OUTSOURCE

VOLUME 5, ISSUE 6 JULY 2017

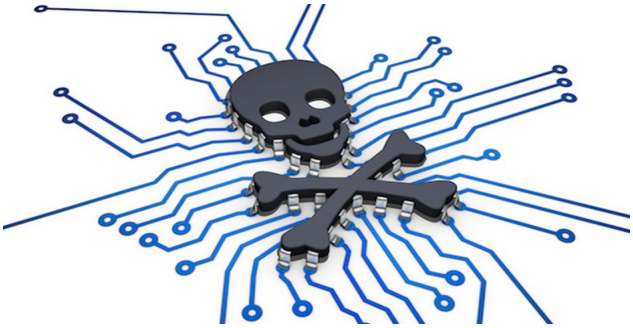
THE SOURCE

China-based cyberattack hits logistics operators, shippers

By: William B. Cassidy, Senior Editor 7/18/2017

Inside this issue

Cover Story:
CYBER SECURITY: Supply Chains in Peril



A sophisticated computer attack launched from China stole financial records, customer data and shipment manifests from as many as seven shipping and logistics companies, using handheld scanners infected with malicious software to crack through corporate security systems.

The first cyberattack known to specifically target global shipping companies raises concerns about the security of supply chain information management systems, especially when a plethora of new peripheral devices are being plugged into enterprise-wide computing systems.

"We're moving into a new era of threat factors," said Carl Wright, general manager of security firm TrapX, which discovered the malware when testing a customer's security system. "Over the last two years, there's been a tremendous amount of profit from cyberattacks." This is the first enterprise-scale attack on supply chains Wright and TrapX have seen, he said. "We've recognized the risk, but heard more of things on the consumer level, like malware-infected phones," he said. "This is the first time I've seen something like this." TrapX and the victims of the attack have not released estimates of the breadth or economic impact of the attacks. But the threat is clear. In addition to specific information, the attackers gained "complete situational visibility" into logistics operations and shipper information.

The attack, dubbed "Zombie Zero" by TrapX, which released a report on the attack, underscores the growing security risks faced by shippers and their logistics and transportation partners in a wireless, mobile world where technology changes almost constantly. Zombie Zero involved a particularly nasty type of polymorphic "advanced persistent malware" that adapted when it detected firewalls and found other routes to the data it was programmed to capture. The software sent that captured information back to a database in China.

The names of the logistics companies targeted in the attack have not been released, but they all purchased handheld scanners from a Chinese supplier, Wright said. Those scanners functioned as a Trojan Horse, with malware embedded in their Windows XP operating systems. Once the handheld scanners were connected to the logistics operator's wireless network, the malware activated and began to attack and compromise servers with the word "finance" in their host name. "They were pretty much able to get any data they wanted," Wright said. In the next phase of the attack, the malware uploaded a "weaponized payload" that established a stealth "command and control" network linked to a network in China. Not only were the attackers able to collect data, they were able to view and manipulate data on the servers as well.

China-based Cyberattack Hits Logistics Operators, Shippers

(Cont'd from page 1)

The attack was discovered two months after the scanners were initially deployed, he said, when a logistics company asked TrapX to demonstrate its security solution, based on a "grid" of so-called high-tech honey pots designed to attract and detect malware and hackers. "Within a few minutes, we detected these communications and the attacks their existing technology wasn't detecting," Wright said. "Within 90 minutes, we had an anatomy of the attack. We could see where the network was communicating out to the other network in China."

Tracing sales of the handheld scanners, TrapX eventually identified a total of seven logistics operators that moved goods by land, sea and air and one manufacturer that were attacked. The attackers, and their ultimate motive, have not been identified. The scanned data — which included the origins, destination and value of many shipments — was sent to a Chinese "botnet" or network of connected Internet-based programs that terminated at the Lanxiang Vocational School, an institution already accused of involvement in cyberattacks on Google. The manufacturer of the handheld scanners is located close to the Lanxiang Vocational School, TrapX said. The malware was embedded not only in many — though not all — of the company's handheld scanners but was downloadable through its online support website as well.

"It was a very sophisticated attack, more like we would see from a nation state than a crime syndicate," Wright said. "It's hard to speculate about the total motivation." The investigation into the attack is ongoing, he said. TrapX published a report on the attack last week and will publish updated information as the investigation progresses.

