Naval Automation
Cyber Defence Guidelines

Cdr. Davide CARDELLICCHIO[a,1]
[a]*Italian Navy General Staff*

Abstract. It's been 15 years since "cyber risk" was identified as the new millennium threat, potentially affecting organizations, industries, governments and society. Despite choral worries, the naval context has seemed to remain unaffected for years, as long as ships could have been considered "isolated systems" floating offshore. But, as new technologies[2] (either commercial or military) had spread out on in this rapidly becoming "information-dependent" and "inter-connected" shipping industry, cyber risk finally become a threat [1]. As the matter turned into business, many solutions have been developed in order to grant cyber-security, at every user level (i.e.: personal, office, enterprise, server farm). Could these solutions completely protect a ship themselves? How much a ship-owner has to invest in cyber-security? How he could efficiently face cyber-threat? This kind of questions generally have no straight answer because nobody can find a proper solution without a proper assessment, tailored on the specific case of context.
This work is intended to advise ship owners on the importance of an effective cyber-risk assessment before the choose of a cyber-security solution and, in the meantime, it suggests a simple way to conduct it, formulated on the basis of classical risk-assessment procedures.

Keywords. Italian Navy, Maritime Security, Naval Automation, Cyber Threat, Operational Technology, Risk Assessment, Comprehensive Approach.

1. Introduction.

For many years, cyber risk has never been counted among canonical risks pertaining to merchant or military shipping. The need to communicate, supervise routes, reduce manning, monitor either technical or logistic parameters, provide remote assistance and, last but not least, to give leisure and moral support to the crew, has today led ship-owners to add computerized and interconnected assets to their fleet. However, this evolution has opened the door to cyber risk.

In recent times, many episodes, too often fictional, have brought terms like "hacker" and "cyber-attack" to the headlines. As a direct consequence, there has been one "rush to safety" by individuals and companies, while statutory organizations have generally had a more cautious and measured approach. As a result, Information

[1] Corresponding Author, email: davide.cardellicchio@marina.difesa.it.

[2] Integrated automation, Internet of Things (IoT), Satellite communications (SATCOMS) and various PC-based management systems.

Technology (IT) domain can nowadays count on a complete range of cyber-defense tools, and farms with a poor organizational attitude to guarantee their effectiveness.

Furthermore, these solutions respond much more to cost-to-convenience rather than cost-to-effectiveness criteria, leading to the failure of the main objective: proper protection. That does not mean that complex and expensive solutions are generally effective, but that every problem has its own specific solution and that ship-owners are the only ones responsible of the assessment and the choose of the right compromise between investment and residual risk.

As evidence of its importance, IMO, various Registers and maritime Organizations have made available high-level and practical guidelines on the subject [2][3][4][5]. However, the present work provides a slightly alternative approach and some useful advice to give ship-owners a greater awareness of the problem.

2. The paradigm of cyber security: naval automation vs office.

From a naval point of view, cyber matters cannot be approached in the same way, primarily because of the objectively high value of the target (ships, but also cargo, crew and, possibly, passengers). Choices concerning safety and security must consequently be weighted and coordinated carefully.

Moreover, operational requirements identifiable in the Operational Technology (OT) context are diametrically opposed to those related to IT where the canonical approach to cyber defense is "confidentiality first, then integrity and then availability". OT world has instead an “industrial approach”, that is "availability first, then integrity and then confidentiality". Technically, this means that in OT domain is more acceptable the loosing of information rather than interruptions or the loose of services. The damage potentially caused by a delay in the alarm system or in the control process of complex machineries - such as gas turbines - in fact, could lead to disastrous consequences. Cyber defense solutions implemented on board must therefore be suitably stratified, so as not to affect the performance of the OT domain and accurately protect the IT one.

Finally, one of the basic aspects of cyber defense is the adequate understanding of the term "security", which cannot be, in any case, dis-related to time context nor taken as a univocal and immutable measure. The goodness of any technological or organizational choice, in fact, is measurable only in the very moment in which the measure is carried out: as time goes by, the discovery of new vulnerabilities and the unstoppable evolution of threats will force a complete re-evaluation.

