MARITIME REPORTER AND ENGINEERING NEWS

Tel 352 692 5493
Fax 352 692 5494

Dennis L. Bryant
Bryant's Maritime Consulting
4845 SW 91st Way
Gainesville, FL 32608-8135

August 2017

Balancing Efficiency and Security

Dennis L. Bryant

We live and operate in a complex society. That society would be impossible without modern computers and other information technologies. Those technologies have largely been developed piecemeal to address particular issues, and for the most part they have generally achieved their particular goals. Maximum efficiency is gained when multiple technologies are joined to coordinate their work. Computers get smaller and faster, with ever-growing memory. Joining computers together allowed for creation of the internet. Placing small efficient computers and related technologies on satellites allowed for establishment of the global positioning system and wireless internet connections such as Inmarsat. Putting computers and satellite communications equipment on ships allowed the collection of myriad data and rapid ship-shore communications worldwide. It also allowed for installation of such technologies as AIS and ECDIS. All of these and other developments have fundamentally changed the maritime industry, generally for the better.

But there have been downsides. The technology requires an increasing level of training for the human operators. This has proven especially difficult for the maritime industry where crew turnover is high. There are multiple manufacturers of the same equipment, such as ECDIS, and each takes a different approach to providing the desired service. As a result, the training received on a piece of technology on one ship may be largely useless on another ship. There is no standard method for integrating all the technologies on a ship so as to work together. Multiple individuals on each ship have access to the technologies. These individuals have widely varying levels of training and experience with those technologies.

A few examples

The Aegis cruiser *USS Yorktown* (CG-48) was commissioned in 1984. For twenty years, until its decommissioning in 2004, it was one of the most powerful and sophisticated warships in the US Navy. The continuing quest for sophistication, though, almost did it in. In 1996, the *Yorktown* was selected to be the testbed for Navy's Smart Ship program. The cruiser was heavily computerized, with an integrated control center on the bridge and other computers monitoring all shipboard activity. Unfortunately, crew training and system segregation were neglected. The computers were all tied together into one network. On September 21, 1997, the cruiser was operating solo about 100 miles off Cape Charles, Virginia. A crewmember in the

E-mail dennis.l.bryant@gmail.com
Internet http://brymar-consulting.com/

engineering department, while ordering supplies, mistakenly entered a zero as the divisor in a mathematical equation. Dividing anything by zero results in an infinite number. The computer crashed. That caused all the other computers on the ship to crash. The ship totally shut down. Not only did the engines not work, neither did the radios. The ship could not send an SOS or notify its headquarters of the dilemma. It took approximately 2 and ½ hours to get the radios back on line so that a message could be sent to headquarters in Norfolk. Assistance was dispatched and the cruiser was escorted back to port. The Navy immediately declared the whole incident secret. It was not until some months later that a report of the computer crash appeared in a technical publication. The Navy then acknowledged the incident, stating that the *Yorktown* had experienced "an engineering local area network casualty." Needless to say, the Smart Ship program was extensively revised.

On the night of 10 June 1995, the cruise ship Royal Majesty grounded on Rose and Crown Shoal just east of Nantucket Island. The ship was equipped with all the latest electronic navigation equipment, including an integrated bridge system. The GPS receiver was located in the chart room, which was seldom visited. GPS signals from that receiver were transmitted to repeaters on the bridge and to the integrated system. Unfortunately, the antenna wire connecting the GPS antenna to the GPS receiver had come loose. The GPS receiver defaulted to its dead reckoning mode. A flashing red light on the GPS receiver clearly indicated this situation, but the repeaters on the bridge and on the integrated system had no such warning signal. The integrated system showed that the ship was on its planned course from Bermuda to Boston. The current, though, had carried the ship west into shoal water. The navigation team on the bridge had gotten so comfortable with the process that they relied solely on the integrated system, not checking the radar, the fathometer, or even paying attention to the buoys and the shore lights until the grounding.

In June 2017, someone or some group (suspicion has fallen on the Russian government) slipped some malware into an update to a software system utilized by the Ukrainian electrical grid. That malware not only shut down the national grid, it also hobbled the remaining portion of the Chernobyl nuclear plant. It then migrated to computer systems worldwide. Among those incurring this collateral damage were: Rosneft (the largest Russian oil company, largely owned by the Russian government - touché); a major international law firm; a multinational advertising and public relations company; and A.P. Moller-Maersk (the world's largest shipping company). Sadly, this malware attack was largely preventable. One of the security vulnerabilities exploited by the malware to infect the various computer systems had been identified months previously. Patches had been issued by Microsoft and various computer security companies. It appears that at least some of the affected entities neglected to fully install and activate the available patches.

The threat

Bad actors infiltrate computer systems for a variety of reasons and utilize a variety of techniques. Sometimes, these individuals or groups want to steal the data. Sometimes they want to hold the data for money, utilizing so-called ransomware. Sometimes they are malicious and

just want to destroy data. And sometimes, as in the most recent incident, they lose control of the malware and it impacts unintended third parties.

Malware can be hidden in some other company's software that is then downloaded into a computer of the intended target, as happened initially in the June 2017 incident. Malware can also be hidden in a file that gets uploaded into a computer system. This is a common technique. The file is usually sent to someone with access to the computer system in an innocent-looking email, often appearing to be from a friend or co-worker. There are generally indications that something is amiss (e.g., the email address is unusual; the subject of the email is odd; the URL of the link suspicious; etc.). All it takes is one unsuspecting individual to accept and open the email or upload from an infected memory stick to corrupt the entire computer system with the malware.

Efficiency and cybersecurity

Companies must adopt a robust comprehensive cybersecurity system, keep it up-to-date, and continually train their staff regarding the importance of cybersecurity. The threat evolves rapidly. Entities cannot assume that because they updated their system six months ago it is still effective against current threats. They cannot assume that only the company's main computer needs to be kept current. They cannot assume that because they are small fish, they will be ignored. As the June 2017 incident demonstrated, many of the computer systems that were infected were not intended targets. Some malware, once released, will attack any computer in any computer system that is unprotected. Don't be collateral damage.

There is a balance in our modern world between efficiency and security – you can't have one without the other. Don't turn off your computers and other electronic devices, but don't assume that they will always do exactly what you and only you want. You don't leave your car unlocked, so why would you leave your IT system unlocked?