Shippers are well aware of emerging threats posed by cyberattacks, especially after the massive online theft of customer information from retailer Target earlier this year. Wright urges them to consider more dynamic and adaptive modes of defense. "Enterprises have been executing the 'defense-in-depth,' a layered strategy, since the early 2000s, and that hasn't been working as well in the last several years," Wright said. That's because the sophistication of data centers and the "bad actors" have both increased. "This supply chain attack is a good example of things to come," Wright said.

PETYA MALWARE

Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting.

Blinded by Cyberattack, Shipping Giant Maersk Slowly Restarts Operations

By Costas Paris June 30, 2017

A.P. Moeller-Maersk, the world's biggest containership operator, is still struggling to restore its global computer network after a major cyberattack this week forced the company to rely on phone calls and texts to keep operations going. "I was in a meeting when it happened," Chief Operating Officer Vincent Clerc said in an interview from the company's headquarters in Copenhagen. "Screens went blank, the whole network was hit in a few minutes. We were surprised because you don't expect something like this to happen."

Maersk suffered computer outages at its APM Terminals at ports in the U.S., Europe and India. It stopped taking new cargo for almost three days and is still working to restore basic communications like email. Containers piled up at ports because they couldn't be loaded on trucks, trains or other ships as there was no access to end-user destination data. "In Los Angeles containers were unloaded, but it was hard to operate the gate and forward them to customers," Mr. Clerc said.

APM Terminals in New Jersey and Los Angeles started delivering imports Friday (3 days after the attack), though neither site is yet accepting containers loaded for export. APM's Elizabeth, N.J., facility is its largest on the East Coast and typically processes about 4,500 containers a day, according to Giovanni Antonuccio, the terminal's manager of client services. APM facilities in Mumbai, Buenos Aires and other foreign ports are also back in operation, though the Maasvlakte II terminal in the Netherlands, one of two APM facilities in Rotterdam, hasn't yet reopened. "We are making progress in taking new orders since yesterday and expect to return to some kind of normalcy on Monday," Mr. Clerc said.

Once Maersk realized it was hit by a cyberattack it shut down its entire network to protect its applications from being infected. "We didn't kick in the backup system because we feared it would be infected as well," Mr. Clerc said. Instead the company resorted to a mostly manual system and used mobile and satellite phones to communicate with ships, terminals and clients.

Security experts said that while the virus appeared to be a variant of "ransomware" --dubbed Petya, the cyber-attack appears to have been designed to cause disruption rather than make money. The virus spreads quickly from system to system, locking data and rendering computers inoperable.

TRIVIA QUESTIONS

1) **The wings of some planes are bent to decrease drag. These features are called?**
   A. Ailerons **B.** Aircurves **C.** Drag Resistors **D.** Air Highs

2) **A plane's "Black Box" is not really black but….?**
   A. Red **B.** Yellow **C.** Orange **D.** Blue

3) **The rise of the bicycle during the Victorian period resulted in a fear of what?**
   A. Bicycle Foot **B.** Bicycle Face **C.** Bicycle Leg

4) **Bicycles were formerly called what?**
   A. Velocipedes **B.** Bicipedes **C.** Cyclemobiles **D.** Foot Pumpers

5) **The rise of the railroad established which?**
   A. Taxi Cabs **B.** Standardized Time Zones **C.** Railroad Stations becoming Social Parlors

6) **Which INCOTERM is used when the shipper is responsible to bring the shipment to the destination port?**
   A. FOB (Free On Board) B. FAS (Free Alongside) C. CFR (Cost & Freight) D. FCA (Free Carrier)

Answers Later In The Newsletter

FUEL REPORT

U.S. On-Highway Diesel Fuel Prices* (dollars per gallon) http://www.eia.gov/petroleum/gasdiesel/

	6/26/17	7/03/17	7/10/17	Change from week ago	Change from year ago
U.S. National Average	$2.465	$2.472	$2.481	↑ 0.009	↑ 0.067

Definition of Conservation **(www.businessdictionary.com)**
Usage, improvement, and protection of human and natural resources in a wise manner, ensuring derivation of their highest economic and social benefits on a continuing or long-term basis. Conservation is achieved through alternative technologies, recycling, and reduction in waste and spoilage, and (unlike preservation) implies consumption of the conserved resources.

