Cyber Risk Metrics Survey, Assessment, and Implementation Plan

May 11, 2018

HSSEDI
Homeland Security Systems Engineering & Development Institute

Acknowledgement for DHS Sponsored Tasks

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. MITRE Corp. operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) as an FFRDC for DHS under contract HSHQDC-14-D-00006.

The HSSEDI FFRDC provides the government with the necessary systems engineering and development expertise to conduct complex acquisition planning and development; concept exploration, experimentation and evaluation; information technology, communications and cyber security processes, standards, methodologies and protocols; systems architecture and integration; quality and performance review, best practices and performance measures and metrics; and, independent test and evaluation activities. The HSSEDI FFRDC also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSEDI FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under:

HSHQDC-16-J-00184
This HSSEDI task order is to enable the DHS Science and Technology Directorate (S&T) to facilitate improvement of cybersecurity within the Financial Services Sector (FSS). To support NGCI Apex use cases and provide a common frame of reference for community interaction to supplement institution-specific threat models, HSSEDI developed an integrated suite of threat models identifying attacker methods from the level of a single FSS institution up to FSS systems-of-systems, and a corresponding cyber wargaming framework linking technical and business views. HSSEDI assessed risk metrics and risk assessment frameworks, provided recommendations toward development of scalable cybersecurity risk metrics to meet the needs of the NGCI Apex program, and developed representations depicting the interdependencies and data flows within the FSS.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

Approved for Public Release; Distribution Unlimited.
Case Number 18-1468 / DHS reference number 16-J-00184-02

HSSEDI
Homeland Security Systems Engineering & Development Institute

Abstract and Key Words

The Homeland Security Systems Engineering and Development Institute (HSSEDI) assists the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) in the execution of the Next Generation Cyber Infrastructure (NGCI) Apex program. This brief summarizes a series of HSSEDI reports analyzing cybersecurity risk metrics for the NGCI Apex program.

The series of reports identifies existing metrics and surveys relating to cybersecurity, as well as provides an Implementation Plan for a Confidence Survey specific to the NGCI Apex program. The series concludes with three recommendations: 1) the NGCI Apex program should develop a scalable framework for cybersecurity risk metrics, drawing on concepts from two prominent modeling approaches; 2) the NGCI Apex program should implement a Confidence Survey to continuously gather feedback regarding cybersecurity issues affecting the set of national, critical infrastructures; and 3) the Confidence Survey should serve as an initial step on the trajectory to scalable, cybersecurity risk metrics which meet the needs of the NGCI Apex program.

- **Keywords**
  - Next Generation Cyber Infrastructure (NGCI) Apex program
  - Critical Infrastructures
  - Cybersecurity Risk Metrics
  - Cyber Threat Models
  - Confidence Surveys

Key Takeaways

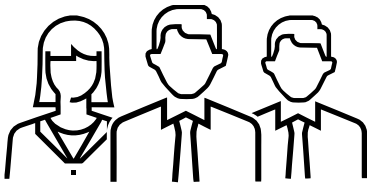
Challenge

The NGCI Apex Program currently lacks metrics to assess its impact on cybersecurity risk within the financial services sector (FSS).

HSSEDI's Recommendations to meet the Challenge:

- The NGCI Apex Program should collaborate with the FSS to develop a scalable framework for cybersecurity risk metrics.
- The NGCI Apex Program should implement a Confidence Survey to continuously gather feedback from the Cyber Apex Review Team (CART) regarding cybersecurity issues.
- The Confidence Survey should serve as an initial step in the development of a cybersecurity risk metrics framework meeting the NGCI Apex Program's needs.

Executive Interviews



Interviews with executives from **11** financial institutions, market utilities, and industry organizations. Executives were responsible for cybersecurity threat modeling, risk assessment, and mitigation.

Observations Relevant to Cybersecurity Metrics

- Each organization had a program of risk metrics and measures; developed largely for the specific organization
- Organizations tended to utilize hybrid risk management frameworks specific to the organization
- Risk modeling generally incorporated subjective assessments of threats and vulnerabilities. Some efforts at quantification around consequence
- General recognition of dependence on qualitative approaches and the need to share data to: (a) inform development of more quantitative metrics and (b) mature risk management capabilities

HSSEDI did not find a metrics framework that could be implemented in the immediate term to meet all NGCI Apex Program's needs.

