SOP-GEN-033 Cyber Security

1.0 Introduction

This document outlines the various information assets on our ships, as well as a consideration of the most likely threats to data loss, loss of service. It consists of an inventory of the components, and a list of threats that we consider significant enough to mitigate against. Any threat to our systems that is not considered on this list is either deemed highly unlikely, or impractical to mitigate against.

This cyber security risk assessment is limited to only those systems used in the management and maintenance of the ship's operations. Information management and associated risks to systems that are part of the survey work are in accordance with the requirements of our clients on a project by project basis.

2.0 Our Cyber Security Philosophy

Protecting systems against cyber security threats can never be fully mitigated.

For example, updated virus definitions on a laptop will only mitigate against viruses that are known. The laptop still has a chance of acquiring a virus within the window between its initial release and its eventual incorporation into anti-virus definitions.

In many cases, the protection against a threat requires expending costs that outweigh the value of the asset protected. Such costs can be intangible in nature, for instance, the loss of work product from employees who are required to implement aggressive security procedures that limit or impede their access to the information resources

necessary to do their jobs, is a real security cost that over time is greater than the value of the asset.

We strive instead to provide a balance. We protect to a reasonable degree, recognizing the risks of our choices and provide for rapid recovery from the occasional loss.

We also take care to not put sensitive information on systems that have a high potential to be compromised. However, for machines that do contain sensitive information, we take extra measures to protect against their potential compromise.

Such machines are typically not available to other machines on any network, limiting the dissemination of such information to a manual process, which is highly unlikely. Physical access to such machines is also limited to only IT personnel and upper management.

Since, the machines on our ships are physically available to persons we do not control, we are forced to consider such machines as unsecure, and not store sensitive information on them.

3.0 Information Assets on Our Ships

The following is an inventory of information assets that typically exist on our vessels to aid in the management of the vessels, and are subject to a cyber security threat assessment.

- The Ship File Server
- The Bridge Email Computer
- Computer-Based Maintenance & Compliance Computer
- Watchkeeper Computer
- Engineer / Captain Laptop
- Ship Network

4.0 The Ship File Sever

The ship file server provides a publicly available drive that is accessible as a temporary and unsecured storage area for non-sensitive information.

It also provides for an automation platform to acquire information and share such information back to the home office. For instance, it reads the current latitude and

longitude of the ship from the VSAT System, and once every 2 minutes shares that information with the Shore-Based Servers at the home office.

4.1 Risks to the File Server

- Power failure
- Malware & Intrusion
- Hardware failure

5.0 Power failure

A power failure is a risk to the service provided by the machine and a potential risk to the hardware on the machine.

5.1 Power Failure – Mitigation

We provide a UPS system that protects against power surges and power loss. We also label the UPS with the date the system was put into service to give us an idea of the age of the battery. We periodically change out batteries, or UPS systems as needed.

6.0 Malware & Intrusion

The risk of Malware and Intrusion for the ships file server is very low, considering its isolated on the network behind a firewall, with no ports forwarded to it from outside of our networks.

There is of course, the exposure of the files on the shared drive, that are subject to destruction by malware on the computers that have access to them (i.e., ransomware). Thus, there is the risk of time lost necessary to recover them.

6.1 Malware & Intrusion – Mitigation

The only real source for malware would be from machines on our networks. This is mitigated by limiting through the router, which machines can access the firewall.

We also have as a matter of common practice, the installation of Rootkit detection systems.

The files on the shared drive are protected from malware by a backup system. This backup system saves all versions of the files every day for a minimum of thirty days to a

location on the server that is inaccessible to other machines on the network. We consider it highly unlikely that such damage will go undetected for 30 days.

7.0 Hardware Failure

The primary risk posed from hardware failure is to the availability of the servers' resources, and data loss.

7.1 Hardware Failure – Mitigation

The primary method of protecting against data loss is through the use of a Raid array such that, both hard disks must fail in order for the machine to fail.

Other hardware, such as the Motherboard, Power Supply. etc. we do not protect against failure, since there are typically other sources for the same information, that are perhaps more inconvenient, but not so much so, to require that we have a redundant file server system on board the vessel.