"Leaders don't make excuses—-they make improvements."

Marina Barragan, Desert Mirage High School student, testifying during an EPA hearing on setting a more ozone pollution standard.

COSCO and OOCL in Planned US $6.3B Merger by ASC Staff on Jul 11, 2017

Merged shipping lines COSCO and OOCL will be third largest in the world and spur further consolidation in global shipping. The Chinese shipping giant filed papers with the Hong Kong Stock Exchange announcing its intention to buy a 90.1% majority stake in Orient Overseas Container Lines' (OOCL) parent company Orient Overseas International Limited (OOIL). The Shanghai Port Group would buy the remaining 9.9% of shares at a 37.8% premium.

While OOCL's shareholders appear ready to accept the deal, it still needs to clear regulatory approvals in China, the U.S. and the European Union. If those approvals are given, COSCO-OOCL will become the third largest shipping company in the world (Maersk Line and MSC are the largest and second-largest), and the second-largest shipping line serving the United States from Asia. The new company would control 11.6% of global container capacity, although OOCL will continue to operate as an independent brand, according to Joc.com.

COSCO's purchase of OOCL is not just another deal, however, it should have European shipping giants Maersk and MSC worried. Splash 24/7 reports that the shipping line intends to eventually overcome Maersk Line as the world's largest container line. There are reports that once the OOCL acquisition is finalized, COSCO may set its sights on acquiring French line CMA CGM, which controls 11.2% of the shipping market. That would make COSCO-OOCL-CMA CGM the largest shipping group by a huge margin.

The deal is being seen by some as the beginning of a wider shift in the shipping industry, away from a shippers' market and into a carriers' market. If all pending deals are approved in the next year, by July 2018, 61% of world container capacity will be moved by just five ocean carriers.

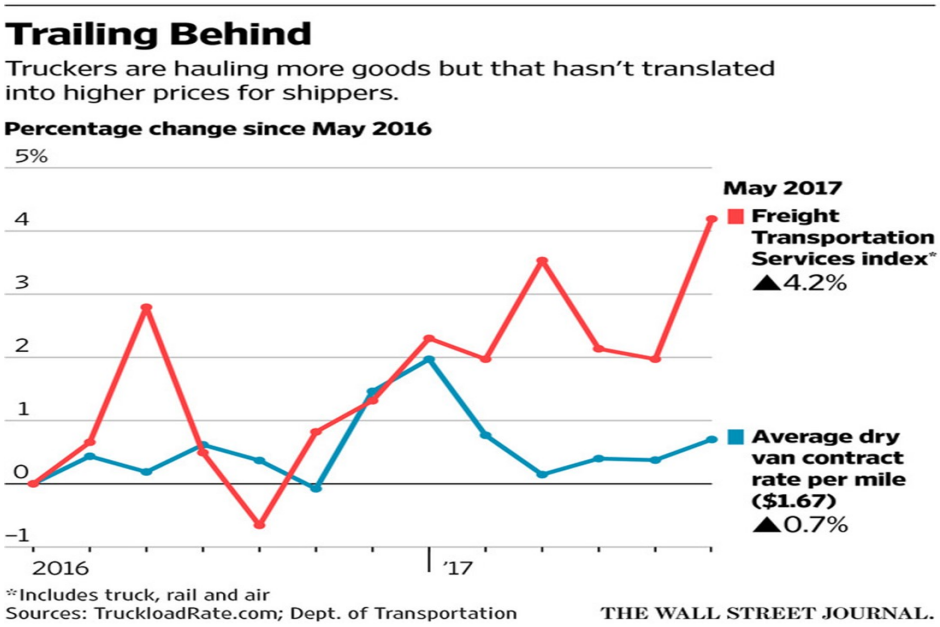
Kuehne raises Hapag-Lloyd Stake James Baker July 17, 2017

Germany's Klaus-Michael Kuehne has increased his holding in Hapag-Lloyd following travel company Tui's exit from the Hamburg-based container line. Mr Kuehne, who owns logistics giant Kuehne + Nagel, has raised his stake in Hapag-Lloyd from 14.1% to 17.6% in a vote of confidence for the carrier. On Tuesday, Tui, which has had an investment in Hapag-Lloyd since it bought the company in 1998, sold its remaining stake to focus on its cruise activities. Speaking to Reuters, Kuehne Holdings executive chairman Karl Gernandt said: "The ongoing shipping industry consolidation offers Hapag-Lloyd new growth perspectives and strengthens its positions among the most important shipping companies across the world."

