



An essential white paper on Cyber Security



Prepared by:

Ashwini Almad
Cyber Security Strategy & Planning
Royan Carvalho
Systems, Networks, Cyber Security
Richard Fernandes
Operations Head (Software)


Capt Ruchin C Dayal
CEO – eDOT Solutions
Master Mariner
FIIMS, AMS-SAMS, AFNI, MAIMS



Introduction – The Risk

Today, the digitization of the shipping industry has automated and integrated nearly all relevant critical processes resulting into a highly productive environment. Improved automation of the communication and bridge systems requiring greater network connectivity are being catered to with advanced shore to ship satellite connectivity.

Other increasing requirements such as the proliferation of BYOD (Bring Your Own Devices) with 24x7 connectivity pose a greater risk of compromise of organization's critical assets. Cybercriminals have been employing both targeted and commodity attacks to gain foothold within an environment and steal critical data to benefit financially or steal proprietary technology.



What you can do to combat cyber attacks

Reducing The Impact
Most cyber attacks are composed of four stages: **Survey, Delivery, Breach and Affect**. The following **security controls**, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey

Delivery

Breach

Affect

User Education
Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Network Perimeter Defences
Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection
Can block malicious emails and prevent malware being downloaded from websites.

Password Policy
Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration
Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

Patch Management
Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring
Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection
Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration
Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access
Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training
User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls
Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Controls For The Affect Stage
Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help. *To Cyber Security* outlines many of the features of a complete cyber risk management regime.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.


Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

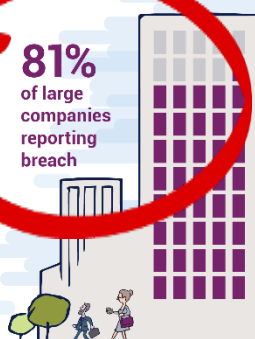
Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

£600K-£1.15m
Average cost of security breach



81%
of large companies reporting breach



For more information go to www.ncsc.gov.uk @ncsc

Insulation of the critical safety operational equipment (like the radar, ECDIS, GMDSS, etc.) from external cyber-attacks is hardly an option today; while cyber safety aspects need to be recognized as critical to the actual safety of the ship, the cyber security in form of keeping the integrity of critical data intact cannot be undermined. A malicious attack on a ship can be debilitating and prevent cargo bookings, production of cargo documents, payments of ships dues and supply invoices that could lead to financial loss and disruption to services.

In 2017, the targeted attack at MAERSK, triggered by ransomware, possibly has costed the company as much as \$300m in lost revenue. Several shipping bodies such as the IMO and BIMCO have provided general guidance which can be leveraged as a baseline or framework in building a cybersecurity strategy. But as a part of the risk management plan, shipping organizations must assess if they are likely to be a victim of an attack and build defenses accordingly. Cyber safety as well as Cyber-security

will require a careful study and adoption of necessary, contemporary & sustainable strategy. This white paper provides recommendation for security controls and processes that must be implemented to address the growing threat landscape. A defense in-depth approach will provide organizations the confidence to combat cyber-attacks and protect their critical infrastructure.

Challenges

Targeted attacks were viewed as black swan events that happened to other organizations, not any more. A look at the attack landscape and the techniques involved across a range of industries must acknowledge the changing threat environment and adjust their own risk calculus and defenses accordingly. Here are a few cybersecurity risks weighing on the shipping industry.

Adoption of New Technology

Adoption and cloud, BYOD (Bring Your Own Device), IoT is on the rise. While BYOD adoption can be considered the future of employee satisfaction and entrepreneurial management, it also poses challenges with security and privacy.



The increase in web applications, cloud computing and Software as a Service (SaaS) offerings, and the Bring Your Own Device (BYOD) phenomenon are driving employees, business partners and customers to increasingly access information on devices are not managed by IT departments.

This has resulted in security implications for data leakage, data theft and regulatory compliance. To protect valuable information, organizations must stop making a distinction between devices in the corporate network and devices outside of it.

New Attack vectors

Similar to other sectors, emerging cyber threats in the port environment are diverse and complex. Cyber risks manifest themselves as both safety and security concerns. Every day our networks and devices expose to risks and security attacks perpetrated by cybercriminals. Vessel and facility operators use systems and cyber dependent systems for navigation, communications, engineering, cargo, ballast, safety, environmental control, and emergency systems such as security monitoring, fire detection and alarm systems.

A recent set of attacks against critical infrastructure entities, such as oil and gas pipeline operators, utilities and even some city and state governments reveal new motives and methods. The attackers were not out to steal data but were looking to disrupt services.



The attackers used a new attack vector that has not been seen before. Instead of attacking their primary targets directly, they attacked less secure vendors that those targets use.

Lack of Security Personnel



With digital transformation and the evolution of web and cloud applications and services currently offered, it's hard for the shipping industry to fill many of their information technology (IT) positions, let alone ones that require security expertise.

They don't have the right sized teams and operate in an understaffed mode. Often, the cybersecurity teams lack basic as well as advanced skills in areas of patch management, security analytics, cloud computing security, putting more pressure on the most experienced staffers to pick up the slack.

