AAPA Cybersecurity Conference

Cybersecurity Solutions For Port Managers

Chuck Floyd, CEO
Security Solutions Technology

Security Solutions Technology, LLC

- Headquarters – Potomac, MD
- Veteran-Owned & SDVOSB
- Company formed in 2004 by senior government & industry executive
  - Focus on cybersecurity & critical infrastructure services
  - More than 3 decades of federal government & commercial (Fortune 500) experience
  - History of transformational leadership
  - Port assessments for DHS grants
  - Cybersecurity Subject Matter Experts (SMEs on staff)

Port Cybersecurity

- U.S. ports handle $1.5+ trillion in cargo annually
- GAO — No cybersecurity standards for U.S. ports
- President's proposed 2016 budget — $14B cyber- security budget
- U.S. Congress provided $786M for cybersecurity operations
- DHS — Port Security Grant Program
- DHS — Cybersecurity Education & Training Assistance Program

- Agencies involved
  - National Protection & Programs Directorate (DHS)
  - Cyber Threat Intelligence Integration Center
  - National Security Agency
  - National Institute of Standards & Technology (Executive Order 13636)
  - Office of Cyber & Infrastructure Analysis
  - Office of Cybersecurity & Communications
  - U.S. Coast Guard
  - GSA (IT Schedule 70)

Cybersecurity Attack Findings

- 97% of organizations had been breached, meaning at least one attacker had bypassed all layers of their defense-in-depth architecture.
- 1/4 of all organizations experienced events used by advanced persistent threat (APT) actors.
- 3/4 of organizations had active command-and-control communications (attackers had control of their system)
- After an organization breach, attackers attempted to compromise the organization more than once per week (malware vs advisory)
- NIST Cybersecurity Framework Recommendations
  - Authentication
  - Automated Indicator Sharing
  - Conformity Assessment
  - Cybersecurity Workforce
  - Data Analytics
  - FISMA Compliant Solutions

Port Issues from Cyber Attacks

- Affects electronic payments (customers and employees)
- Affects computer systems (stealing of information)
- Affects use of cranes
- Affects use of electronic gates
- Affects the electronic manifest
- Affects communications with ships
- Affects the logistical chain (through-put)
- Affects port productivity
- Affects the reputation of the port

Port Security Objectives

- DHS requires a Port Authority to complete an assessment of its cyber security readiness prior to a Grant.
- Endpoint Management & Protection Solution (Detect, Prevent, Attribute, Record, Monitor)
- Insider & Outsider threats
- The objective of this assessment include:
  - Alignment of the Port Authority security approach to NIST Framework
  - Assessment of the existing information technology capabilities
  - Assessment and review of all cybersecurity and information assurance policies and procedures
  - Assessment of the existing cybersecurity training and future requirements
  - Conduct targeted audits of the Port Authority Security and Privacy Environment
  - Identification of gaps in the existing people, process, and technology capabilities
  - Development of a Roadmap to address the identified gaps
  - Developing a prioritized list of projects to address the gaps
  - Developing the execution plan for addressing the gaps

