Case Study:

Using Cybersecurity Risk Management Techniques to Improve the Security Posture of a Major Cruise Ship Line

COMPUQUIP
CYBERSECURITY

I. Introduction

Risk management plays a critical role in helping IT teams and business leaders identify where an organization is most vulnerable and what data is involved in higher-risk environments. The ultimate goal is to manage IT-related risks more effectively in order to better protect the company, its applications, its vendors, and its customer base. Promoting greater awareness of security threats and data vulnerabilities at all levels of your organization is an essential aspect of cyber risk management. This case study will explain the risk management techniques used by Compuquip Cybersecurity to increase the security posture of a cruise ship line.

> *Promoting greater awareness of security threats and data vulnerabilities at all levels of your organization is an **essential aspect** of cyber risk management.*

II. Project Background

People who have never been on a cruise before probably don't realize the complexity of the infrastructure or the number of systems in place for operating the ship. For example, there are shipboard monitoring and control systems that focus on alarms and monitoring, tank gauging, pump and valve control, engine monitoring, navigation, HVAC, and more. These and many other systems are critical to the operation of the vessel and the management of the crew, as well as the safety and satisfaction of the passengers. Similar to the complex industrial control systems (ICS) found at energy, transportation, nuclear, utility, and water plants, which are managed via a supervisory control and data acquisition systems (SCADA), cruise ships also have marine SCADA systems that are necessary to help control all of the systems involved.

When a leading cruise line needed a cybersecurity vendor with extensive knowledge and experience working with SCADA systems, they called upon Compuquip Cybersecurity. Coming into the project, and after sitting down and discussing the cruise line's needs and concerns about their current security posture, we devised a plan that revolved around a complete risk management approach. Additionally, the cruise line mentioned that they currently did not have visibility into all of their vendor networks and the assets behind those networks on each ship, which is a huge security concern.

Coming into the project, and after sitting down and discussing the cruise line's needs and concerns about their current security posture, we devised a plan that revolved around a complete risk management approach. Additionally, the cruise line mentioned that they currently did not have visibility into all of their vendor networks and the assets behind those networks on each ship, which is a huge security concern.

This was a fixed fee project that was delivered on time and within budget.

III. Risk Management Techniques

A successful risk management strategy should consist of several key areas. Specific to this organization and industry, we focused on the following high-level areas/steps:

- Asset Discovery
- Risk Assessment
- Prioritize Risk
- Remediate Risk

Several tools and tests were used to assist us in this project, allowing us to identify risk, analyze networks and assets to compare to a physical audit, set up monitoring and alerting to changes in IoT devices and their behavior, as well as implement reactive security orchestration, automation, and response (SOAR) between security layers and technologies. We also performed a penetration test to identify any weaknesses within the internal networks as well as from the external network coming in.

IV. Business Benefit

The benefit of these risk management techniques used consists of the following:

- Identify security vulnerabilities
- Determine new security requirements
- Justify spending
- Make smart purchases
- Improve planning
- Document due diligence

Savings Impact

The savings impact of these risk management techniques proved to be substantial. By increasing visibility across different networks, automating processes, and giving the operations team the ability to orchestrate various security tasks, the cruise line was able to save both time and money while also improving passenger safety.

Translatability

The basic risk management areas mentioned above are easily translatable to various parts of cybersecurity. From the steps such as asset discovery, risk identification, and remediation, management teams will be able to make better budgetary and planning decisions. Also, WiFi analysis and unique use case deployments were performed, which can be passed onto other departments within the organization.

V. Lessons Learned

The biggest challenge faced here was in the interaction with the various systems that were controlled by their respective vendors. This introduced a logistical challenge of coordinating time to gather the appropriate information in order to properly deploy the solution. Identifying the number of systems involved and understanding the interaction between them during the discovery process significantly reduced the chance of delays or other problems during implementation.

VI. Conclusion

Assisting a cruise line by deploying a risk management approach across their entire organization was not only rewarding, but also showed us the many systems that are vital to the smooth operation of each ship in the fleet. With cyber risks continuing to grow, making good risk management decisions really does matter. Rushing through the decision-making process and always saying "no" are not the right answers. A better answer is to implement a consistent risk management program like what was done here. Cyber events may still threaten your organization in the future, but with the help of Compuquip Cybersecurity, you will be better prepared to deal with them.

COMPUQUIP
CYBERSECURITY

Email: info@compuquip.com

Phone: 789-641-5437

Address: 2121 Ponce De Leon Blvd. Suite 530
Coral Gables, FL 33134

Follow us on: