MAGAL S3
Security, Safety, Site management

17 Altalef Street
Yehud Industrial Zone, Israel 56100
T: 972-3-539-1444 F: 972-3-536-6245
www.magal-s3.com

# New Cyber Frontiers (Antwerp Port Case study)

To many people, the word “cyber” makes them think simply of office computers and websites. But, cyber means much, much more.

Remember the thriller “The Italian Job”? A crime organization, with very some sweet criminals, is committing a huge gold theft. For escaping they take control of traffic lights, trains, communication systems and control centers.
Is that scenario possible only in the movies? Here is a true story from less than a year ago.

A crime organization used to transfer to the port of Antwerp huge cargo of drugs, hidden as bananas from South America. For that purpose, the organization hired a Belgian group of hackers, who cracked the management systems of two piers in the port. These systems manage the transport, storage and shipment of thousands of containers passing through the port each day. Cargo management systems now days include television cameras for automatic container identification and for documentation for insurance purposes; the systems manage loading and unloading queues, perform billing and more.

The hacking enabled the crime organization to locate every container, even before the real client appeared to collect it. When the security breach was exposed, the port installed a firewall. However, the criminals did not give up; they penetrated physically into the port and installed wireless bridges on the operating computers, opening a direct access to the operating system. It took the port about two years to find the reason for the disappearance of containers at the port. In our virtual world, whatever disappears from the management systems - vanishes.

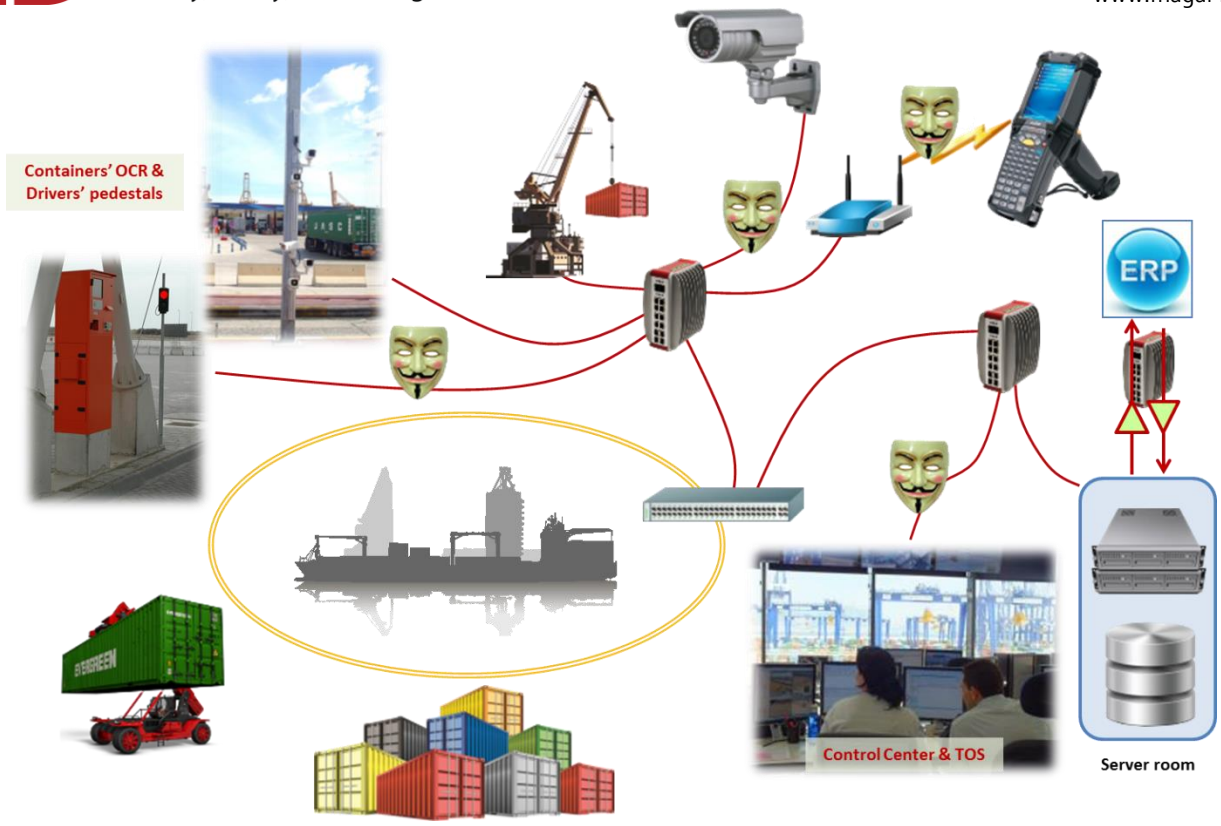
**Typical Architecture of a Cargo Management System**