Cyber High-Level Plan

Discovery & Assessment

Gap Analysis

Project Identification & Planning

Project Execution

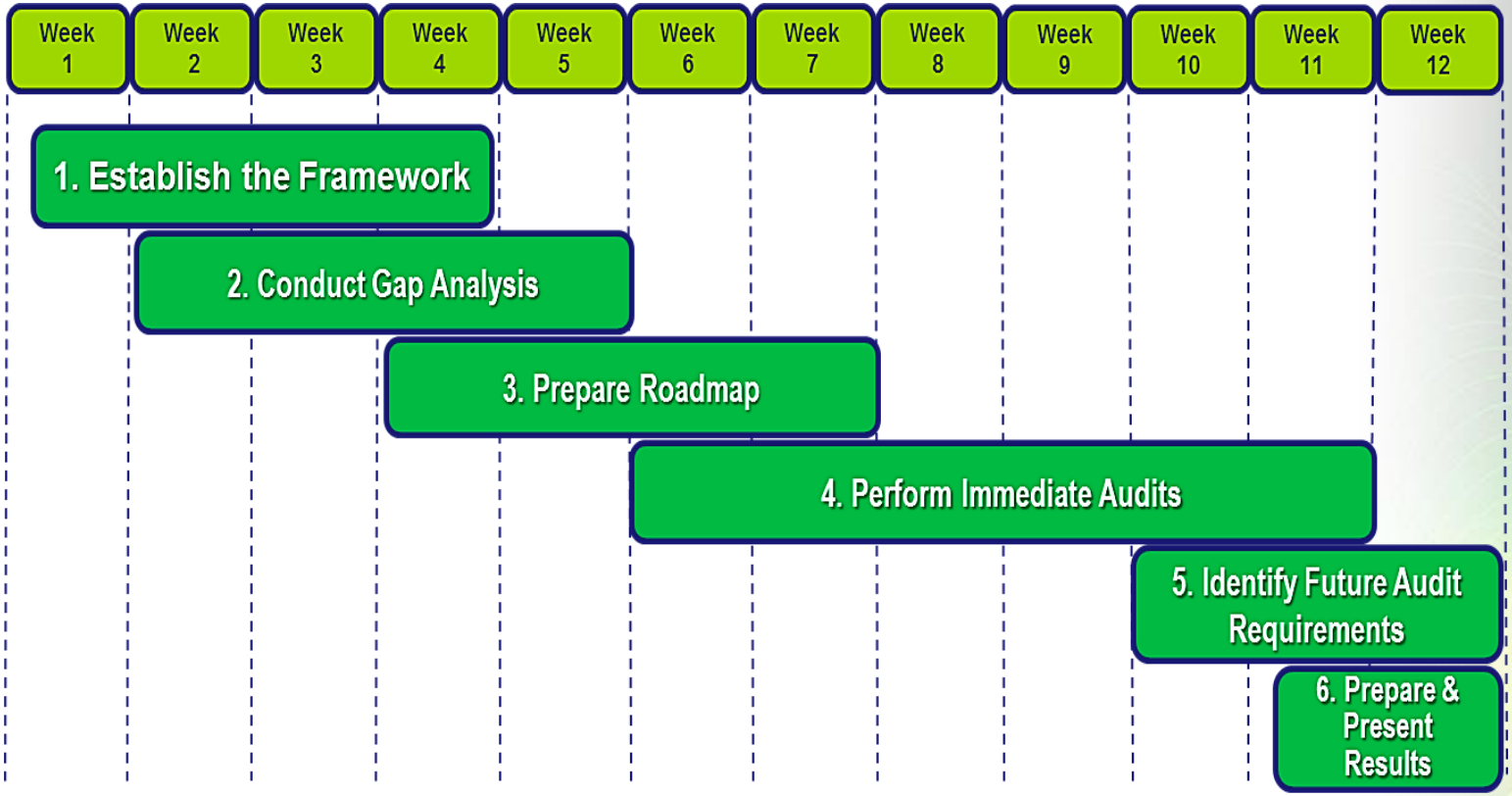
End-To-End Support

Project Approach

Establish the Framework	Conduct Gap Analysis	Prepare Roadmap	Perform Immediate Audits	Identify Future Audit Requirements
➢ Map all current security projects, policies, & training against the NIST Cyber Security Framework	➢ Identify gaps in the security projects, policies, & training vs. the NIST Cyber Security Framework ➢ Prioritize the gaps per the threat landscape	➢ Lay out a plan for new required security projects, policies, & training to close the gaps in the Port Authority compliance to the NIST Cyber Security Framework	➢ Identify & conduct immediate term audits to verify projects / controls already deployed	➢ Lay out a plan for subsequent future audits for other already-deployed controls & for still-to-be deployed controls

Proposed Project Schedule

The project timeframe is based on the elapsed time required to complete the project. The availability of Port Authority resources or delays in the RFP response period, response evaluation, etc. may extend this timeframe.



Task 1: Establish the Framework

Task 1 Summary

Objective:

- Establish a Cyber Security Framework & prepare a baseline for the Port Authority using existing studies & sources of relevant information.

