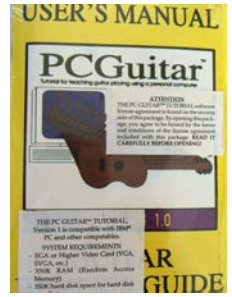
MARINE CFO

Dean Shoultz

- Dean Shoultz
  - Started first technology company in 1982, professionally in 1985 (pre-internet, pre-everything, BBS days)
  - Authored PC Guitar in late 80's
  - Authored popular mid-market accounting systems used by thousands of companies
  - One generic accounting customer was a large OSV operator in the Gulf of Mexico
    - Approached us to extend the generic system for specific use in the marine industry
    - What originally started as a back office ERP system became Marine specific
    - Moved to onboard data collection utility
    - Understand their perspective and pain points deeply
  - Technology experience
    - Software
    - Cloud
    - Mobility
    - Big Data
    - IoT



I’m Scared, Very

- Concerned over how naïve our country seems to be
  - DNC cyber attack gets a few hours of press
    - Not a Pearl Harbor moment, but profound
  - Press about building walls to keep friendly neighbors out
    - Billion dollar walls can be tunneled under for a few hundred dollars
    - IT firewalls are the same way, can be subverted by a kid in his bedroom
  - States are attacking us
- All companies will become tech companies
  - Who would have though Amazon would have become one of the largest commodity technology companies on the planet
  - They had to do it themselves, speaks to infancy of industry
  - Perception of technology departments seems “quaint”, as if the train wreck wasn’t coming
- False perception of security
  - HTTPS…ex employees of certificate issuers. Keys everywhere
- Reminds me of global warming
  - Move slow, be indifferent to coming storm, and hope it works itself out
  - Lack of concern

Why I’m Scared

- Deep understanding of technology
  - Realize the importance
  - Business, automation, etc.
- Unique vantage point of where it has come from, and where it is going
- Extreme patriot

Why Is It Becoming More of a Problem

- IoT 15T gold rush will lead to blatant mistakes, born of greed
- Exponential growth of data
- Exponential growth of mobile technologies
- Automation
- Increasing need to share slices of information
  - Horizontal and vertical partitioning
  - API's

Increased Security Risk for Marine Industry

- More connected vessels
  - IoT and sensors
  - Smart clients
- More connected business
  - EDI (pickups, drops, arrivals, etc.)
  - API integrations
- Cloud and mobility usage
  - Data at rest
  - Data in motion
- Vessel connectivity methods
  - WiFi, 4G
- Automation, autonomy, remote devices
- AIS is miserably unsecure, yet struggling to innovate with it
- Gross under-estimation of vulnerabilities

Marine IoT Topology: 100's of Targets

Vessel365 BY MARINECFO

Data Sources

Streaming Vessel Diagnostics

Public API'S and Datasets

Commercial Data and ERP

Legal and Insurance Data

Social Media

Ingest Processes

Windows Azure

Bi-directional API's

Email

Regionally consumed and replicated

FTP, FTPS. SFTP

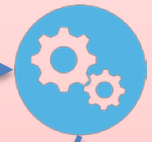
- Ingest targets
- Egress targets
- Data in motion targets (protocols)

Processing

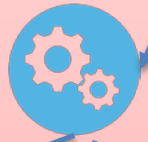
Windows Azure

Cleanse

Transform



Organize



NoSQL/JSON

Relational

Key/Value Pairs

- Data at rest targets
- De-normalized targets
- Storage targets
- CDN targets

Compute

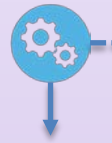
Windows Azure

Machine Learning

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Learn

Predict



Present

Consumers

Operators
Inspectors

Regulators
Surveyors

HSE
USCG

Legal
Insurance

- Virtualization targets
- Consumer targets (endless)

Applications – 100's of targets

- Enterprise apps
- Cloud apps
- Mobile apps
  - API calls
  - Provider attacks
- Data Center
- Solution Providers

Anatomy of an Attack

- Typically 4 phases
  1. “Survey” or gaining information about an operator or vessel through social media, technical forums and hidden properties in operators’ websites.
  2. “Delivery” in which attackers attempt access to office or vessel systems and data. This can be done from within the operators’ office or vessel or through remote internet connectivity.
  3. “Breach” is the extent which an attacker can access office or vessel system and data.
  4. “Affect” is extent of damage the attacker create within the office or vessel system and data.

