Final Report: Leveraging The Cyber Risk Portal As A Teaching & Education Tool

Supply Chain Management Center
R.H. Smith School Of Business,
University Of Maryland College Park

Submitted By:
Dr. Sandor Boyson
Ms. Holly Mann
June 10, 2015

The main objective of this project was to complete the tasks of enhancing usability of the Cyber Risk Portal, which is a set of enterprise IT Supply Chain Risk Management Tools built in a partnership between the University Of Maryland's Supply Chain Management Center and the Information Technology Lab of the National Institute Of Standards & Technology.

Enhanced usability objectives for this project were addressed through the following project accomplishments:

- Worked extensively with an industrial designer to re-imagine the user-interface of the portal and construct a new visual architecture. Had several team sessions to put together the roadmap to achieving the portal re-design. Developed messaging strategy and value proposition definition. Revised portal user interface. Designed CyberChain identity mark, sourced and selected all images for portal.

- Implemented a streamlined, user-friendly portal design and navigation. Our programmers changed the visual layout and screen prompts to be more flowing and simplified. This task involved extensive revision of Drupal operating platform configuration settings and style sheets (Appendix 1)

- Worked with instructional design team to prepare the strategy for collecting, processing and positioning new multi-media content on the portal. Developed scripts for video interviews and tutorials, enhanced background images and graphic titles

- Completed portal home page -level expert videos with NIST and University/Industry experts (Jon Boyens, NIST, Hart Rossman, Sandor Boyson, and Holly Mann, Smith School Of Business/SCMC, and Chris Keagan, Beecher Carlson).

- Each video involved preparatory scripting of interviews, creation of CyberChain video identification (intro/outro); onsite recording of subjects at the school's production facilities and editing lengthy interviews into three to six minute polished segments.

- These videos are intended to orient organizations to the foundational knowledge of the NIST Cybersecurity Framework, and help them gain an understanding (to the category/sub-category level) of NIST control families, and related IT supply chain risk management best practices. In addition, we added insurance industry best practices content with the help of our insurance industry subject matter expert. (Appendix 2)

- Developed specific portal sub-page tutorials to accompany each of the portal assessment applications (Strategic Readiness, NIST Control

Families, Network Threat Mapping, Cyber Risk/Insurability Benchmarking), and the Executive Results Dashboard. (Appendixes 3-7)

- These five tutorial subjects are now active online learning modules that are composed of various multi-media components such as video, power point, and narrative voiceover screen captures explaining navigational drill downs.

Another sub-objective of this project was to explore and conduct market testing/opportunity research. We completed the following tasks:

- We initiated a series of activities aimed at better defining user requirements in two critical market segments for the Cyber Risk Portal: the Federal Procurement Community and the Insurance Industry.

- We conducted meetings at our school with a focus group of GSA, DOD, DHS and NIST representatives to demo the portal and solicit feedback. We also conducted an intensive one on one design session with three GSA representatives to more fully scope out their portal user requirements.

- We presented the portal at two major insurance industry conferences in Washington DC and New York.

- We completed preliminary discussions with GSA and submitted a proposal to the agency to sponsor trials of the cyber risk portal with GSA's IT Vendor Community.

- We completed preliminary discussions with both an Insurance Industry Broker (Beecher Carlson) and a Major Insurer (Zurich) to

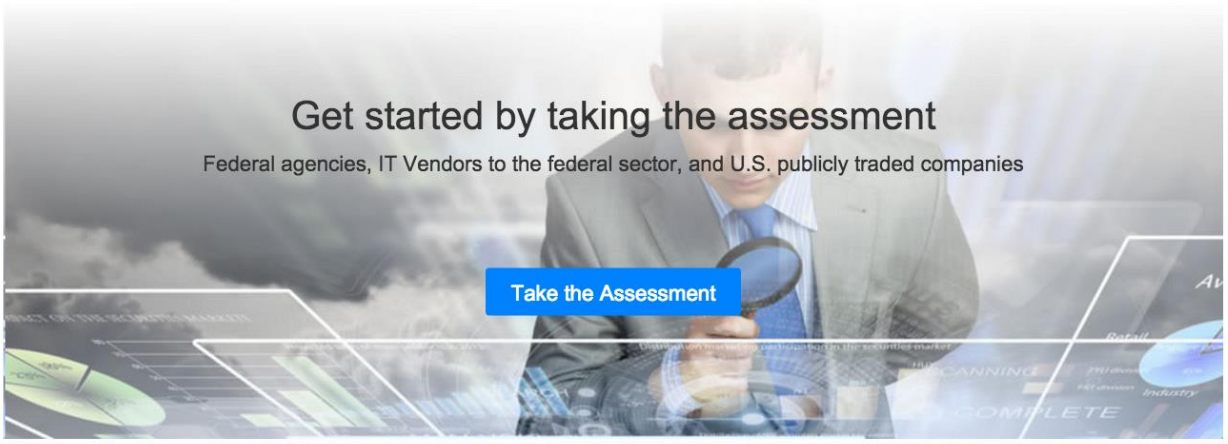
participate in sponsoring trials of the cyber risk portal with current or prospective underwriting clients.

- Finally, we briefed our NIST ITL project sponsors on the results of this project on June 8, 2015 at NIST and discussed options for further research.

Username Password LOG IN Home Register Alerts & News

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

About CyberChain



Learn about cyber supply chain risk

Learn about cyber supply chain risk

Understanding the portal research foundations

Understanding the NIST framework

Understanding risk insurance analysis

Understanding network mapping

Understanding the portal and privacy assurances

The tools you need!

Enterprise Assessments

Description text here which will likely run onto two line and link

Network Mapping

Description text here which will likely run onto two line and link

Insurance Analysis

Description text here which will likely run onto two line and link

Alerts

CVE-2015-3610 (homecontrol_for_room_automation)
The Siemens HomeControl for Room Automation application before 2.0.1 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle... Read more

News

Oracle Releases April 2015 Security Advisory
Original release date: April 15, 2015 | Last revised: April 16, 2015
Oracle has released security fixes to address 98 vulnerabilities as part of its... Read more

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Instructions For Completing The Enterprise Assessments

+ New assessment

Thank you for participating in our enterprise assessment survey. This survey is designed to evaluate your organizational activities and degree of capability in the area of cyber supply chain risk management. The assessment consists of three parts:

Part One: Respondent Profile which collects basic information about your company and provides the basis for our benchmarked results.
Part Two: Strategic Readiness Survey which assesses the structural readiness of your organization to meet the challenges of the cyber supply chain.
Part Three: Enterprise Assessments which distills cyber supply chain best practices developed by the U.S. National Institute Of Standards & Technology into a series of specific questions about your operating practices.

Please note: Each tab will become visible upon the completion each section, in the order they are presented to you. Once you have completed these parts, you will have access to the results listed under the Executive Dashboard. IMPORTANT: the Executive Dashboard tab will not be visible until you have completed **ALL** Enterprise Assessments

View Tutorial: How to complete Assessments

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Enterprise Assessments

Instructions | Part 1 | Part 2 | Part 3 | Risk Insurance Analysis | Executive Dashboard

+ New assessment

Control Family 1: Uniquely identify supply chain elements, processes, and actors	✔	edit assessment
Control Family 2: Limit access and exposure within the supply chain	✔	edit assessment
Control Family 3: Create and maintain the provenance of elements, processes, tools, and data	✔	edit assessment
Control Family 4: Share information within strict limits	✔	edit assessment
Control Family 5: Perform supply chain risk management awareness training	✔	edit assessment
Control Family 6: Use defensive design for systems, elements, and processes	✔	edit assessment
Control Family 7: Continuous integrator review	✔	edit assessment
Control Family 8: Strengthen delivery mechanism	✔	edit assessment
Control Family 9: Assure sustainment activities and processes	✔	edit assessment
Control Family 10: Manage disposal and final disposition activities throughout the system or element life cycle	✔	edit assessment

Instructions for Part Three: Enterprise Assessments. These assessments are designed to distill cyber supply chain best practices developed by the U.S. National Institute Of Standards & Technology into a series of specific questions about your operating practices. Once you have completed all assessments, you will be able to view your results under the Executive Dashboard tab in the IT Supply Chain Risk Management Index.

