Proceedings of the 19th International Symposium on the Packaging and Transportation of Radioactive Materials
PATRAM 2019
August 4-9, 2019, New Orleans, LA, USA

Paper No. 1439

Bridging the Gap between Cyber and Physical Security

Anna Wikmark
Swedish Nuclear Fuel and Waste Management Co.

Mikael Hammarström
Knowit Secure AB

ABSTRACT

The systems installed to support physical security, or physical protection, are a mixture of servers, clients and products best described as Internet of Things, IoT. This means that they are highly capable products with network features just as any computer. The physical protection systems are designed to keep unauthorized people out and provide authorized access to the areas they are protecting. The purpose of cyber security is basically the same as for the physical protection systems.

The team responsible for the cyber security are typically part of the IT staff, while the systems for physical protection are often installed and maintained by external subcontractors. It shall not be taken for granted that the coordination between these two parties is effective, if even existing. This paper describes the challenges The Swedish Nuclear Fuel and Waste Management Co has experienced bridging the gap between cyber security and physical protection for the Swedish Nuclear Transport System. There are a wide range of issues, from managing to get the cyber security team and the physical protection team working together to the need to evaluate if the manufacturers of physical protection products are taking the cyber security of their products seriously. You pass questions like ”Has there been an improvement since the Mirai botnet almost brought down the Internet by using default credentials in IoT including CCTV cameras?” and at the end you cannot get rid of the worrying ”Have you really found all of the weak spots when it comes to cyber security?”

INTRODUCTION

The Swedish Nuclear Fuel and Waste Management Company, SKB, is owned by the nuclear power companies. They have a statutory duty to deal with the disposal of Swedish nuclear waste and to pay for these operations. SKB is responsible for taking care of the Swedish nuclear waste and for planning of this work funding. SKB has a fully implemented system for dealing with nuclear waste. Since the mid-1980s both the Final Repository for Short-Lived Radioactive Waste (SFR) and Central Interim Storage Facility for Spent Nuclear Fuel (Clab) have been in operation. Safe transport of radioactive waste from the nuclear power plants takes place using the SKB owned INF-3 vessel, M/S Sigrid.

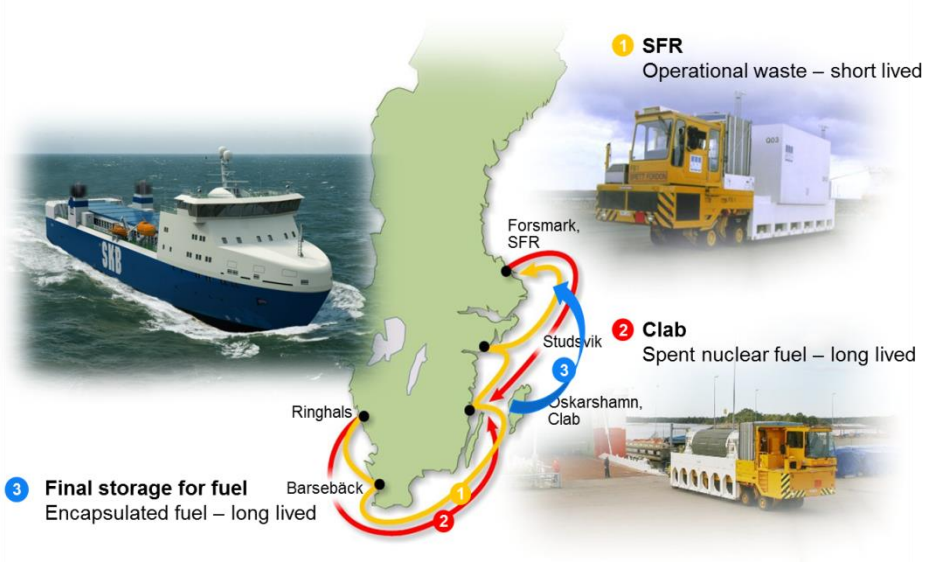

Figure 1 SKB Transport System

SKB, has been transporting irradiated nuclear fuel since the beginning of the 1980s and has experienced the rapidly increased security focus over the years after the 9/11 attack, followed by regulatory requirements on enhanced security. The increased requirement on physical protection was one of the major reasons to the SKB business case for procurement of a new vessel for the maritime transports and when M/S Sigrid was built in 2013, the security and safety abilities were important factors for the vessel design. SKB has gained a lot of experience facing the challenges of developing the security system on board the vessel. The vehicles for road transport of the spent nuclear fuel and operational radioactive waste are also subject to specific safety and security regulations and SKB has learnt that it requires in-depth knowledge of both the regulations as well as a good technical and operational understanding to install and manage an effective nuclear transport security system. The field of cyber security is specifically challenging since the information technology has entered the arena for availability rather than for physical protection reasons.

