Presentation to:

AAPA Cybersecurity Seminar

March 11-12, 2015

Understanding the Business Risk

Mike Macaluso
CFO, Port Tampa Bay
Cybersecurity is the body of technologies, processes and practices. Designed to protect networks, computers, programs, and data from attack, damage or unauthorized access.
BETTER QUESTION…

WHAT IS CYBERSECURITY AS IT RELATES TO PORTS AND WHAT DO WE NEED TO PROTECT?

Different Things for Different Ports
Based upon business requirements & objectives
Landlord Operating

For Port Tampa Bay:
- Credit Card Information
  - Customers paying invoices with credit cards
  - Parking Garage
- Port Access Information
- Employee Information

“The identity I stole was a fake! Boy, you just can’t trust people these days!”
HOW IS UPPER-LEVEL MANAGEMENT INFORMED ABOUT THE CURRENT LEVEL AND BUSINESS IMPACT OF CYBER RISKS?

- Ongoing Meetings with Port President
- Executive Steering Committee

“ Somebody broke into your computer, but it looks like the work of an inexperienced hacker.”
WHAT IS OUR PLAN TO ADDRESS IDENTIFIED RISKS?

- Ongoing Process
- Work with Partners (Microsoft VAR, etc.) to evaluate network
- Penetration Assessment Testing
- Review Infrastructure for Intrusions Quarterly
DOES OUR CYBERSECURITY PROGRAM APPLY INDUSTRY STANDARDS AND BEST PRACTICES

- Yes, to the extent possible keeping cost justification in mind
- Constant Communication with Partners and relevant associates
- Recognition by Port President of the Critical Nature of Cybersecurity
- Continual Evaluation of IT Budgets, Acquisition Plans, etc. to Ensure Cybersecurity objectives are met.
- Co-Location Site (DR/BC) – Duplication of Processes
- Cybersecurity Insurance

“Memo: To all personnel, effective immediately we will be using the new security standards in all company correspondences, so please remember to use the secret-say ode-cay.”
WHEN DOES UPPER-LEVEL MANAGEMENT GET NOTIFIED OF ANY CYBER INCIDENTS

- Port President immediately & always
- No Matter How Extensive the Incident
- Other levels of management as required

“"I’m no expert, but I think it’s some kind of cyber attack!”
What do we do to respond to a cyber attack?

- Address the situation immediately, contact partners as necessary
- Report to Port President first, others as required
- If operations are compromised, determine most expedient method of restoring

"The virus is that bad, huh?"
DO WE TEST OUR RESPONSE PLAN?

- Equipment
- Daily Reporting
- External partnerships
- Continual Assessments