IVEY | Publishing

School of Business
D'Amore-McKim
Northeastern University

W19132

CYBERATTACK: THE MAERSK GLOBAL SUPPLY-CHAIN MELTDOWN[1]

David Wesley and Professors Luis Dau and Alexandra Roth wrote this case solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

On June 26, 2017, Jim Hagemann Snabe had just arrived in California, where he was scheduled to speak the next morning on global risks and uncertainty at Stanford University's Directors' College. As he skimmed the participants' handout, he took note of the usual suspects: inflation, trade, energy price fluctuations, monetary policies, macroeconomic trends, and strained markets. Unbeknownst to Snabe, an event unfolding halfway across the globe was about to challenge those conventional notions of risk.

That night, while fast asleep in his Palo Alto hotel room, Snabe was suddenly jolted from his slumber by an incoming call on his cellphone. The Maersk chairman glanced at the iPhone dock on his bedside, which read "4:00 a.m." in a dim blue digital font. Who could be calling at this hour, he wondered.[2]

"We've suffered a major cyberattack!" exclaimed the caller. "The network is down for the entire company—every system, in every location around the globe." Not even the telephone lines were spared. Maersk, which accounted for 18 per cent of global container shipping, had gone dark.

JIM HAGEMANN SNABE

Jim Hagemann Snabe was born in the small Danish commune of Egedal, approximately 30 kilometres from the Swedish border but spent his early childhood in Nuuk, a remote outpost in Greenland where his father was a helicopter pilot. It was a lonely and isolated existence in a place where it took a week or longer to receive a message from the outside world. Returning to Denmark for his high-school education was not easy, but he found solace in the "cold logic" of computers, on which he programmed simple games.[3]

A self-described "nerd," Snabe attended Aarhus University in the late 1980s, where he studied mathematical proofs. However, his main love continued to be computers, and he secured part-time work in the business school's information technology department. "Mathematics is a lonely enterprise," explained Snabe. "My thesis was only read by three people, including my mother, and she did it out of courtesy."[4]

Upon receiving his master's degree in 1990, Snabe became a trainee at software giant SAP, Germany's second-largest company after Siemens.[5] In the mid-1990s, Snabe left SAP for IBM, but returned less than two years later after being offered a position as regional manager for SAP's Nordic region. "At that time,

I thought I was smart and could solve problems on my own," he recalled. "But later I learned that putting the right team together with the best people is more important."[6] Over the next decade and a half, he continued to rise within SAP's ranks until 2010, when he was appointed chief executive officer (CEO). In May 2014, after leading a transformation that saw SAP's stock price more than double, Snabe resigned "to start a new professional life that allows me to spend more time with my family."[7]

Shortly after Snabe announced his retirement, Siemens invited him to join its supervisory board to improve the company's "technology and software competence."[8] He was also elected vice-chairman of Allianz, a German financial services firm that focused on insurance. Over the next couple of years, Snabe wrote a book on leadership, gave seminars at business and leadership conferences, and taught business courses as an adjunct professor at Copenhagen Business School. While promoting his new book, Snabe was asked how "leadership is changing in the digital world." He replied:

> Most companies try to avoid changes until they are in trouble. Many talk about a need for a "burning platform" to change everything. I believe that in the digital world, the ability to reinvent yourself comes from the ability to create a burning desire, not a burning platform.[9]

Finally, in January 2017, Siemens elected Snabe to be supervisory board chairman, promising to further accelerate the company's digital transformation.[10] As if taking the helm of Germany's largest conglomerate was not enough, a few months later Snabe also agreed to serve as chairman of A. P. Møller-Maersk, the world's largest shipping company. It was a move that prompted the *Financial Times* to declare him "Europe's top industrialist."[11]

Shepherding Maersk through "the biggest transformation in its history" would not be easy after the company reported the largest loss of any Danish enterprise. Still, if Maersk could modernize, many believed that Snabe was the one to do so. Not only was he younger, at 51, than the chairmen who had preceded him, he also had "an exceptional gift for finding a clear path through a forest of opportunities, threats, and complexity."[12]

A. P. MØLLER-MAERSK[13]

A. P. Møller-Maersk, commonly known as the Maersk Line, was founded in 1904, when A. P. Møller and his father purchased a used steamship operating out of the Danish port of Svendborg. Ten years later, the company added more steamships to meet the demands of the "Great War" that had engulfed Europe. Shortly after the war, Maersk built its own shipyard and established an overseas office in New York City, where it operated a shipping route from the United States to Asia. Although during the Second World War, most of the company's ships were requisitioned by various Axis and Allied countries, and many were sunk during the war, Maersk was able to resume operations after the war along its original routes and added new routes to the Middle East and Africa.