Definitions

For the SKB work on cyber security and physical protection within its transport system the following definitions have been developed, influenced by the IAEA Safety Glossary [1] and IAEA Nuclear Security Series No. 17 [3].

Physical protection	The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances, their associated transport facilities and crew.
Information Security	Information security includes Cyber security and the aim is to protect information and information carrying systems from illegal access and any other negative influence. The information must be correct at any time and the sharing shall be on a strict need-to-know basis.
Cyber Security	Also known as computer security, a particular aspect of information security that is concerned with computer-based systems, networks and digital systems.

REGULATIONS ON CYBER SECURITY IN PHYSICAL SECURITY SYSTEMS

Requirements on information security are found in legislations, regulations and company policies and procedures and the list of applicable requirements on information security in a physical protection system on and nuclear cargo vessel is long. Unfortunately, the regulations on information security in physical protection systems for nuclear activities are sometimes in conflict with the non-nuclear legislation for shipping [2]. It is therefore an important activity to initially identify all applicable requirements from all legislation areas and evaluate the impact for the concerned system. Examples of identified legislations and regulations that is on the list applicable for the cyber security on the SKB nuclear cargo vessel are

- Regulations on physical protection and security for nuclear facilities issued by the Swedish Radiation Safety Authority, SSM
- Protective Security Act
- Act on Public Video Surveillance
- Data Protection Act including protection of personal data
- Vessel Safety Act
- Act on Maritime Security

IAEA has published a guide on implementing computer security at nuclear facilities [3] and there are also standards that help organisations to build an Information Security Management System, ISMS, to keep information assets secure, for example the ISO/IEC 27000 family and Cyber Security Management System, CSMS, in the standard series IEC 62443. Everyone who install systems in an environment where security and safety are top priority want products that are efficient, robust and

with little or no false alarms. The price is important but not the key choosing factor. A systematic method is needed to ensure that the physical protection systems installed have robust cyber security, provide sufficient flexibility and can be maintained to the right price without lowering the security.

SKB METHOD FOR IMPLEMENTATION OF CYBER SECURITY

Information security consists of both administrative measures, technical security and an effective organisation, see figure 1. The company quality management system should include how security is managed organisational, through work instructions and handling of information. Technical security includes measures for IT systems and infrastructure as well as physical protection for premises and equipment.

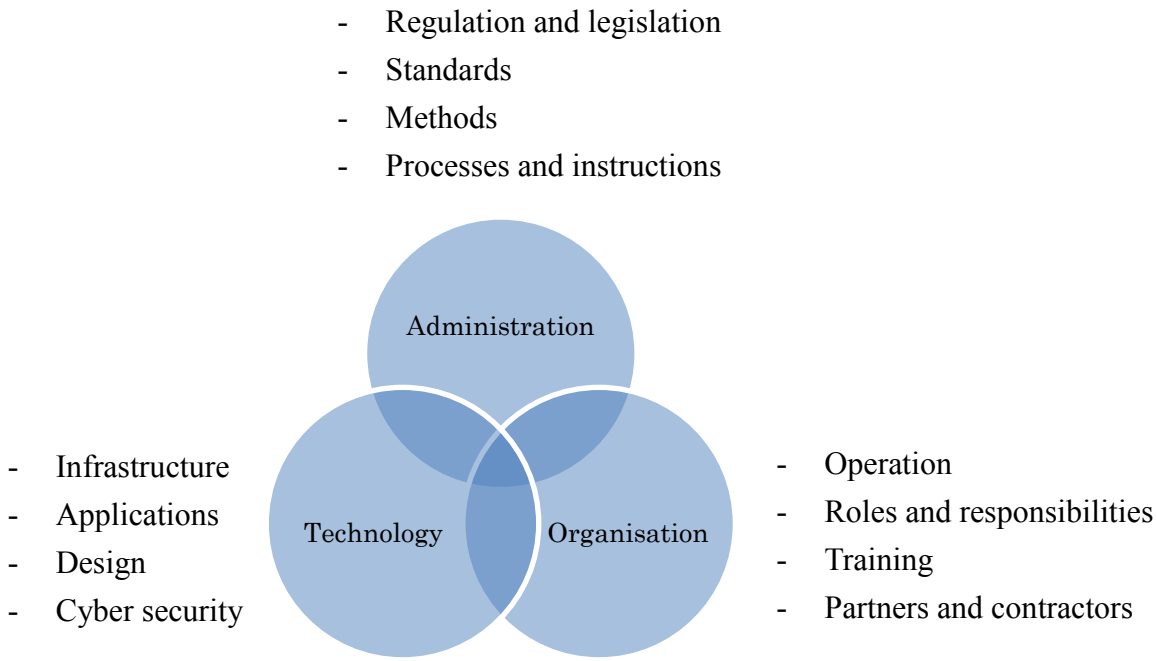

Figure 1: The relation between the fundaments of information security

To assure an effective transport security system, meeting all regulatory requirements on physical protection and information security (including cyber security) without putting any of the safety aspects aside, SKB has established a working method that has been used for both the ship and the vehicles within the transport system for the Swedish nuclear industry. The method is based on the process described in the IAEA NSS No. 13 [4] and is further described in [2]. The work with cyber security has itself followed an established process. The process governs all SKB activities in the area of information security with the purpose to meet regulations, mitigate risks and to protect information and systems carrying information from unauthorised access or other negative influence. The process is linked to the processes for Radiation Safety, Security and Code of Conduct.