Key Recommendation

The NGCI Apex Program, working with the FSS, should pursue the development of a quantitative, cybersecurity risk metrics framework.

Should cybersecurity risk metrics be quantitative?

Pros	Cons	Mitigations
▪ Transparency ▪ Repeatability ▪ Reproducibility ▪ Scalability	▪ Reliance on input data ▪ Confusion with precision	▪ Transparency in the transformation from input data to output data ▪ Metrics assessing range of risk

Two prominent quantitative, cybersecurity risk modeling approaches to aid in development of framework:

- Factor Analysis of Information Risk (FAIR)
- Hubbard and Seiersen (H&S) approach

HSSEDI
Homeland Security Systems Engineering & Development Institute

Support for Quantifying Cyber Risk

"The first step in developing 'a consistent, repeatable methodology to support the ongoing measurement of cyber risk' is articulating and agreeing to the objectives and the purpose of quantitative methods. ***The need to develop tools to quantify cyber risk and to assist risk management is well-recognized, as is the current lack of commonly accepted measurement practices. . . .*** *As there is no common method to quantify cyber risk across firms or sectors, significant time is needed to develop a consensus on a risk measurement standard that would enable financial services to measure and mitigate their individual risk."*

- The Financial Services Sector Coordinating Council (FSSCC)
commenting on the Enhanced Cyber Risk Management Standards ANPR

Similar to the FSSCC, HSSEDI believes that significant time would be required to develop a framework for the FSS and the first step should be establishing a dialogue with relevant stakeholders.

HSSEDI
Homeland Security Systems Engineering & Development Institute

Wide Range of Opinions on Quantifying Cyber Risk

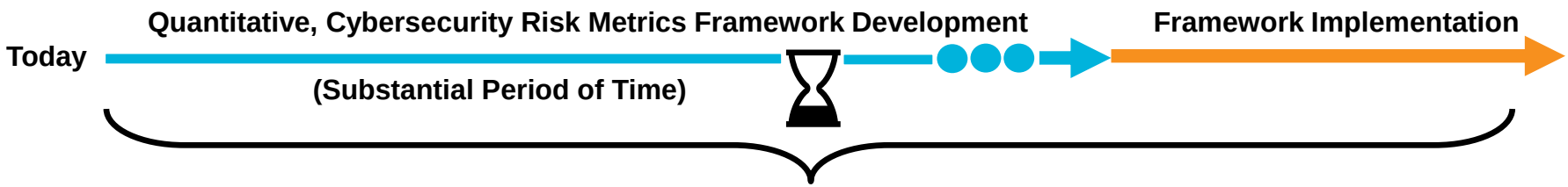
"No quantitative framework for measuring risk is available. There are too many variables to create an acceptably accurate measurement of residual risk. All acceptable models are qualitative."

– Bank of Montreal (BMO) and Canadian Imperial Bank of Commerce (CIBC) commenting on the Enhanced Cyber Risk Management Standards ANPR

"In TIAA's experience, risk analysis using FAIR has been an invaluable contribution to our management of IT risk. While TIAA intends to continue to utilize FAIR, we recommend against mandating it or codifying any other specific methodology, *in line with our belief in a flexible, risk-based system of layered security that is able to adjust as needs arise. And as emphasized above, the adequacy of this testing can be assessed through supervisory examination."*

– Teachers Insurance and Annuity Association of America (TIAA) commenting on the Enhanced Cyber Risk Management Standards ANPR