Kuehne Holdings has been an investor in Hapag-Lloyd since the Hamburg-based rescue mission for the company was launched in 2008 in an effort to keep it out of the hands of NOL. Hapag-Lloyd's new ownership structure is: CSAV 22.6%, City of Hamburg 14.9%, Kuehne Holdings 17.6%, Qatar Holdings 14.4%, Saudi Arabia's Public Investment Fund 10.1%. The remaining shares are in a free float.

Dramatic Drop in Containers Lost at Sea By The Maritime Executive 2017-07-10

The World Shipping Council (WSC) estimates that the average number of containers lost each year has dropped since 2014 by 48 %. Based on the most recent survey results, an average of 568 containers are lost at sea each year, not including catastrophic events. If catastrophic events are included, that average more than doubles to 1,582. In 2014, these figures were 733 containers and 2,683 containers respectively. The larger number of losses in 2014 was due primarily to the complete loss in 2013 of the *MOL Comfort* in the Indian Ocean and all of the 4,293 containers on board and, in 2011, the grounding and loss of the *M/V Rena* off New Zealand, which resulted in a loss overboard of roughly 900 containers. WSC data consistently demonstrates that container losses in any particular year can vary quite substantially based on differences in weather and other unusual events. The data also consistently shows that the majority of containers lost at sea result from catastrophic events. For example, in 2013, there was a total loss of 5,578 containers – 77 percent of which occurred with the sinking of the *MOL Comfort* in the Indian Ocean. In 2015 the total loss of vessel *El Faro* occurred and all containers were lost. This event alone accounted for almost 43 percent of the total containers lost into the sea in 2015. In 2016, the international liner shipping industry transported approximately 130 million containers packed with cargo, with an estimated value of more than $4 trillion.



Answers to Trivia

ArcBest Announces Space Based Minimum Charges for LTL Shipments July 06, 2017

ArcBest announced it will apply space-based cubic minimum charges for less-than-truckload shipments, effective Aug. 1. The Arkansas-based company, parent of ABF Freight and Panther Premium Logistics, said the minimum charges better reflect recent freight shipping trends, including the growth and shift toward bulkier shipments across the supply chain. Many shipping and logistics solutions also now include unique requirements, according to ArcBest.

"The logistics industry continues to change rapidly," said Judy McReynolds, ArcBest chairman, president, and CEO. "We believe this initiative is the natural step for us to take now to ensure that the value we provide is appropriately reflected in the compensation we receive for our shipping and logistics services. We view this as a logical complement to the current weight-based pricing common in the LTL industry."

Because of the rise of internet-based commerce, light weight but bulky shipments are becoming more common for carriers. These shipments take up a lot of space but don't weigh much, which is increasing the handling costs of the shipments for LTL carriers like ArcBest, according to a Journal of Commerce report. While this could increase costs for shippers, it may also encourage smarter packaging. A new process will require customers to provide freight dimensions or have ArcBest calculate it for them, to determine applicable cubic minimum charges that will supplement weight-based metrics when appropriate. ArcBest already has dimensional data on more than 90% of the freight shipped through its asset-based network, according to the company.

To further capture shipment dimensions and validate shipment dimensions provided by customers, ArcBest will install static dimensioners at the majority of its distribution centers, expected to be in place by Aug. 1.

Hyperloop One Completes 'Breakthrough' Test in Nevada Desert July 19, 2017 by Lewis King

http://aircargoworld.com/hyperloop-one-completes-breakthrough-test-in-nevada-desert/

In the November issue of Outsource's newsletter "THE SOURCE" was an article on the Hyperloop project, (Outsource provided transport services between Cambridge MA and the Nevada desert for a portion of the project), appeared. The link above is a follow-up illustrating the advancement of this innovative freight movement project.