3. The need for the analysis and the approach to risk management.

Cyber security must not be seen in its exclusive technological aspect, because the problem is related, and largely, to human behaviour and weaknesses. The complexity of the problem moves away from the certainties of mathematics to penetrate the heuristic dimension of social domain. Although the context is different, there are no great conceptual differences between a modern-day hacker and a seductive post-war spy stealing information from unwitting political figures.

For any company it is necessary to carefully evaluate, among many problem, the impact of the fragility of the human element. An example, as trivial as enlightening, is that of the company that chooses the password management policy by imposing high complexity, absence of sequences and use of special characters, no popular terms, a password change every 20 days, etc. A policy as ingenious as socially ingenuous, because it will no longer be the "brute force" attack causing the collapse, but the employee's need to remember the password (humanly understandable), that will lead him to transcribe it on an support less secure and less inaccessible than his Personal Computer.

4. A methodological proposal

The most effective way to orient in this complexity is a preventive and adequate assessment of risk to which the system is exposed; one of the most effective methods, widely used in every contexts - including military - in which the number and the uncertainty of the variables involved is significant, is the "comprehensive approach" applied to "risk management". This tool provides a multi-domain analysis of the problem and the measure of it along its three main dimensions: the resources to be protected, the vulnerabilities of the IT-OT system and the threats in the environment. Through these, it is therefore possible to ideologically measure the "volume" of the problem, for the subsequent analyses aimed at its reduction. Even the most recent civil legislation (e.g.: ISO 9001: 2015, etc.) actually exploits this methodology.

4.1. Resources to be protected

This dimension is the most subjective one, as it provides for the evaluation of the economic loss related to the assets to be protected, which can however be both material and immaterial. In example, the downtime of a "mission critical" plant or of the entire ship, in addition to the consequent costs for repairs and possible towing in a safe harbour. However, also the impact on sales subsequent to any image damage or on the insurance, potentially increasing after one or more IT incidents, is certainly not to be underestimated.

Furthermore, the measurement must include the estimate of the economic loss caused by the compromising of information, whether these are of either technical or logistical nature, or related to the company business model. Every asset or intellectual property of the entire organization must be considered, remembering that the target of a cyber-attack could only be the "entry point", an intermediate objective for a different and bigger scope: a naval unit server can represent the door to access to financial data in the company central server, etc.

In a multi-layered optic, resources to be considered are not only those identifiable with a plain approach, as a company asset (or the company itself) can have an intrinsic value in the wider national or international context, not only economical. Consider, for example, the social impact (sense of insecurity, distrust, mass panic, and their political or economic consequences) of one or more public attacks toward banks or institution, even if they have not led to particular material direct consequences

4.2. Threats

The starting point here is the non-erasable presence of so-called "untargeted" attacks. Among them are all malicious applications circulating on the web, addressed to the entire community and generally non-specific (with the exception of ransomware). They can be considered as mines, wandering through computer platforms and responding to the most varied needs, not least that of the illicit personal gain. Just because of their generality, such threats are heavily widespread and, on the other hand, they are easily manageable using good procedures and updated antiviruses.

Although "untargeted" attacks can give rise to huge economic losses, the threat of greater magnitude is probably identifiable in the "targeted" attack, which is the one deliberately addressed to the specific person / organization. All types of malware, including generic ones, are a good choice if they could be functional to the attacker's purposes. Given the need for resources (time and money) to produce an effective malicious application, the discriminant - in this case - is just the value of the targeted resource that, in some cases, can justify the disproportionate use of the means available. It could be considered, for example, the strategic value and magnitude of potentially damage associated with either energy production infrastructures or airport traffic's management systems or also penitential structures management systems [6].

Furthermore, behind a threat, whether a targeted attack or not, there is always a conscious actor, his motivation and his means. Each organization should take into account this aspect and carefully analyse the environment in which it operates to identify potential hostile subjects, even if defined only by general features (e.g.: activists in the social layer, competitors in the commercial layer, etc.). Where appropriate, a company must also adequately consider the role it play in the national and international context and the value of its contribution - even if not directly related to its business - to the economy and the livelihood of its "country system". The assumption that the threat is only "untargeted" or that it comes from known and predefined directions could be a serious under-sizing of the problem.

4.3. Vulnerabilities

The dimension of vulnerability must be explored in its various forms, which can be substantially divided into three types of fragilities: technological, procedural and human related.

Technological vulnerabilities are the weapons used by hackers, term which can be referred either to the evil ones or the good ones, those driven by ethical values (so called "White hats"), who put their skills at the service of computer protection. With the competition in new software's development and the hardware's frenetic innovation, the complexity of IT systems is growing up today at an exponential rate, such as the number of technological vulnerabilities detected. Scrolling some free databases accessible on the web (e.g.: exploitDB, etc.), it is possible to gain awareness on what this exactly means: this is a specialized battlefield, not conveniently practicable by a company that does not make IT protection its core business.

Where organizations can (and must) play an active role is the field of "procedural vulnerabilities": all those fragilities related to the incorrect application of good standards of conduct. Obviously, the robustness of a house's door is irrelevant if

exiting your first floor apartment you left the window open. Hence, it is necessary to conduct an internal detection campaign, aimed at identifying all the potential procedural fragilities and, subsequently, countering them with appropriate and widely disseminated regulations. It is also necessary to take into account a more or less significant period for the refinement of procedures, but the expected result is undoubtedly effective.

Finally, to reap the benefits of the regulatory effort, it is necessary to manage the human element, which is almost ever the most fragile link in the security chain, such as in the previous example on password management policy. The message to be disseminated within the company is that IT security is not a specific prerogative of IT personnel, but that it is an everyone's responsibility. The objective is therefore the acquisition of an "organizational culture" oriented to cyber security, which must be appropriately stimulated and supported by the necessary investments in training. Various levels can be identified, from a basic preparation suitable to all the personnel, to the advanced training targeting the few "insiders" who can access - or even manage - the company's critical resources.

4.4. Risk mitigation

The analysis of risk and the measure of its "encumbrance" are only the first step towards the correct management of the cyber problem. Afterwards, it will be necessary to study and implement a set of solutions able to minimize the scope within levels deemed acceptable. As already said, ship-owners are solidly in charge of the balance between the investment and the financial losses due to a possible fail.

Unless punctual and specific needs, it is possible to attempt a not excessively coarse approach to complex problems, based on the Pareto[3] principle. This method is aimed to specialize investments in the protection of the "most valuable targets", chosen on the base of the asset's value, from the owner's point of view, in conjunction with the related gain achievable from any hostile actor.

From a technical point of view, priority should be given to actions aimed at preserving business continuity, including those limiting the effects of failures and failures (passive protection) as well as deliberate cyber-attacks. The question to be asked to the company's management is: "which is the impact of a loss or temporary unavailability of data on my business"? And then: "How long lasts the data recovery procedure (if any exists)?", "Is this time frame compatible with my operations?" and "the disaster recovery process has been validated?". Each method has its related cost and its performance: a simple periodical data backup may be sufficient for some companies, while others must choose a real-time backup on geographically distant servers and a hot-swap management of the services.

IT vulnerabilities can generally be limited to minimum level through the continuous application of security updates (the so-called patches) periodically released by major software houses. In the maritime field - and in OT applications - this good practice is unfortunately not always effective as related computer systems cannot be

---

[3] Vilfredo Pareto, 1848-1923, Italian engineer, economist and sociologist. According to the intuitive formulation of its principle, in complex systems about 20% of the causes affect 80% of the effects

updated with adequate frequency (or cannot be updated at all), often due to the limited number of known incidents. Consider, for example, the firmware of a generic machinery's PLC[4]: the manufacturer, that is the design authority, will not be able (except in a few cases) to provide assistance on the process controller, or to incorporate in its logistic management the configuration variants of the PLC. Possibly, it will limit itself to manage the development of the logic only if this is no longer compatible with the new firmware. As a further complication, it will be mandatory to foreseen a five-year-long cycle of obsolescence resolution for the hardware, and decennial cycle for the operating systems, whose operational life cannot cover 30-40 years of the vessel's life. In these occurrences, if a choice exists, it is always convenient to ask whether it is not appropriate to modernize also the SCADA's supervision, which may be one or two generations behind.