Addressing NGCI Apex Program's Needs



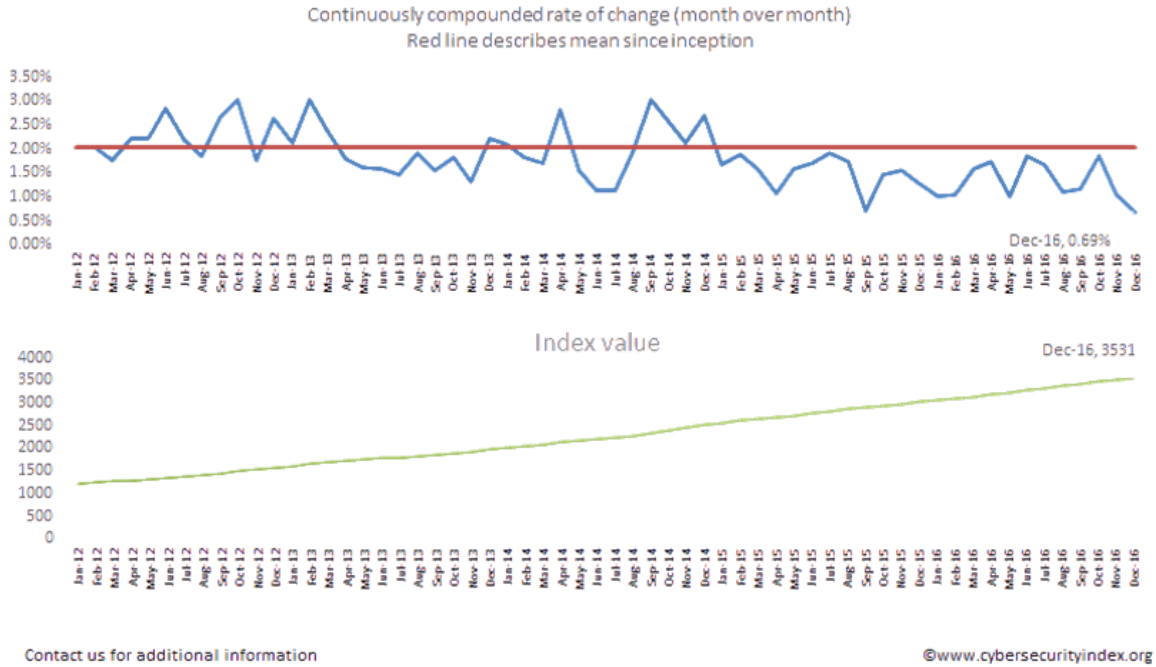
The NGCI Apex Program needs a mechanism to:

- improve the program's understanding of the cybersecurity risk present within the CART
- measure the success of its past investments
- measure the CART's desire for future technology investment
- aid in developing an FSS quantitative, cybersecurity risk metrics framework
- aid in implementing the framework by quantifying loss event frequency and loss magnitude risk components

HSSEDI recommends a Confidence Survey regularly administered to CART members.

Index of Cyber Security (ICS)

ICS is "A measure of perceived risk" where "A higher index value indicates a perception of increasing risk [and] a lower index value indicates the opposite"
[Geer & Pareek].

