Discussion of Role of the Insurance Industry in Federal Cybersecurity

Executive Report

Cybersecurity Community of Interest

Date Released: February 26, 2018

Synopsis
The risk of cybersecurity is headline news almost every night. Over the past 24 months, the discussion around cybersecurity has changed from a technical problem to be solved to a major risk that needs to be managed. In the United States, no discussion of major risk management can be held without addressing the role of the insurance industry. Cybersecurity is no different. Insurance is embedded in our daily lives when dealing with risk. From the requirement for businesses to hold insurance to the critical role in national safety to recover from major disasters such as hurricanes, epidemics and even war, insurance is a key element of the solution.

So what is the insurance industry’s role in the cybersecurity fight? Who pays for the recovery of a major cyber attack and how does insurance provide needed support? Should Government contractors be required to hold insurance to assure that critical federal programs can survive an attack? Is there enough coverage that critical infrastructure and major business can recover from a cyber attack?

The ACT-IAC Cybersecurity Community of Interest (COI) took up this issue and held discussions with several agencies, industry leaders and insurance companies. The result of this study is found in the following paper.
This page is intentionally blank.
American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology (ACT) is a non-profit educational organization established to create a more effective and innovative government. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over thirty years of experience, to produce outcomes that are consensus-based. The findings and recommendations contained in this report are based on consensus and do not represent the views of any particular individual or organization.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC does not accept government funding.

ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of IT. For additional information, visit the ACT-IAC website at www.actiac.org.

Cybersecurity Community of Interest

The ACT-IAC Cybersecurity Community of Interest mission is to facilitate collaborative development and implementation of solutions and best practices related to cybersecurity challenges. The COI provides opportunities for industry and federal government to identify, raise awareness, and provide solutions to cybersecurity challenges critical to protecting our national interests.

Disclaimer

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which a number of individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable
information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

©American Council for Technology, 2018. This document may not be quoted, reproduced, and/or distributed unless credit is given to the American Council for Technology-Industry Advisory Council.

Further Information

For further information, contact the American Council for Technology-Industry Advisory Council at (703) 208-4800 or www.actiac.org.
Contents

Cybersecurity and Risk Management ....................................................................................................... 1

From Confidentiality to Availability, the New and Urgent Role of Insurance ................................. 1

Insurance and the Federal Government ....................................................................................... 2

Summary ................................................................................................................................................... 3

Contributing Authors ................................................................................................................................ 3

Reference .................................................................................................................................................. 3
Cybersecurity and Risk Management

Over the past year, the cyber discussion has turned dramatically from a focus on a technical solution to that of risk management. As the part of this conversation, almost every study on improving cybersecurity calls for a risk-based approach to acquisition, decision making, and operational action. This includes the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which calls for a major shift to a risk-based cyber approach across all federal agencies. The insurance industry is in the business of managing and responding to risk and their role is repeatedly raised in relation to the cybersecurity challenge. In the final report by the Commission on Enhancing National Cybersecurity, established by President Obama, the following recommendation was made, which included the role of insurance in the cyber community:

Action Item 1.4.1: NIST, in coordination with the NCP 3, should establish a Cybersecurity Framework Metrics Working Group (CFMWG) to develop industry-led, consensus-based metrics that may be used by (1) industry to voluntarily assess relative corporate risk, (2) the Department of Treasury and insurers to understand insurance coverage needs and standardize premiums, and ...

Estimates of money spent on insurance premiums for 2016 exceed $2.5B with an estimated growth to $7.5B over the next five years. The growth in the insurance market has had significant impact on acquisition processes, new technologies, management approaches, and legal interpretations related to cyber risk management. But as cyberattacks continue to increase in both number and complexity, the cyber insurance industry is being forced to change how it responds. Many corporations now require vendors to have cyber insurance to assure cyber risks are being appropriately addressed throughout the supply chain.

From Confidentiality to Availability, the New and Urgent Role of Insurance

Within the cyber security community, the impact of a cyberattack is often characterized by one of three categories: Confidentiality, Integrity, and Availability. Confidentiality refers to the loss of information that should be kept private, such as a breach that steals Personally Identifiable Information (PII) or Personal Healthcare Information (PHI). Integrity refers to a cyberattack that changes data and/or affects systems by degrading the trust of the data. Finally, Availability cyberattacks influence the operation and overall use of computer-related systems.

During 2017, a major shift has been seen in the type and impact of cyberattacks from major Confidentiality breaches to serious Availability attacks. This shift has become a critical piece in the discussion of the insurance role in Federal Government. Previous cyber insurance discussions focused on Confidentiality breaches, such as the attack on the Office of Personnel Management (OPM). The
cost of responding to these breaches is usually spread out over months, or even years, after the event. As a result of such attacks, a debate has ensued on whether federal contractors should be required to hold insurance based on the need to pay for the recovery and response to a major data loss breach through services, such as notifying affected users, paying for credit monitoring or legal costs, and ensuring systems recovery. While this debate continues, it is universally acknowledged that the ultimate responsibility for protecting federal information lies with the Federal Government. Recent Availability attacks, however, dramatically changes the discussion when it comes to insurance and the Federal Government.

Availability attacks incur significant costs almost immediately. The WannaCry and Petya/NotPetya cyberattacks completely brought down major infrastructure and systems around the world. These included the United Kingdom National Health Service, the automotive manufacturer Honda, and major portions of FedEx, which recently reported that the attack on their TNT subsidiary will have a major impact on their revenue and operation, and affect their overall financial performance. Even in the United States where there was minimal impact to systems, hospitals around the country had to mobilize teams to evaluate and protect against the attacks. Major costs were immediately incurred to recover the impacted systems and protect against vulnerable ones. Financial support was needed without delay—not spread over months as would be the case in a Confidentiality breach.

Insurance and the Federal Government

As a result of these high-impact Availability attacks, the discussion of cyber insurance and how the Federal Government should be involved has changed dramatically in the past year. Major infrastructure systems from hospitals to financial to power systems must have the means address potential major Availability attacks. This includes not just commercial, but federal systems, which are operated by contractors in many cases. This shift in discussion has resulted in the need for several near-term actions, including:

- Establishment of a dialogue between government and industry on insurance requirements;
- Discussions with the insurance industry over coverage and support of major infrastructure systems;
- Determination of responsibility for addressing the overall insurance issue; and
- Reporting and response for insurance-related topics to OMB, White House, and Congress.
Summary
Over the past few years, the discussion around the cyber insurance role and the Federal Government has been evolving, but with the recent Availability attacks, there is now a growing urgency to take immediate action. The first step would be to identify which agency should assume the responsibility to address this challenge. Once identified, a dialogue with other federal agencies, contractors, infrastructure providers, and the insurance industry needs to be established to address questions, such as “how much insurance should be required by government contractors?” and “does the cyber insurance industry provide for the proper response to a federally related attack?” It is recommended that a joint government, contractor, and insurance provider discussion be established to address the items listed above and that this dialogue be established in the near future as the rise in major Availability cyber-attacks are projected to continue to rise.

Contributing Authors
This paper was written by a consortium of government and industry. The organizational affiliations of these contributors are included for information purposes only. The views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development.

Chip Block Evolver
Alan Young AT&T
Ann Marie Keim National Aeronautics and Space Administration
Matt Sexton Booz Allen Hamilton
Kenneth Adams KPMG

Project Sponsor
Donald Johnson Department of Defense, Office of the Secretary of Defense

Reference
1 COMMISSION ON ENHANCING NATIONAL CYBERSECURITY, December 1, 2016