By the time of A. P. Møller's death in 1965, the company operated nearly half of Denmark's entire merchant fleet. In the 1970s, the company began operating container vessels, which became the defining symbol of the company's global shipping operations. The size of those ships continued to grow over the years, from fewer than 3,000 TEUs to more than 20,000 TEUs in 2018.[14] Maersk also began manufacturing its own containers and developing internal logistics capabilities. In 2005, it acquired Damco, a leading provider of supply-chain management and merged it with Maersk Logistics under the Damco name.

By 2017, Maersk operated out of 343 ports worldwide and managed approximately 18 per cent of the world's container shipping. That meant that "every 15 minutes on average a container ship will come to a port somewhere with between 10 [thousand] and 20 thousand containers," explained Snabe.[15] "For each container shipped, there may be up to 30 different parties involved, communicating up to 200 times."[16] Although the placement and management of orders was typically electronic, most of the "underlying processes" had not changed in decades. Much of it was managed on paper and there was no consistency between countries. Snabe's focus would be to modernize the supply chain partly by digitizing those underlying processes.

> We want to transform the industry by reducing the complexity. . . . The opportunities from digitisation are significant. It has the potential to both simplify the customer experience and improve the productivity of assets, primarily ships and ports, effectively reducing costs across the value chain. It is my sincere belief that this company is best positioned to front the digitisation of the shipping industry. . . .[17]

In 2016, Maersk lost nearly $2 billion[18] on $27 billion in revenue (see Exhibits 1–3). The losses were largely blamed on shipping industry overcapacity, leading to a nearly 20-per-cent drop in freight prices.[19] It was the second annual loss since the devastation of the Second World War. However, by early 2017, demand had increased to the point that it outstripped supply, prompting CEO Søren Skou to predict "reasonable . . . supply-and-demand fundamentals" that would lead to an estimated $1 billion in profit by the end of 2017.[20] He added that, because the "price war" was over, "things are looking a lot better now than they did a year ago. We are starting [2017] from a strong position."[21] At the same time, Skou warned that a trade war between the United States and China could result in a 25-per-cent drop in Chinese exports, negatively impacting Maersk.

WAR IN UKRAINE

For much of its history, Ukraine has been a battleground between east and west. At various points in the 20th century, it was occupied by Poland and Germany to the west and Russia to the east. In many of these conflicts, Ukrainians aligned with various occupation forces. During the Second World War, for instance, some Ukrainian nationalists supported Germany's invasion of the Soviet Union, which had annexed Ukraine in 1921. By the end of the war, 28,000 towns and villages had been razed, and as many as eight million Ukrainians—roughly 20 per cent of the country's population—had lost their lives.[22]

The defeat of Germany by the Red Army left Ukraine entirely in Soviet hands. For the next four decades, Ukraine led the Soviet Union in economic growth and output, even surpassing Western European countries in the output of some key commodities.[23] It also became an important location for technology, hosting various Soviet weapons, aerospace, and energy centres.

The fall of the Iron Curtain led to Ukrainian independence in 1991. However, unlike other former Soviet republics that experienced rapid economic growth in the 1990s, Ukraine was plagued by hyperinflation and a severe recession that saw its gross domestic product fall by 60 per cent. At the same time, state failures pushed many Ukrainians toward the black market, and despite its independence, Ukraine continued to rely heavily on Russia, with which it conducted nearly 40 per cent of its trade.[24]

Tensions over the role of Russia in Ukraine's economic and political affairs came to a head in 2013, when anti-government forces mobilized against pro-Russian president, Victor Yanukovych. Many Ukrainians wanted their country to strengthen ties with the West and perhaps eventually become part of the European

Union, while Yanukovych sought to strengthen Ukraine's ties with Russia, which, for its part, saw the encroachment of the European Union and NATO (the North Atlantic Treaty Organization) as a threat to its security.