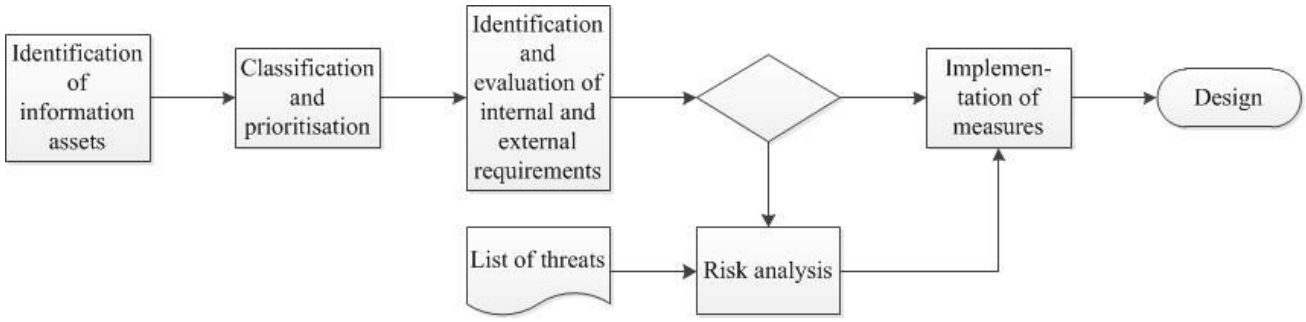

Figure 2: SKB process for implementation of cyber security

PROTECTION OF PHYSICAL PROTECTION SYSTEMS

A common way to protect a security system is by air gapping. This means that the system is physically isolated from other systems that have no functionality in the physical protection. As a way of segmentation this is a good procedure of course but is by no means enough as the only security measure for a physical protection system. It is not uncommon that anti-virus, windows update, and firewalls are turned off.

CHALLENGES DESIGNING A ROBUST CYBER AND PHYSICAL PROTECTION SYSTEM

Designing secure IT systems within the physical protection field can be challenging. Procurement of the systems is done a turn-key solution and is procured as a package with all necessary IT equipment included. For a physical protection system, it is important to maintain control over the infrastructure equipment but many times the supplier of the system cannot guarantee the functionality if key infrastructure equipment come from the organizations ordinary suppliers.

To manage the design and installation without creating an unstable system that no one will take responsibility for, there are a number of challenges to handle. A key to success will be to involve all stakeholder use each parties' strengths in the design and installation of the system. It shall however not be taken for granted that the coordination between the parties is effective, if even existing. The challenge starts there.

Challenge No 1. - Security by design

When designing a physical protection system, cyber security requirements need to be involved early in the design process. It is not uncommon that they are taken into account when it might be too late to correct design flaws. Depending on the project setup there should either be a complete list of requirements of design principles for the security system up front or the security experts can be involved from the start in the design process.

If the aspects of maintenance are not considered already in the design process you might run into trouble. Your server room shall probably not be shared with other administrative systems or it should at least be physically protected within the server room, with access control and Closed-Circuit Television, CCTV. Another aspect that is important to deal with early in the design process is network segmentation and not to forget is the General Data Protection Regulation, GDPR in the physical protection system. There will be personal records in the access control system, CCTV system and probably even in some servers if Active Directory, AD, is used.

Challenge No 2. – Hardware and software asset management

To be able to track unauthorized changes in the system you need to have an inventory to begin with. This is relevant to the hardware, software and also the physical protection hardware. The equipment used in the network infrastructure should also be documented.

The software and firmware on these devices also need to be documented to keep track of new releases and the possibility that they can include useful new features or more importantly updates, if there has been found a security vulnerability.

Secure configuration of the network equipment is important, which leads to the challenge to combine the third-party suppliers with your own need of secure configuration.

Challenge No 3. – Secure configuration

The first questions to ask is “Who should do the configuration of all the equipment?” and “How involved is the physical protection team?”. Let it be an alert signal if only the physical protection team is involved which can result in only basic or no configuration of the hardware in the system.

Most products have a default password. Do not let it be up to an external party to forget or ignore to change it and do not use the same password for all units. Give directions on the settings and configuration to be used. If possible, set the passwords yourself so that the information remains within your organisation.

