KANE RUSSELL COLEMAN LOGAN

One Mission. Your Mission.

International Ports Back on Track after Global Cyber Attack

News / July 13, 2017 / Ryan Cantu

After a major cyber attack wreaked havoc on companies and governments worldwide in late June, international companies like A.P. Moler-Maersk have brought their IT systems back online. Maersk's Asia Pacific chief executive Robbert van Trooijen has confirmed that all of Maersk's affected ports were back to releasing cargo and that bookings have rebounded.

The so-called "Petya" attack, which was originally targeted at Ukrainian businesses and government agencies, spread globally and ultimately affected international companies like Maersk. The attack did not affect the physical loading of goods but instead disrupted data-driven technologies such as arrival notices and customs clearance, which caused congestion at ports in the United States, India, Spain, and the Netherlands. Maersk in particular was forced to suspend its main platforms from taking orders for six days. Fortunately, Maersk was able to work with its vessel-sharing partner Mediterranean Shipping Company (MSC) and other suppliers and subsidiaries to avoid serious disruptions by diverting several vessels to terminals that were unaffected by the attack.

Though the attack's reach was broad, affecting everything from individual bank customers in Ukraine to hospitals in Pennsylvania, the attack on Maersk had a significant impact on international commerce because this company handles one in seven containers shipped globally, making it a market leader in an industry that still sees 90% of global commerce transported by sea.

Unlike other recent attacks that have specifically targeted businesses for financial gain, the recent ransomware attack may have been political in nature, first targeted at Ukrainian governmental and business organizations on the day before the anniversary of Ukraine's break from the Soviet Union before spreading worldwide. Additionally, sources believe that the specific ransomware was adopted from National Security Agency technology that hackers stole from that agency this April.

The geopolitical origins and nature of the attack raise the question of whether there are limits to what companies can do internally to prevent future attacks. Van Trooijen stated that Maersk had already been in a "strong position" with its cyber security, adding that "there was nothing in terms of patches that we missed." Van Trooijen does not believe that Maersk was intentionally targeted by the attack. Thus, the prospect of future attacks highlights the importance of stronger efforts by not only individual companies but also by key governmental agencies. "The N.S.A. needs to take a leadership role in working closely with security and operating system platform vendors such as Apple and Microsoft to address the plague that they've unleased," said Golan Ben-Oni, the global chief information officer at IDT.

In the meantime, companies can help minimize the impact of future attacks by implementing contingency plans such as the partnerships between Maersk and its partners that helped keep business moving even when several of Maersk's terminals were disabled.