8.0 Ship Laptops

The vessels that are operated by TDI-Brooks International Inc. are provided with e-mail laptops set up with tdi-bi.com e-mail accounts, and used for communications back to the office and other parties. Also included, are Computer-Based Maintenance and Compliance laptops used by Ship Crew and are complemented by Engineer & Captain laptops located by the engine room / captain's room.

The foreign operated vessels are provided with ISF Watchkeeper laptops which are required since they operate in International Waters and the crew must document seafarer work and rest hour compliance.

8.1 Risks to the Ship Laptops

- Power failure
- Malware & Intrusion
- Hardware failure
- Theft

8.2 Power Failure

A power failure is a risk to the service provided by the machine, and a potential risk to the hardware on the machine.

8.3 Power Failure – Mitigation

The laptops are connected to a UPS system that protects against power surges and power loss. The laptops also have batteries which provide some additional leeway in case of power lose.

8.4 Malware & Intrusion

The risk of malware and Intrusion for the ships laptops is low considering they are isolated on the network, behind a firewall and provided with antivirus and malware software. However, no system is 100% protected. Thus, there is the risk of time lost, necessary to recover them. The laptops anti-virus software is automatically updated and checked remotely for any issues, monthly.

8.5 Malware & Intrusion – Mitigation

The source for malware would be from users clicking on phishing links, or installing malicious software, or other machines on our networks. This is mitigated by training users not to click on suspicious links or open unknown e-mail attachments, visit non work-related sites, download software and by limiting through the router which machines can access the firewall. We also have, as a matter of common practice, the installation of Rootkit detection systems.

The files on the laptops are protected from malware by a backup system when files are saved to the N-drive. This backup system saves all versions of the files every day for a minimum of thirty days to a location on the server that is inaccessible to other machines on the network. We consider it highly unlikely that such damage will go undetected for 30 days.

All laptops are set up to be remotely connected to from the main office and for monitoring, updating, and software repair.

8.6 Hardware Failure

The primary risk posed from hardware failure is to the availability of the laptop resources, and data loss.

8.7 Hardware Failure – Mitigation

The primary method of protecting against data loss is backing up data on the N-drive located on ship server and through the use of a raid array, such that both hard disks must fail in order for the machine to fail.

Other hardware, such as the laptop itself, power supply, monitors etc. We do not protect against failure from, since there are typically spare components and laptops which can be repurposed in case of emergency on board the vessel.

8.8 Laptop Theft

There is a possibility that the laptops might be stolen but this event has not occurred. The greatest risk is while docked, and by outside parties.

8.9 Laptop Theft – Mitigation

A TDI asset sticker is placed on each TDI laptop and logged into our Equipment Tracker. In addition, the laptops are monitored remotely, and ship crew can be contacted to verify location of laptop

9.0 Ship Network

9.1 Risks to the Ship Network

- Power failure
- Unauthorized Access
- Hardware failure.

9.2 Power Failure

A power failure is a risk by disabling the use of the network, due to outages of the routers and switches required to properly route the network traffic. This is usually a temporary issue when the ship changes from ship generator to shore power or vice versa.

9.3 Power Failure – Mitigation

We provide a UPS system that protects against power surges and power loss. We also label the UPS with the date the system was put into service to give us an idea of the age of the battery. We periodically change out batteries, or UPS systems as needed.

9.4 Unauthorized Access

Unauthorized Access refers to individuals accessing our networks, data, applications, or devices, without receiving permission.

9.5 Unauthorized Access – Mitigation

We implement and apply reasonable security safeguard practices and procedures, to protect the network and infrastructure assets, as well as the data and information the network accesses, processes, or transmits. Unauthorized access is managed by VLANs on the managed switches separating various groups of users and resources appropriately.

9.6 Hardware Failure

The primary risk for network failure is due to the integrity of the network cable being cut, disconnected, or reconnected to the wrong ports. In addition, due to the misconfiguration or outage of routers, or switches, could detrimentally affect the network intentionally or unintentionally.

9.7 Hardware Failure – Mitigation

The primary method of protecting against network failure is a proper implementation of the network using patch panels, securely placed in cabinets, and following planned, and standardized network configurations. Currently we have updated to CAT6 cabling, providing a more robust and stronger connection interface.