In the protection system there will be a combination of clients and servers. Do they really need to be a part of the equipment you buy from the security company or could you procure the IT hardware yourself and configure them according to the specification of the software supplier of the security systems? Will this automatically make the warranty process impossible or can it be handled? These are questions to consider and answer and our experience is that the pros are bigger than the cons to be active in this area.

Challenge No 4. – Network security

It is necessary to monitor a physical protection system in order to prevent and detect an intrusion. There are quite a few things to consider when implementing network security in the physical protection system.

- Is the network segmentation done correctly?
- Are all relevant threats identified?

A systematic risk analysis is highly recommended. When doing the risk analysis, you should include a wide range of threats and use the impact the threat has on the physical protection level as a consequence. Consider the threat as a combination of the intentions and capabilities of the threat actor and not only as a probability with a guessed number.

Do not forget to use firewalls where appropriate and use a log server to be able to do log analysis.

Challenge No 5. – Log management

Anyone that wants to know what happens on their network and within the clients and servers, need to implement log management. Use a standalone log server to do this. It is even possible to send log events to the server from some physical protection equipment, like CCTV cameras.

A good advice is to include log management in the procurement requirements of the protection system. A positive side effect will be that the companies that cannot provide it will sometimes forward this to the R&D at their company, which will benefit future customers. Once the log analysis is set up in a secure way, it can really help detecting and mitigating a breach. Do not forget that this should be done by skilled staff!

Challenge No 6. - Procurement

It is not an easy task to procure physical protection systems. There are a lot of different systems on the market and they compete in having new and exciting features. As a customer with high requirements on solid performance and robust cyber security it is hard to make informed decisions. Very few of the suppliers of CCTV cameras and access control equipment give guidance on how they work with secure development of their products. Some of the software developers for CCTV systems claim they work for improved security in their software. Price is always one of the key factors when their customers choose products. There is a way to handle this. First, have cyber security requirements as an integrated part of the procurement requirements. Use the word should instead of shall for the cyber security requirements so that you can include requirements you might know that no systems have. Let the suppliers describe how security is handled in their development process, and how the products are tested for vulnerabilities. Let them also describe how reports from security researchers that find vulnerabilities are handled.

If everyone is asking for at least basic security features and a development process with security on the agenda it will probably make a huge improvement for all end users.

A common problem with IoT products is poor password management. This is a reason that the Mirai botnet [5] could happen. Now some systems force you to change the default password when logging in for the first time but with the companies spending very few resources on security, future botnets will probably happen again.

Challenge No. 7 – Maintenance and patch management

When a protection system is finally installed there are still things to consider. You have to balance the requirements of availability with the aspect of what information and capabilities you give the supplier of the physical protection system. You would probably not give the supplier access to drawings, but many times let them leave the site with the configuration of your protection systems in their laptops.

There could also be a conflict between the need of software updates and the need for availability and the tough change requirements. The process to upgrade could be so steep that its avoided partially or totally.

To keep up with all software related vulnerabilities you need to put in some effort. There are continuously numerous vulnerabilities disclosed and the ones found and not made public are called zero days. The research put in to find vulnerabilities in physical protection software is nowhere near the efforts put in commercial software where there also sometimes are bug bounties involved.

You should also make strong regulations on how USB flash drives are used in the system. If you can you should block all USB ports from using unauthorized USB drives. But there is also a need to implement a secure process for the use of the authorized USB sticks. And do not forget to use dedicated laptops for the teams maintaining the system. Do not let the maintenance be done with their own laptops.

Challenge No. 8 – Shadow IT[1] and the users

So now we are getting close to having a finished system but there are still things to check. Make sure the users do not have administrative privileges. Make use of a local Active Directory server and have the Cyber security team configure it properly. Do not leave the users without guidance. Evaluate shadow IT in your risk analysis for every system. The users are smart and will find ways to work

[1] Shadow IT, also known as Stealth IT and Client IT, are Information Technology (IT) systems built and used within organisations without explicit organizational approval, for example systems specified and deployed by departments other that the IT department (Source Wikipedia 190602).

their way around some of the security controls if they are found to delay or make their work more burdensome. Train the staff and have a dialog with them about the parts where they find that the security is having negative impact on the usability and availability.

CONCLUSIONS

A lot can be done as a customer and a user when it comes to making sure your physical protection systems are well adapted and correctly used for a strong cyber security. The key winning factors are that you are willing to bend existing methods from the physical protection industry and that you involve all relevant parties when designing the security systems. Let's join and work together, not only in bridging the gap but also in the future to close it.

REFERENCES

[1] IAEA Safety Glossary 2007 Edition

[2] How to Handle the Conflict between Safety and Security, A. Wikmark, S. Engqvist, T Bengtsson

[3] Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17

[4] Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13

[5] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/