Top 25 Cargo Airlines 7/13/07

The annual World Air Transport Statistics report from Iata showed that in freight tonne km (FTK) terms, FedEx was the busiest airline in the world last year with scheduled traffic totalling 15.7bn FTK on the back of a slight 0.6% year-on-year decline in demand.

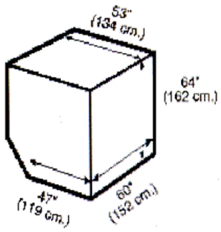
	Scheduled FTK (m)	Ranking +/-	2016	Y-o-Y %	2015
1	Federal Express	0	15,712	-0.6	15,799
2	Emirates	0	12,270	0.9	12,157
3	United Parcel Service	0	11,264	4.2	10,807
4	Cathay Pacific Airways	0	9,947	0.1	9,935
5	Qatar Airways	+1	9,221	20.4	7,660
6	Korean Air	-1	7,666	-1.2	7,761
7	Lufthansa (1)	0	7,384	7.2	6,888
8	Cargolux	0	6,878	9.0	6,309
9	Singapore Airlines	0	6,345	4.3	6,083
10	Air China	0	6,089	6.5	5,718
11	China Southern Airlines (1)	0	5,939	10.9	5,355
12	China Airlines	0	5,273	-1.3	5,343
13	AirBridgeCargo Airlines	+3	4,914	20.8	4,069
14	China Eastern Airlines (1)	-1	4,561	0.4	4,542
15	Etihad Airways	-1	4,481	1.8	4,400
16	All Nippon Airways(1)	+2	4,315	12.4	3,840
17	Polar Air Cargo	-2	4,211	0.6	4,186
18	British Airways (1)	-1	4,117	1.5	4,055
19	Asiana Airlines	0	3,813	6.1	3,595
20	Turkish Airlines	n/a	3,640	n/a	n/a
21	KLM (1)	0	3,564	-0.1	3,567
22	United Airlines	+1	3,534	10.2	3,206
23	EVA Air	-3	3,480	-7.4	3,757
24	Air France (1)	-2	3,419	0.1	3,416
25	LATAM Airlines Group (1)	n/a	3,278	n/a	n/a
	Total		155,315	4.1	149,146

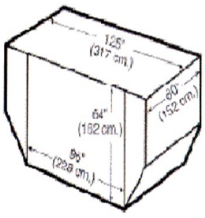
Source: IATA

Notes: (1) Additional notes regarding coverage; see IATA WATS report

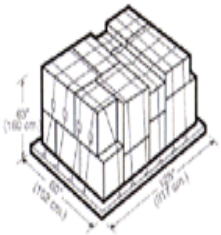
(some) Air Container Dimensions

LD-2 (Equivalent to IATA Type 8D)
Internal Capacity: 120 cu ft/3 cbm
External Dimensions:
47" L x 60" W x 64" H
Maximum Gross Weight:
2,700 lb/1,225 kg

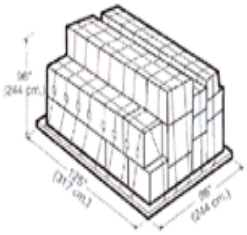




LD-8
(Equivalent to IATA Type 6A)
Internal Capacity: 243 cu ft/6.9 cbm
External Dimensions:
96" L x 60" W x 64" H Contoured
Maximum Gross Weight:
5,400 lb/2,450 kg

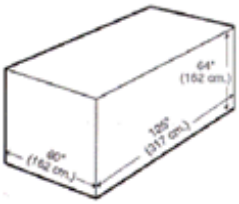


P9A Lower Deck Pallet
(Equivalent to IATA Type 6)
External Displacement: 242 cu ft / 6.9 cbm
External Dimensions:
125" L x 60" W x 63" H
Maximum Gross Weight:
7,000 lb/3,175 kg

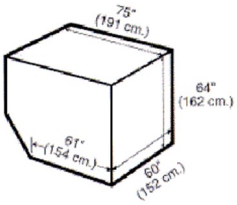


Main Deck Pallet
(Equivalent to IATA Type 2)
External Displacement: 606 cu ft / 17.16 cbm
External Dimensions:
125" L x 60" W x 63"
Maximum Gross Weight:
15,000 lb/6,804 kg