A port’s cargo management system is assembled with many features, some of them deployed outside, and therefore physically accessible. For example:

- Cameras installed on or near cranes, used to view container identification numbers and document the physical condition of containers (damage control for insurance purposes)
- License plate recognition systems for identifying vehicles at entrance and exit points, as part of cargo’s dispatch mechanism
- Portable wireless terminals for field work
- The Command and Control room – the nerve center of the system
- Interfaces to external systems such as enterprise resource planning, to track employees and contractors, and accounting systems

MAGAL S3
Security, Safety, Site management

17 Altalef Street
Yehud Industrial Zone, Israel 56100
T: 972-3-539-1444 F: 972-3-536-6245
www.magal-s3.com




In most cases, the network relies on fiber optic infrastructure, which in itself seems independent, isolated from the outside word and therefore immune from threat. The reality of course is much more complicated, with much vulnerability to cyber-attack.

**The target: Operational Systems**

Let's take for example a physical security system for a critical site such as a port. Today, rather than take the risk by a brutal penetration through the fence, one can disable the communication between the fence sensors and the control center, or freeze an image of a digital camera (IP), in a way that a guard will be sure that the site is calm and empty. Every beginner hacker can help criminals to penetrate the access control system and issue a "legit" card that would open the main gate.

Physical security networks are not fundamentally different from other operational networks; and thus, it is relatively easy to disrupt the site operation by neutralizing the electrical system, the air condition or by a direct hit of the management system on the site (such as cargo handling at the port). Of course, the most effective attack will be achieved by an integrated operation of cyber-attack combined with physical assault.

The main challenge of protecting operational networks is the lack of awareness. Until a few years ago, operational networks were simple, connected by basic wiring, and if they were networked, it was by special protocols and disconnected from the outside world. Today, nearly everything is networked, connected to digital controllers and managed by remote computers and smartphones.

Operating networks are vulnerable for several other reasons. Starting with the layout - when sensors are located outside, they may be accessible to "enemies"; it is relatively easy to disconnect an IP camera on the fence or in a safe city for a while and physically connect to the network. In addition, contrary to the IT world, most security players (consultants, manufacturers, and integrators), have limited skills in the

17 Altalef Street
Yehud Industrial Zone, Israel 56100
T: 972-3-539-1444 F: 972-3-536-6245
www.magal-s3.com

field of cyber-security. And last - the security products market is fragmented to thousands of small manufacturers, which makes it difficult to develop appropriate standards.

**The opportunity**

Nevertheless, operational networks have a number of characteristics that enable to secure them with reasonable effort, mainly because they are simple and relatively static. The network subscribers are relatively fixed; the network protocols are pretty much defined; the communication topology is fixed (Camera No. 17 speaks through a switch number 3 to the PC); external communication is well known. Therefore, tailored solution to these networks provide adequate and affordable cyber security

**Holistic security is needed**

Today it's clear that cyber threats are everywhere. A common mistake is using a firewall to protect the access points, and assume that this can provide sufficient protection. Now days it is clear that threats can start from the inside – through a USB flash disk, a software update, a virus in an IP camera, a technician opening WiFi channel for maintenance, a connection to a cell phone, a virus from the supply chain, etc.

To deal with attacks on operational networks, Cyberseal of the Magal group developed a network device which identifies abnormal behavior. This third layer switch hosts security mechanisms for checking abnormal network behavior (even at lower levels than layer 3). The switch can detect cases such as changes in cable length or tapping to communication lines - fiber-based or copper; physical disconnecting of network segments; changes of terminal equipment addresses (MAC, IP); changes of protocols; malicious IP packets; changes in communication flow direction and even a sudden change in the bandwidth or the power consumption of PoE users .

Additionally, when it comes to operating networks, it is necessary to have an integrated management system for physical security and cyber-security. Therefore, the complete solution of Magal includes the Fortis$^{4G}$ system which is actually an integrated SIEM system with PSIM - Physical Security Information Management. The system can manage all other cyber security elements such as the Firewall, server agents; workstations, and special equipment to monitor cellular communication. In addition it managed the physical security solution.

Beyond collecting and presenting information, the central management system allows immediate response automatically or semi-manually to cyber events such as disconnecting elements from the network or disconnection power to a problematic component.