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Risk Insurance Analysis

Instructions | Part 1 | Part 2 | Part 3 | Risk Insurance Analysis | Executive Dashboard

Risk Insurance	✔	edit assessment

Congratulation! You have completed the Assessments. As a U.S. publically traded company, you may also participate in the Insurance Risk Analysis.
View Tutorial: How to complete Risk Insurance Analysis

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Enterprise Assessments | Network Mapping | Insurance Analysis | About CyberChain

- Getting Started
- HQ
  - Intergalactic HQ
- Key Hubs & Nodes
  - Important Partner Software Development Center
  - Add Node
- Transactions
  - Add Transaction
- Key Actors

No actors have been added yet.

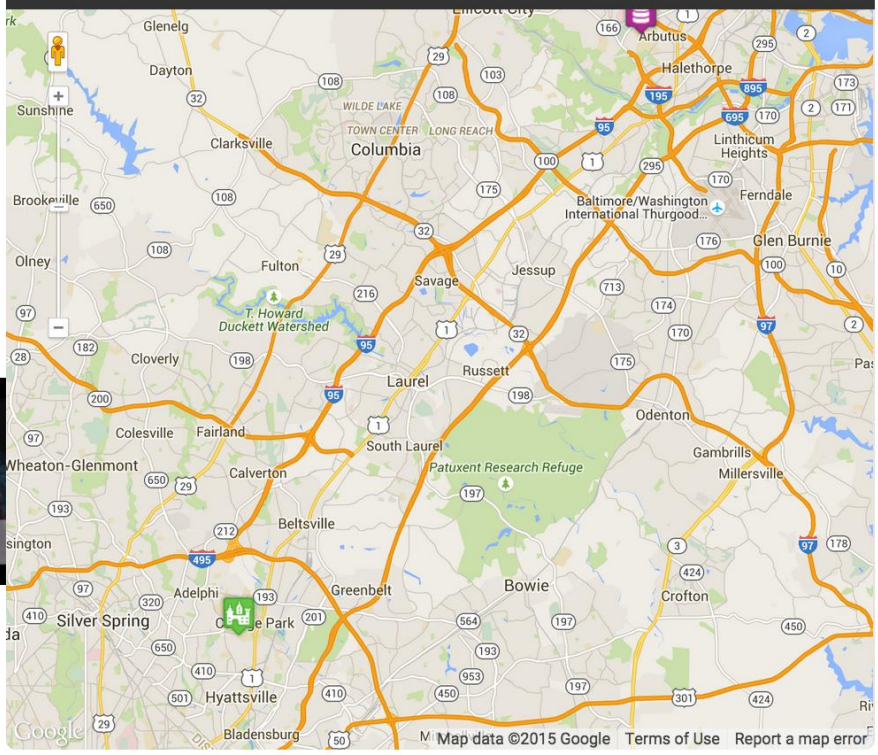
Add Actor

- Video Tutorial

Total # of Transactions: 0
Total Possible Risk: 0
Actual Risk Score: 0

Total # of Nodes: 2
Total Possible Risk: 20
Actual Risk Score: 2.8

Supply Chain Risk Score: 0
What does this score mean?



CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Executive Dashboard

Instructions | Part 1 | Part 2 | Part 3 | Risk Insurance Analysis | Executive Dashboard

+ New assessment

Below are active links to each section of your assessment results. After you have completed your review of each section, click on the **"Back to Dashboard"** link to go back to the Dashboard menu. Please take a few minutes to provide us your **Feedback**.

Executive IT Risk Intelligence Index
This is based on the President's Cyber Security Framework Order (October 2012); and incorporating subsequent NIST research and feedback from multiple stakeholders. This Index determines your organizational ability to identify, protect, detect, respond, and recover from cyber attacks.

IT Supply Chain Risk Management Index
This is a capability maturity model developed by University of Maryland based on extensive research of over 50 supply chain initiatives, and surveys of hundreds of individual firms, to determine your organizational ability to manage risks throughout the entire IT supply chain from both defense in-depth and defense breadth perspectives.

IT Network Vulnerability Mapping Index
This model uses critical hub and key process analyses (Nessus, CVSS) to determine the highest risk transactions in your IT supply chain.

Insurance Risk Analysis (for U.S. publically traded companies only)
Willis Insurance company has mined corporate cyber risk events, impacts, and disclosures reported to the Security and Exchange Commission; see how your organization compares to peers in your industry in terms of reporting and transparency.