LD-11 (Equivalent to IATA Type 6)
Internal Capacity: 242 cu ft / 6.9 cbm
External Dimensions:
125" L x 60" W x 64" H Contoured
Maximum Gross Weight:
7,000 lbs/3,176 kg



LD-3 (Equivalent to IATA Type 8)
Internal Capacity: 150 cu ft / 4 cbm
External Dimensions:
61" L x 60" W x 64" H Contoured
Maximum Gross Weight:
3,500 lb/1,588 kg



INFRASTRUCTURE

Connecticut's Fiscal Woes Spell Bad News for Road, Rail Renewal

Connecticut's roads, bridges and rail projects may face hazards ahead after the state failed to pass a budget—and close a two-year deficit of $5.1 billion—lawmakers are now taking aim at infrastructure projects. Both Republicans and Democrats in the House proposed capping transportation bonds at $700 million for the current fiscal year, well below the $1.3 billion the Connecticut Transportation Department wanted. James Redeker, commissioner of the Transportation Department, said a $700 million cap on new bonds could result in delays for several federally funded projects, and others would be canceled.

Connecticut's transportation options are already looking bleak. Its special transportation fund, which pays for debt service on transportation-related bonds and operations for the Transportation Department, is projected to be insolvent in three years, according to Gov. Daniel Malloy's budget office. Budget cuts proposed by House Democrats and Republicans could speed up that insolvency, industry experts said. The aging condition of the state's transportation system comes at a price. The state estimates that drivers spend up to 40 hours a year stuck in traffic at the cost of $1.6 billion in lost time and fuel, and $2.6 billion in operating and fuel costs and accidents.

U.S. Seaports, Private-Sector Partners Plan to Invest $46 Billion by 2017 in Port Infrastructure (as per the American Association of Port Authorities www.aapa-ports.org) Lack of parallel state & federal investment in intermodal connections hamper job creation, efficiency benefits

In a recently completed survey that the American Association of Port Authorities (AAPA) initiated, U.S. seaport agencies and their private-sector partners plan to invest a combined $46 billion over the next five years in wide-ranging capital improvements to their marine operations and other port properties. While port authorities and their business partners are making major investments into port facilities, studies show the intermodal links—such as roads, bridges, tunnels and federal navigation channels—to access these facilities get scant attention by state and federal agencies responsible for their upkeep, resulting in traffic bottlenecks that increase product costs and hamper job growth.To help remedy these problems, AAPA continues to advocate for a national freight infrastructure strategy and for the U.S. Congress to quickly pass a reauthorized multi-year transportation bill that targets federal dollars toward economically strategic freight transportation infrastructure of national and regional significance.

"Infrastructure investments in America's ports and their intermodal connections – both on the land and waterside – are in our nation's best interest because they provide opportunities to bolster our economic and employment recovery, help sustain long term prosperity, and pay annual dividends through the generation of more than $200 billion in federal, state and local tax revenue and more than $22 billion in Customs duties," said Kurt Nagle, AAPA president and CEO. "From a jobs standpoint, America's seaports support the employment of more than 13 million U.S. workers and create 15,000 domestic jobs for every $1 billion in manufactured goods that U.S. businesses export."

According to economist John C. Martin, Ph.D., president of Lancaster, Pa.-based Martin Associates, U.S. Bureau of Economic Analysis formulas show that investing $46 billion in infrastructure at U.S. ports creates more than 500,000 direct, indirect and induced domestic jobs, accounting for more than 1 billion person-hours of work. "Those are really significant job numbers," emphasized Dr. Martin. "From a dollars-and-cents perspective, it's hard to over-emphasize the value of investing in ports, particularly when you factor in how much these investments help lower the cost of imports and make our exports more competitive overseas." Mr. Nagle added that, despite substantial investments by port authorities and their private-sector business partners, inadequate infrastructure connecting ports to landside transportation networks and water-side shipping lanes often creates bottlenecks, resulting in congestion, productivity losses and a global economic disadvantage for America. "These congestion issues and productivity losses have the potential to stymie America's ability to compete internationally and to create and sustain jobs," he said.

