pool would enable insurance markets to provide systemic risk insurance coverage to American businesses in a highly efficient manner at no cost to the American taxpayer.

20. As the CSC report recommended, Congress should codify a "Cyber State of Distress" declaration that would "trigger the availability of additional resources [for the private sector and state and local governments] through a 'Cyber Resilience Response & Recovery Fund.'" A Cyber State of Distress would be less severe than a state of emergency but would still mandate a response that exceeds federal civilian authorities' everyday support for critical infrastructure and the private sector. This mechanism would ensure sufficient resources and capacity are available to respond to or, more importantly, preempt significant cyber incidents.

CONCLUSION

The private cyber insurance marketplace can address significant, but not all, risk exposures facing the DIB. Ubiquitous adoption of cyber insurance within the DIB, including cyber BI coverage, would strengthen the DIB's resiliency and limit associated behavior-based risks within the DIB. The 20 recommendations contained in this memo are consistent with the recommendations of the Cyberspace Solarium Commission. Taken together, these recommendations would have a meaningful impact on the maturity of the cyber insurance market such that cyber insurance would materially improve defense supply chain security and the resiliency of the defense industrial base.

Appendix: Anonymized Participant List

Private Industry Participants:

- Vice president and chief technology officer of a business risk consulting firm
- Director of a cyber risk consulting firm
- Enterprise risk manager for a federally funded research and development center (FFRDC)
- Supply chain threat subject matter expert for an FFRDC
- Chairman and CEO of an investment management firm
- CEO of an angel investor firm
- Chairman of a cyber insurance startup
- President of a professional services association

Government Officials:

- Representative from the World Bank
- Senior director at the Cyberspace Solarium Commission
- Legislative director for a member of Congress
- Senior director in the Executive Office of the President
- Senior official in the Defense Department's Industrial Policy Office