Regulatory Compliance

International governmental bodies, national governments and industry organizations have all mandated shipping organizations to integrate security into their operations and have implanted regulatory requirements to increase transparency, accountability, and efficiency of operations.

Deficiencies in the security infrastructure or operations results in increased cargo inspections to ensure they do not represent a threat to the receiving port facility. Unanticipated inspections result in delays that cascade through the supply chain, resulting in increased costs to the carrier and loss of revenue for the cargo recipient.



Recommendations

Building a robust cybersecurity policy addresses and aligns several participants in an organization. The primary purpose is to inform the user: employees, contractors, and authorized third party users of their obligations to protect the technology and information of the organization. The policies describe their responsibilities and privileges. The evolving threats come in every shape and form from targeted, non-targeted, commodity, insider, and unauthorized user attacks.

Having a robust cybersecurity strategy and roadmap enables shipping organizations to adopt newer technology with the agility and speed to further their business value. Here is a list of basic controls and policies that must be implemented to provide necessary protection.

All these policies need to be evaluated from an added lens of compliance to avoid any violation or infringement of compliance regulations. The list is non-exhaustive but must be worked upon as a minimum viable model.

1. **Network Security/Firewall Policy**

This policy describes what is allowed to pass through the firewall by default and the process for acquiring exceptions to the policy. This policy includes procedures around device passwords, logs, firewalls, networked hardware, and/or security testing. For example, by default no traffic is allowed to pass through the firewall from the outside directly through to the inside with an Internet routable address. While most companies have this developed to an extent, sophisticated attack techniques and

constant innovation involving access-ready-made 'Exploit as a Service' (EaaS) programs is increasingly easy, making it simple to initiate, successfully deploy and benefit from an attack, even for less tech-savvy criminals. Skillful social engineering is used to prompt the user to run the installation routine of the ransomware.

2. *Email Policy*

This policy includes the company's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. This serves to protect shoreside and onboard personnel from social engineering to obtain sensitive information, prevent web browsers and email clients from executing malicious scripts. For example, you may receive an email that reads something like this: "My organization's requirements are in the attached file, please provide me with a quote. "Producers of ransomware operate in a highly professional manner.

This includes providing a working decryption tool after the ransom has been paid, although this is by no means guaranteed

3. *Incident Response Policy (Disaster management Plan)*

This policy defines protocol when a security incident such as a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data occurs.

4. *Backup/Recovery Policy*

This defines what is acceptable in terms of documentation of backup/restore process, as well as the storing of and length of time to keep backups. Backups are a must considering the regulatory and compliance mandates and the threats of cybersecurity on a daily basis. It requires a well thought out, reliable, efficient backup ensuring the Confidentiality, Integrity, and Availability (CIA) of critical data.

5. *Acceptable Usage Policy*

This policy highlights what is and isn't acceptable usage of the company network resources. The scope of this policy includes any and all use of corporate IT resources, including but not limited to, computer systems, email, the corporate network, and the corporate Internet connection.

6. *Password Policy*

The password policy is the first step in enabling employees to safeguard your company from cyberattack. This policy would apply to any person who is provided an account connected to your corporate network or systems, including: employees, guests, contractors, partners, vendors, etc.

7. *Wireless Access Policy*

With the explosion of BYOD, pervasive wireless connectivity is almost a given at any organization. This policy applies to all wireless infrastructure devices that connect to a network or reside on a site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets.

8. *Patches/Updates Policy*

By policy all the systems must be as up-to-date as reasonably possible to prevent hackers from exploiting published vulnerabilities. This includes systems that contain company or customer data owned or managed by the company regardless of location - systems including Unix, Solaris, Windows servers, and Workstations.

To begin implementation of these policies a thorough assessment of the environment is needed. This assessment will identify vulnerabilities and misconfigurations that could result in loss of operation of system, equipment, network and the ship. A blueprint with the assessment provides the knowledge of the managed assets, unmanaged assets, existing configurations/ patches will help prioritize the list of actions to keep the crown jewels protected.