As recently as 2005, the World Economic Forum ranked the U.S. number one in infrastructure economic competitiveness. Today, the U.S. is ranked 16th, while neighboring Canada is ranked 11th and fast-developing China has risen to 44th. This change in ranking is due mostly to the fact that the U.S. spends only 1.7 percent of its gross domestic product on transportation infrastructure while Canada spends 4 percent and China spends 9 percent. Even as the global recession has forced cutbacks in government spending, other countries continue to invest significantly more than the U.S. to expand and update their transportation networks. AAPA completed its 2012 infrastructure investment survey at the end of May. The following is a regional breakdown of survey respondents:

	Ports Projected Capital Expenditures for 2012—2016	Proj. Private Sector Cap Ex for 2012-2016	Total Projected Capital Expenditures for 2012-2016
NORTH ATLANTIC	$2,122,375,000	$1,206,500,000	$3,328,875,000
SOUTH ATLANTIC	$4,080,678,910	$261,602,000	$4,342,280,910
GULF	$4,340,061,518	$17,782,298,008	$22,122,359,526
GREAT LAKES	$224,650,000	$135,000,000	$359,650,000
NORTH PACIFIC	$1,765,715,068	$5,914,300,000	$7,680,015,068
SOUTH PACIFIC	$5,801,296,561	$2,336,000,000	$8,137,296,561
TOTALS:	**$18,334,777,057**	**$27,635,700,008**	**$45,970,477,065**

OUTSOURCE
THE FREIGHT MANAGEMENT COMPANY

CyberSecurity

Is your company ready, not only for a direct attack but also for the outfall of an attack on others within you're supply chain? Is there a contingency plan? Do you have a disaster recovery plan?

Latest Ransomware Attack Hits Shipping Industry **by Roanoke Trade**

In May, the WannaCry global ransomware attack targeted computers worldwide running Microsoft's Window operating system by encrypting data and demanding ransom payments. WannaCry brought computer systems from Russia to China to the U.K. and the U.S. to their knees, locking people out of their data and demanding they pay a ransom or lose everything. More than 200,000 computers in 150 countries were affected. Now ransomware virus Petya has hit companies worldwide, including shipping giant A.P. Moller-Maersk, which handles one out of seven containers shipped globally.

The Petya cyber attack caused outages at Maersk's computer systems across the world, including at its APM Terminals, preventing new bookings from taking place or providing quotes at affected terminals. The cyber-attack shut down a number of Maersk's IT systems including those it uses to communicate with its customers and business partners. According to *Seatrade Maritime News*, reports from New Zealand indicated the line was using handwritten communication with ports as well as G-mail accounts with customers.

This type of attack quite evidently has a domino effect on the entire supply chain. Just one weak link opens up everyone to potential attacks and subsequent delays. Coordinating ship arrivals, unloading containers and then scheduling storage and trucks to move products out of ports requires a high degree of coordination and efficiency. A big bottleneck in a single port can reverberate widely and quickly.

What is ransomware?
Ransomware is a type of malware that essentially takes over a computer and prevents users from accessing data on it until a ransom is paid. The average ransom amount is $300 to $500 per computer, and the favored payment is bitcoin. In most cases, the software infects computers through links or attachments in malicious messages known as phishing emails. The software usually is hidden within links or attachments in emails. Once the user clicks on the link or opens the document, the computer is infected and the software takes over.

Although ransomware has been around for years, these latest global attacks are much more insidious. Both WannaCry and Petya borrowed leaked National Security Agency code that permits software to spread quickly within an organization's network.

To minimize the potential of a ransomware attack, there are several cyber security steps you can take including:

- Look for malicious email messages that often masquerade as emails from companies or people you regularly interact with online. Avoid clicking on links or opening attachments in those messages, since they could unleash malware.
- Regularly back up data. Remove the external storage device once backup is done so ransomware won't affect the backup.
- Ensure that security updates are installed on your computers as soon as they are released.

Download protection programs that not only fight attacks, but also notify you when there is a threat to your computer.

Be sure to have a business continuity plan in place so that you can get your operations running as smoothly as possible as quickly as possible. In addition, be sure to carry Cyber Liability insurance which can be designed to include cyber extortion coverage in the event of a ransomware attack. Roanoke Trade, which specializes in serving the insurance needs of transportation and logistics providers is available to discuss how Cyber insurance works and the various coverages available in the policy. Please contact one of our Roanoke Trade professionals at 1-800-ROANOKE (800-762-6653) for more information.