Untargeted Attacks

- Use techniques from the internet to locate network weak points onboard a vessel
  - Social Media
    - Attackers manipulate crewmembers into compromising security procedures, through interaction via social media
  - Phishing
    - Sending emails to potential targets directing crewmembers to visit a fake website using a hyperlink
  - Water Holing
    - Fraudulent website in order to exploit crewmembers. Ransomware. Malware which encrypts data on systems until such time as the distributor decrypts the information

Targeted Attacks

- Sophisticated using techniques created for targeting particular operators or vessels
  - Spear-phishing
    - Phishing but individuals are hit with personal emails containing links that automatically download malicious software
  - Deploying botnets
    - Distributed Denial of Service attacks
  - Subverting the supply chain
    - Compromises equipment or software being delivered to the towing operator or workboat

Risk Assessment & Vulnerability

- Perform potential risk assessments of threats that could realistically be faced both ashore and afloat
- The complexities of vessels, and the dependency on connectivity shoreside services via the internet, make onboard systems increasingly vulnerable to cyber attacks
- Stand-alone systems will be less vulnerable to cyber attacks compared to uncontrolled networks or those with direct internet connectivity
  - Vessel and Barge Management Systems
  - Integrated Wheelhouse System
  - Propulsion/Machinery Management
  - Power Control Systems
  - Administrative/Crew Access Systems
  - Communication Systems

Entity Considerations

- Information Technology
- Operational Technology
- Securables
  - Vessel asset hierarchy
  - Crew
  - Facilities
  - Apps and data
  - Sensors
  - IoT Driven Data
  - Systems
  - Much more…

- Human Elements
  - Crew
    - Unintended (injection of malware)
    - Malicious
  - Operators
  - Customers
    - EDI Conversations
  - Service Providers
  - Brokers, charterers
  - Electronic Integrators
    - Land Mines
    - Magic 8 Balls

Fail to Plan, Plan to Fail

- Corporate Culture Plans
  - Engrained in the psyche of the organization
  - Not only an “IT” function
  - On-going
- Mitigation Plans
  - Can delay the attack long enough to discourage the attacker to the point of attack termination
- Disaster Recovery
- Identity Management Plans
  - Active directory
  - Independent security (i.e. SQL, passport, etc.)
- Communication Plan
- Capital Plan
- Must be VERY detailed
  - Written guidance plans only go so far
  - Memorialized and implemented through technology and machinery
  - Change management and training

Technology Solutions

- Secure protocols only
  - FTPS
  - SFTP
  - HTTPS
  - TLS
- Use security tokens that expire in short time periods for API or mobile app calls
  - 3o minutes max
- Certificates for IP calls
- 3 step (or more) authentication techniques

Onboard Cyber Threat Training

- All crewmembers should have Cyber Threat training covering the following:
  - Identify risks related to emails and how to utilize email in a safe manner
  - Identify risks related to internet usage, including social media, forums and cloud-based storage where data is less controlled
  - Identify risks related to the use of personal devices
  - Identify risks related to installing and maintaining software on vessel hardware
  - Identify risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed
  - Identify how to safeguard user information, passwords and digital certificates
  - Identify cyber risks in relation to the physical presence of non-company personnel
  - Detecting suspicious activity and how to report a possible cyber incident
  - Awareness of the consequences of cyber attacks on the safety of the vessel
  - Understanding how to implement preventative maintenance such as anti-virus and anti-malware, updates, and backups
  - Procedures for protecting against 3rd Party removable media before being connected to the vessel's systems

Upgrades, Software Maintenance, & Policies

- The use of hardware and software no longer supported should be carefully evaluated by towing operator as a cyber risk assessment
- All onboard hardware and software installations should be updated to the most current security level
- Procedures for timely updating of software may need to be put in place taking into account the ship type, speed of internet connectivity, sea time, etc.
- Software includes computer operating systems, which should also be kept up to date
- Additionally, the following tasks should be coordinated with the Software Service Partner:
  - Anti-virus and anti-malware tool updates
  - Strict adherence to administrator privileges
  - Deletion of inactive user accounts
  - Strict policy on 3rd party contractor access to onboard systems
  - Strict & robust password policy
  - A clearly defined physical & removable media controls
  - Proper policy for equipment disposal & data destruction
  - Clear lines of support from the Software Services Partner

A Good Defense

- Hardware, software, & data protected by multiple defense layers are more resilient to cyber attacks than a single layer of defense
  - Multiple layers of technical features
  - Robust policies
  - Security procedures
  - Access controls
- Existing security measures preventing access to the ship may be considered as a layer
- Preventing unauthorized access to the vessel and onboard systems has a role in ensuring that vulnerabilities are not introduced
- Operators should align their cyber security policies with the requirements of policy (i.e. Sub Chapter M, DHS Security protocols, etc.)

Response Plan

- Identify the cyber attack incident
- Define response objectives and investigate
- Take appropriate & immediate action against the cyber attack
- Recover & restore systems, data and connectivity
- Debrief

Cyber Security is a Team Effort

- Recovery plans should be accessible to shoreside staff, crewmembers, & the Software Services Partner in accordance with their responsibilities defined in the Cyber Security Plan.
  - The purpose and scope of these responsibilities should be defined and understood by all parties.
- Essential information and software backup facilities (eg the Software Services Partner's assets) should be available to ensure recovery can take place following a cyber attack.
- Recovery of essential system functions related to the safe operation and navigation of the vessel may have to take place with assistance from the Software Services Partner.
  - Services Partner needs to be part of the recovery planning carried out by the crew in cooperation with the shoreside operations.

Conclusion

- Overly willing to help

Thank You

dshoultz@marinecfo.com