Activities performed by SST:

- Map all current security projects, policies, & training as identified in existing studies against the NIST Cyber Security Framework
- Information sources will include Port Authority existing plans current & pending projects & capability investments, any & all other relevant documentations

Client responsibilities:

- Provide Port Authority Primary Point of Contact
- Provide & coordinate timely access to all information sources (reports, committees, personnel) as required
- Provide timely response to data inquiries
- Provide on-site work facilities as necessary

Deliverable(s)* and Time Frame

Deliverable(s):

- Interim Port Authority To-Be Security Architecture report: spreadsheet document cross reference of existing & planned security-related projects & capabilities with NIST Cyber Security Framework
- The Interim To-Be Port Authority Security Architecture will be defined as consisting of in-place security controls or currently planned security projects & capabilities (people, process, technology)
- The Interim To-Be Security Architecture will form the baseline for the remainder of the assessment & audit activities defined in this project

Time frame:

- Duration: 2 – 4 weeks
- Weeks 1 - 4

Assumptions:

- Mapping will be high-level cross reference of identified project needs vs. interpreted NIST Cyber Security Framework
- Mapping will not include specific application, system, or platform configuration items or detailed policy & procedures requirements

Task 2: Conduct Gap Analysis

Task 2 Summary

Objective:

- Identify gaps in existing Interim Port Authority To-Be Security Architecture as related to the NIST Cyber Security Framework
- Prioritize identified gaps per known cyber-threat landscape specific to Ports

Activities performed by SST:

- Identify gaps in the currently defined and planned Port Authority Security Architecture vs. NIST Cyber Security Framework requirements
- Gaps will be defined as areas where existing or planned projects or capabilities sufficient to address NIST Cyber Security Framework do not exist
- Conduct prioritization mapping of identified gaps to known threats

Client responsibilities:

- Provide and coordinate timely access to all information sources (reports, committees, personnel) as necessary
- Provide timely response to data inquiries
- Provide on-site work facilities as necessary

Deliverable(s)* and Time Frame

Deliverable(s):

- Update of Interim Port Authority To-Be Security Architecture report
- Update will identify security-related project and capabilities remaining to be deployed in order to come into risk-managed compliance with NIST Cyber Security Framework
- Update will also identify level of risk associated with each identified gap, with prioritization of high (highest priority), moderate, and low (lowest priority)

Time frame:

- Duration: 2 – 4 weeks
- Weeks 2 - 5

Assumptions:

- Port Authority Security Architecture is defined as the interim to-be architecture consisting of in-place security controls or currently planned security projects and capabilities (people, process, technology)

Task 3: Prepare Roadmap

Task 3 Summary

Objective:

- Complete the comprehensive roadmap for implementing the Port Authority Security Architecture

Activities performed by SST:

- Define security-related project and capabilities remaining to be deployed in order to come into risk-managed compliance with NIST Cyber Security Framework; fill gaps identified previously
- Integrate Interim Port Authority To-Be Security Architecture with gap closure projects resulting in comprehensive roadmap for final Port Authority Security Architecture

Client responsibilities:

- Provide and coordinate timely access to all information sources (reports, committees, personnel) as necessary
- Provide timely response to data inquiries
- Provide on-site work facilities as necessary

Deliverable(s)* and Time Frame

Deliverable(s):

- Update of Interim Port Authority To-Be Security Architecture report to Final Port Authority To-Be Security Architecture report
- Update will define security-related project and capabilities remaining to be deployed in order to come into risk-managed compliance with NIST Cyber Security Framework

Time frame:

- Duration: 2 – 4 weeks
- Weeks 4 - 7

Assumptions:

- Port Authority Security Architecture is defined as the interim to-be architecture consisting of in-place security controls or currently planned security projects and capabilities (people, process, technology)

Task 4: Prepare Immediate Audits

Task 4 Summary

Objective:

- Identify and conduct technical process and/or related technology validation audits for 2 – 3 in-place systems and controls as related to the Interim Port Authority To-Be Security Architecture
- Validate that controls are functioning properly and providing expected level of security protection

Activities performed by SST:

- Identify up to 3 applicable systems and controls to be audited
- Conduct audits IAW NIST Cyber Security Framework; map results to Final Port Authority To-Be Security Architecture to supplement and support gap definition

Client responsibilities:

- Provide Port Authority Primary Point of Contact for each audit
- Provide and coordinate timely access to all systems being audited and required supporting information sources
- Provide timely response to data inquiries
- Provide on-site work facilities as necessary

Deliverable(s)* and Time Frame

Deliverable(s):

- Supplemental update of Final Port Authority To-Be Security Architecture report
- Update will validate existing controls as defined in the Final Port Authority To-Be Security Architecture report based on results of audits
- Audits may confirm lack of effectiveness of existing controls resulting in identification of additional gap(s)

Time frame:

- Duration: 4 – 6 weeks
- Weeks 5 - 11

Assumptions:

- Port Authority Security Architecture is defined as the interim to-be architecture consisting of in-place security controls or currently planned security projects and capabilities (people, process, technology)

Task 5: Identify Future Audit Req.

Task 5 Summary

Objective:

- Define plan for conducting on-going technical process and/or related technology validation audits for systems and controls as related to the Final Port Authority To-Be Security Architecture
- Set expectation for the validation of all controls for proper functionality and that they are providing expected level of security protection
- Set expectation that all controls identified in the Final Port Authority To-Be Security Architecture report will be validated over time

Activities performed by SST:

- Establish a phased, multi-year plan to audit all currently deployed controls as well as all planned controls defined in the Final Port Authority To-Be Security Architecture
- Prepare final report; prepare and present project summary and final result.

- Client responsibilities:
- Provide and coordinate timely access to all information sources (reports, committees, personnel) as necessary
- Provide timely response to data inquiries
- Provide on-site work facilities as necessary

Deliverable(s)* and Time Frame

Deliverable(s):

- Supplemental update of Final Port Authority To-Be Security Architecture report
- Update will include phased prioritization for all controls identified in the Final Port Authority To-Be Security Architecture report as mapped to the NIST Cyber Security framework
- Final presentation

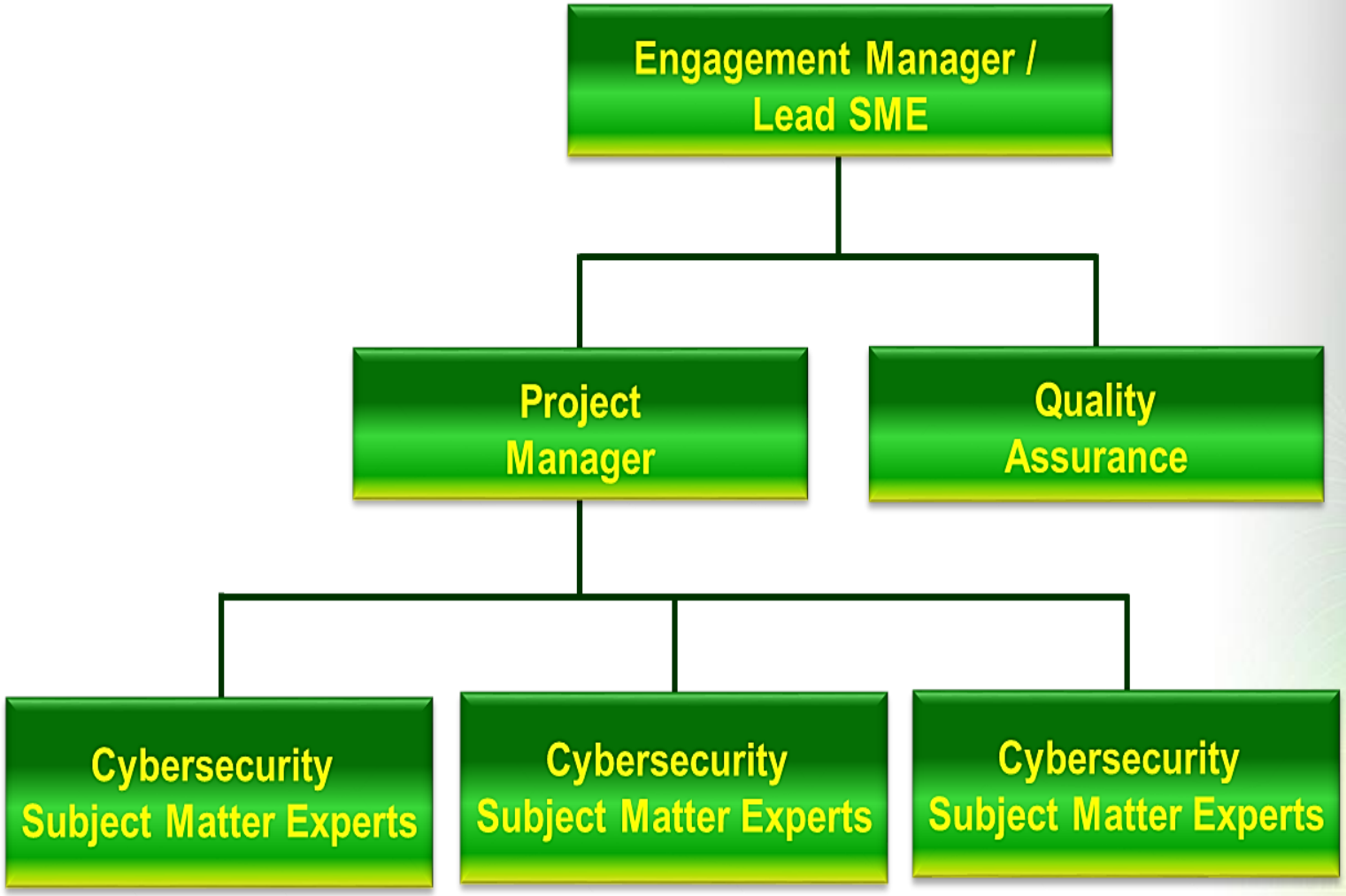
Time frame:

- Duration: 2 – 3 weeks
- Week 10 - 12

Assumptions:

- Port Authority Security Architecture is defined as the interim to-be architecture consisting of in-place security controls or currently planned security projects and capabilities (people, process, technology)

Project Team



Key Assumptions

- The Port Authority will designate a project manager to act as the primary point of contact for this project. The Port Authority project manager will be expected to work closely with the contractor as needed and will: (a) approve project priorities, detailed task plans and schedules; (b) facilitate the scheduling of interviews with appropriate client personnel; (c) notify contractor in writing of any project or performance issues; and (d) assist in resolving project issues that may arise.
- The work effort described in this proposal assumes that Port Authority personnel are available to assist in data gathering and data validation. In the event that Port Authority personnel are not available, a change of scope and/or timeline may be necessary.
- The Port Authority will review and approve documents within seven business days. If no formal approval or rejection with stated cause is received within that time, the deliverable is considered to be accepted by the Port Authority .
- The project manager is to schedule Port Authority resources for project activities and provide meeting facilities as necessary.
- Port Authority personnel will be made available per the final project schedule.

Project Network Security

Best of Breed" Network Security:

- Continuous endpoint threat monitoring to identify unknown malware, detect zero-day threats, and prevent damage
- Cyber intelligence reports and "feeds" for intrusion detection and prevention systems
- Off-site Managed Security Operations Center (MSOC) – Cloud Based Solution
- Professional services: assessments, penetration testing, incident response, safe exercises, & analysis

SAFETY ACT

- Support Anti-Terrorism by Fostering Effective Technologies Act
- Intended to encourage the development and deployment of anti-terrorism technologies by creating systems of "risk" and "litigation management"
- Technologies include:
  - Products, devices, equipment
  - Services – both supporting and stand alone services
  - Cyber-related items
    - Information technologies and networks
    - Integrated Systems
- Applies to an "act of terrorism," which may include cyber terrorism
  - Includes attacks committed by domestic terrorists
  - May include attacks on foreign soil, if harm is to a person, property or entity in the United States

Protections of the ACT

- Two primary level of protection -- different showings to DHS Designation
  - Liability cap at a pre-determined insurance level
  - Exclusive jurisdiction in Federal court
  - Consolidation of claims
  - No joint and several liability for noneconomic damages
  - Bar on noneconomic damages unless plaintiff suffers physical harm
  - No punitive damages and prejudgment interest
  - Plaintiff's recovery reduced by collateral sources
- Certification
  - All the benefits of Designation
  - Government Contractor Defense (presumption that the entity is immune from liability)

- **LOWER INSURANCE COSTS**

AAPA Cybersecurity Actions

- Design a Proprietary Cybersecurity Plan for Port Authorities
- Obtain Certification Approval from DHS
- Obtain Acceptance from Insurance Companies
- Work with the NIST 2014 framework
- Training packages for Board of Directors and Executives
- Assist ports with IT cybersecurity assessments
- Recommend a cybersecurity get-well plan and solutions
- Map cybersecurity programs to budget & investments
- Develop a scorecard to measure progress against set goals
- Issue Association Cybersecurity Certificate
- Recommend a Regional or State MSOC (Managed Security Operations Center)

CONTACT

Chuck Floyd

Security Solutions Technology

Phone: 301-273-5620

Email: chuck@chuckfloyd.com

www.securitysolutionstechnology.com