Considering the high rate of new technological vulnerabilities discovered, it is customary and good practice to adopt active protection systems (hardware and software), such as antivirus, firewalls, intrusion detection / prevention systems (IDS / IPS), network traffic analysers, etc. Unfortunately, these solutions must be chosen and implemented in the manner and to the extent appropriate to the system to be protected. Otherwise, they may be ineffective or uneconomical and, sometimes, even harmful for system's performance or functionality, especially in the OT domain, where availability is the main requirement.

In order to adequately choice the solutions to be implemented, it would obviously be very useful to have a method, as objective as possible, suitable for measuring the robustness of the IT system. In addition to the obvious technical contribution obtainable from the early design phase, this method would add value to the product increasing its quality. Moreover, in the maritime field it would allow virtuous dynamics in the estimation of a possible insurance premium covering cyber risk.

Despite no software suite has been ever considered as the reference standard, some tools currently on the market could in fact meet this need, as they can perform a complete assessment, with enough quality and objectivity. This software allows to model the target system, to define the perimeter of attack and all possible scenarios, and to perform a systematic series of attacks through the use of a database of known exploits, thus verifying the vulnerability of the target in terms of stress to time and resilience to time. Of particular interest is their capacity to manage *0-days*[5] threats and the *black swan*[6].

From what has been said before, it can be observed that any measurement can be stated as valid only at the time when it has been operated and, therefore, has a degree of reliability decreasing over the time. The robustness of a system cannot ever be the result of a single measurement, however accurate it may be, but must correspond

---

[4] Programmable Logic Controller.

[5] Unknown vulnerability, manageable through systematic simulations of model nodes' flaws, in order to measure its residual robustness and the depth of penetration.

[6] Vulnerability with a very low estimated occurrence rate and a very high magnitude of the damage. They are detectable through a systematic analysis made by the software and can be countered with preventive measures (if convenient) or suitable disaster recovery procedures.

to the output over time of an iterative process. This process includes the following steps: measure of robustness, continuous monitoring of the system, investigation of 0-days, patching, implementation of risk mitigation, new system's modelling according to variants, new measure of robustness and so on.

5. Conclusion

Cyber risk is an increasingly significant aspect of the security management of a corporate that wants to protect its business model and maintain or gain a competitive advantage. Hence, ship-owning companies are nowadays fully involved in the problem and must respond adequately to the challenge, with an investment model that has to be first and foremost effective but, above all, tailored to the specific industrial reality. Furthermore, companies have to be warned about the risk of underestimating their role in the general context of "country system".

The application of simple risk management procedures, supported by "comprehensive" analysis of the problem (in a multi-layered environment), is fundamental in order to define the right investment and to plan an effectively security strategy. As a direct consequence, in the near future of maritime domain it is foreseen the birth of new marketing dynamics based on the robustness of the company computer system. The latter is in fact linked to the guarantee of service continuity (influencing corporate value as well as rate tables, number of customers, etc.) and to the level of cyber risk to which companies are exposed (which, instead, can bias on the insurance premium to be paid to protect the asset).

The changing nature of the threat, finally, requires the adoption of an iterative process that allows a conscious and active management of the problem, restraining the destructive effects of cyber-attacks, especially those potentially affecting national resources.

References

[1] Gronholt-Pedersen, J. (2017, 06 27). Retrieved from www.reuters.com: https://www.reuters.com/article/us-cyber-attack-maersk/maersk-says-global-it-breakdown-caused-by-cyber-attack-idUSKBN19I1NO

[2] IMO. (2015). MSC-FAL.1/Circ. 3 on Guidelines on maritime cyber risk mangement.

[3] Det Norske Veritas. (2016). DNVGL-RP-0496 on Cyber security resilience management for ships and mobile offshore units in operation.

[4] Lloyd's Register. (2016). Cyber-enable ships - A Lloyd's Register guidance note (1ª ed.).

[5] BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, & IUMI. (n.d.). The guidelines on cyber security onboard ships (2.0 ed.).

[6] Neumann, T., Rad, T., & Strauchs, J. (2011). SCADA & PLC vulnerabilities in correctional facilities. DEFCON 19, (p. 15). Las Vegas.