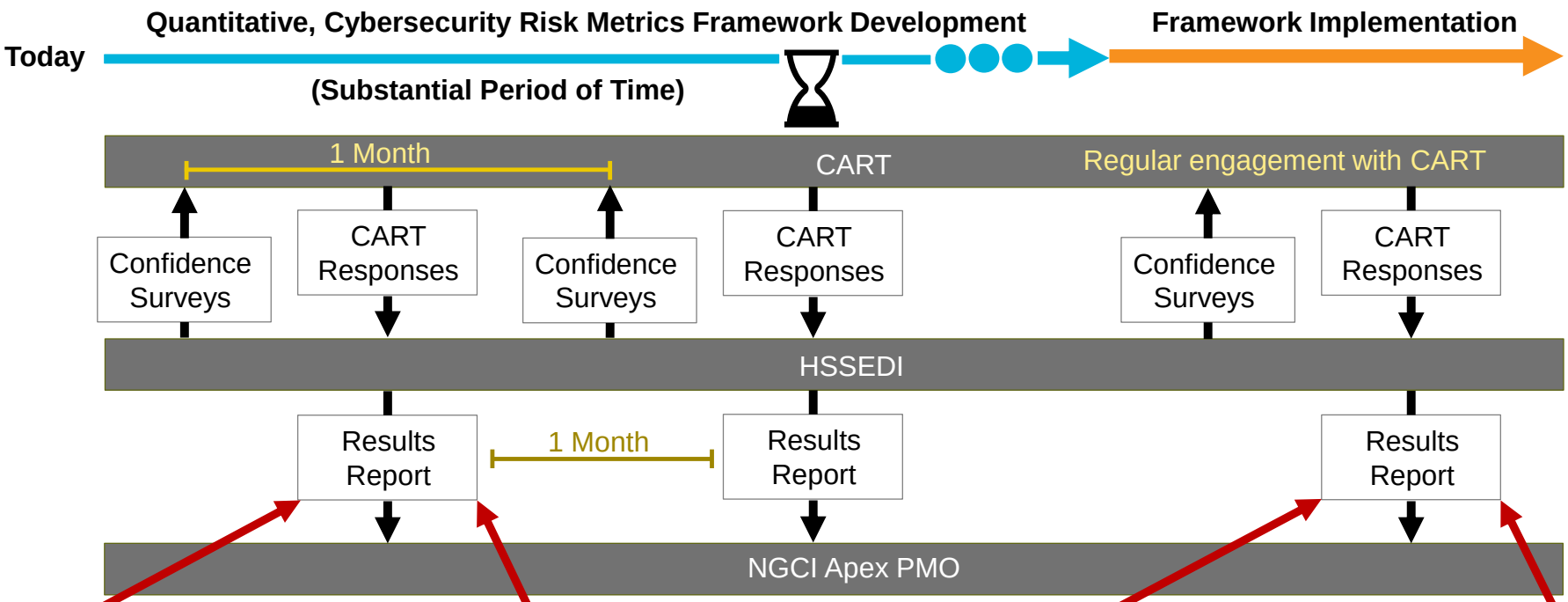


ICS:

- is co-published by Dan Geer and Mukul Pareek
- is computed using data from a monthly survey administered to working cybersecurity experts across multiple industries
- has been updated and released each month since April 2011
- can be broken into sub-indices

HSSEDI
Homeland Security Systems Engineering & Development Institute

Proposed Next Steps



Development Specific Contents

- Results for questions tailored to further framework development

Persistent Contents

- ICS value and sub-indices derived from CART responses
- Metrics quantifying impact of past investments & CART desire for future investment

Implementation Specific Contents

- Loss magnitude and loss frequency of cybersecurity events for use in framework implementation

HSSEDI
Homeland Security Systems Engineering & Development Institute

References

- FAIR Institute. Retrieved from http://www.fairinstitute.org/
- Josey, A., et al. (2014, Jun.). An Introduction to the Open FAIR Body of Knowledge. The Open Group., CA. (Online).
- RiskLens. (Online). Available: http://www.risklens.com/
- Hubbard, D.W., and Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk. John Wiley & Sons.
- Geer, D., & Pareek, M. Index of Cyber Security. Retrieved from http://www.cybersecurityindex.org/index.php
- Geer, D., & Pareek, M. (2016, October). The Index of Cyber Security-Detailed Report, October 2016.
- FRB, OCC, & FDIC. (2016, October). Enhanced Cyber Risk Management Standards (FRB Docket No. R-1550; RIN 7100-AE 61; Docket ID OCC-2016-0016; FDIC RIN 3064-AE45).
- BMO & CIBC. (2017, January). Enhanced Cyber Risk Management Standards: Joint Response from Bank of Montreal (BMO) and Canadian Imperial Bank of Commerce (CIBC). Retrieved from https://www.federalreserve.gov/secrs/2017/february/20170208/r-1550/r-1550_011717_131690_286671592059_1.pdf
- TIAA. (2017, February). Re: Advance Notice of Proposed Rulemaking for Enhanced Cyber Risk Management Standards (Federal Reserve Docket No. R-1550, RIN 7100-AE-61; OCC Docket ID OCC-2016-0016; FDIC RIN 3064-AE45). Retrieved from https://www.regulations.gov/document?D=OCC-2016-0016-0038
- FSSCC. (2017, February). Re: Enhanced Cyber Risk Management Standards (FRB Docket No. R-1550; RIN 7100-AE 61; Docket ID OCC-2016-0016; FDIC RIN 3064-AE45). Retrieved from https://www.regulations.gov/document?D=OCC-2016-0016-0033

Contact for More Information

DHS Science and Technology Directorate

Next Generation Cyber Infrastructure (NGCI) Apex Program

Homeland Security

Science and Technology

Dr. Douglas Maughan (Douglas.Maughan@hq.dhs.gov)
Cyber Security Division (CSD) Director

Greg Wigton (Gregory.Wigton@hq.dhs.gov)
Apex Program Manager