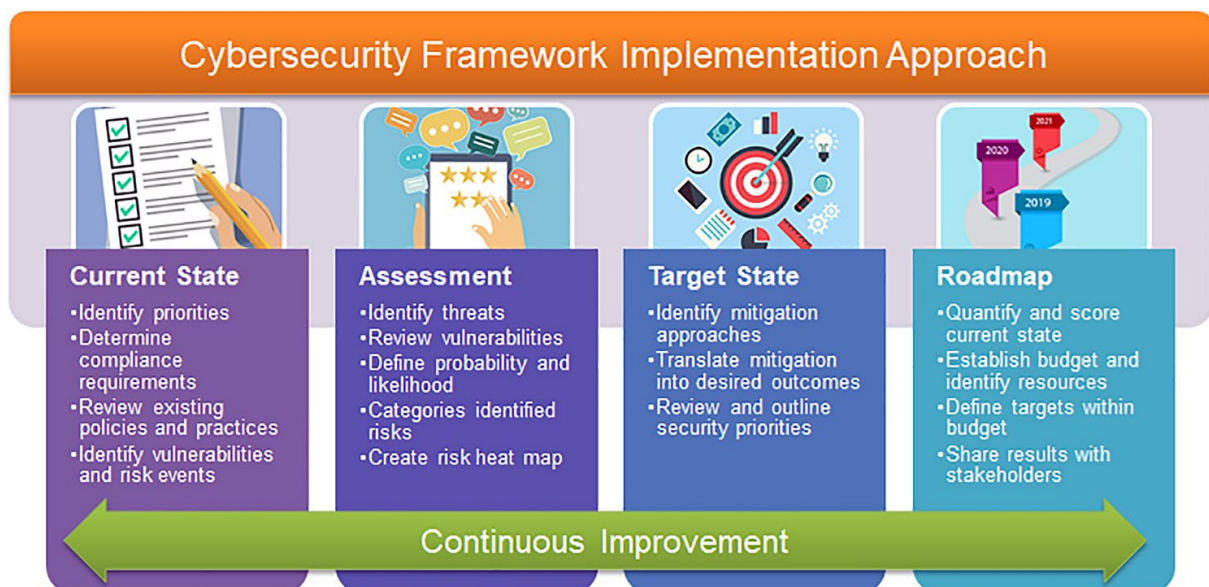
Solution

Engaging with professionals with experience in this field; to create a blueprint which involves assessment and evaluation of existing and potential vulnerabilities and its impact, resulting in a defensive in-depth solution. The solution will have to be prioritized based on technical and procedural actions detailing the effectiveness, cost, and applicability of the recommendation.

It is important that engaged professionals speak the language of ship managers, understand the nuances of the trade and provide practical, cost effective & sustainable solutions.

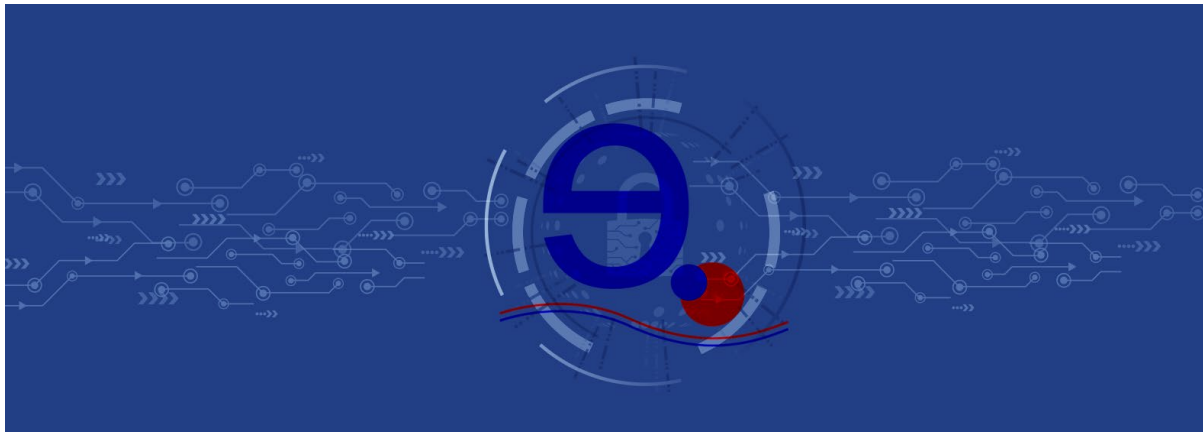
Project Cyber Security & Safety

Here is an example of the processes which the eDOT Cyber Security Professionals follow to implement an effective cyber security solution.



After the initial assessment of the direct control office as well as a visit to a floating asset, a detailed timeline, business case, implementation, and costs are provided. Some of the steps along the way are as follows;

- Assessment Interviews
- Systems Audit
- Risk Assessment
- Procedural Solutions
- Technical Solutions
- Prioritize Recommendations
- Implementation
- Third Party Audit and Reporting
- Continual Analysis and Improvement.



This white paper has been authored by a team from eDot Solutions comprising **Ashwini Almad** - *Cyber Security Strategy and Planning*; **Royan Carvalho** - *Systems, Networks, Cyber Security*; and **Richard Fernandes** - *Operations Head (Software)*; under supervision by **Capt Ruchin Dayal**, *CEO*, eDot Solutions.

eDot Solutions is committed to provide consultancy, as well as dynamic cyber security management services to ship managers, owners and operators. Having successfully merged the shipping and the IT sectors, eDot understands the seafaring mindsets, thus providing real-time value propositions rather than getting lost in over information bombardment.

eDot inspectors are certified ISO 27001 lead auditors, who can help incorporate provisions for cyber security into SMS manuals, thus ensuring compliance to VIQ7.

We'd love to hear from you!

We are here to observe, engage, discover and partner in your journey to make it phenomenal.

You can email us on contact@edot-solutions.com

You may also call us at **+91 832 2501715** or simply walk into our offices.

Our offices are in India, Singapore, Houston and Philadelphia. Office addresses can be found on website www.edot-solutions.com