In 2014, Russia annexed Crimea following an uprising by pro-Russian militias against Kiev.[25] Inspired by the events in the Crimea, other parts of eastern Ukraine attempted to secede, with pro-Russian separatists receiving material support from Moscow. Despite Russian efforts to destabilize the country, integration with the West continued, including a 2016 free-trade agreement with the European Union and a 2017 visa-free travel agreement. Ultimately, the Ukrainian government saw these agreements as steps toward European Union membership.[26]

CYBERWAR

> We anticipate that cyberwar may be to the 21st century what blitzkrieg was to the 20th century.
>
> John Arquilla and David Ronfeld[27]

The rise of fake news, attacks on the media, and interference in both the Brexit vote and the 2016 American election appeared to catch many off guard. Yet, in their seminal 1993 U.S. Department of Defense analysis on cyberwarfare, John Arquilla and David Ronfeld predicted that "widespread multi-organizational networks that have no particular national identity" would attempt to undermine civil society. "A netwar may focus on public or elite opinion, or both," they explained.

> It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.[28]

Despite these warnings, 25 years later, democratic nations around the world appeared ill-equipped to handle the deluge of cyberattacks directed at large and small organizations, nations, and individuals.

Following the overthrow of Victor Yanukovych in 2014, Russia began sponsoring cyberattacks against key components of the Ukrainian economy and infrastructure, beginning with distributed denial of service (DDoS) attacks against pro-Western websites. A DDoS attack involved using compromised computers and devices to send massive amounts of garbage data over the Internet to targeted websites. In some situations, these attacks resulted in service slowdowns, but often they could knock a site off the Internet for days at a time. Meanwhile, Russia engaged in a social-media campaign, blocking pro-Western accounts and disseminating Russian propaganda.[29]

Phishing—whereby attackers sent emails with links and attachments that, when opened delivered a payload of malicious software (i.e., malware)—was frequently deployed against Ukrainian networks. The malware might manifest itself immediately, but often it worked to stealthily provide access to hackers who would steal information or attack assets at a later time. On December 23, 2015, compromised accounts delivered malware to the Ukrainian power grid, causing a widespread power blackout. The malware simultaneously erased computer drives to delay restoration, and a coordinated DDoS attack disabled the power company's phone lines.[30]

Ransomware was a particularly destructive malware that encrypted victims' data so that it could not be read without a decryption key. Ransomware screens often displayed a payment page that required the victim to pay a fee in bitcoin or other cryptocurrency to receive the decryption key. To mitigate such attacks, network administrators were admonished to back up data on a regular basis, because even when ransoms were paid, the decryption keys did not always work. The best mitigation involved completely erasing the computer drive and restoring the system from an uninfected backup.

NOTPETYA RANSOMWARE

NotPetya was a particularly virulent strain of ransomware that targeted a Ukrainian financial program known as MeDoc. In the weeks leading up to the attack, MeDoc employees opened phishing emails that contained malware attachments or linked to malware servers. The attackers then used leaked U.S. National Security Agency exploits, such as EternalBlue and EternalRomance, which the U.S. government had developed for Internet surveillance. EternalBlue gave attackers remote access to infected systems through vulnerable Microsoft Windows' file and printer sharing protocols, while EternalRomance escalated privileges to control and modify systems without detection.[31]

Although Microsoft issued an emergency patch for the vulnerability in March 2017, many organizations had yet to update their systems.[32] Once computers were infected, attackers could install other software, monitor communications, and steal data and passwords.[33] With those passwords in hand, infecting patched systems became trivial, allowing the attackers to hide the NotPetya ransomware in a software update that was pushed out to MeDoc customers on June 22, 2017.

In fact, a few weeks before NotPetya's devastating attack, Microsoft announced that it had "uncovered a well-planned, finely orchestrated cyberattack that targeted several high-profile technology and financial organizations." Microsoft cybersecurity researcher Elia Floria explained:

> An unknown attacker was taking advantage of a silent yet effective attack vector: the compromised update mechanism or software supply chain for a third-party editing tool. The software vendor that develops the editing tool was unaware of the issue. In fact, while their software supply chain served as a channel for attacking other organizations, they themselves were also under attack.[34]

Floria further noted that the effectiveness of supply chain cyberattacks depended on "the common trust relationship" that exists between customers and suppliers.

NotPetya was also not a true ransomware program, but one that mimicked ransomware by offering to restore infected computers after victims paid a ransom of $300 (see Exhibit 4). However, the attackers provided no means for victims to pay the ransom or receive decryption keys. Instead, NotPetya sought to permanently destroy and disable infected systems and networks.

The sophistication of the tools employed and the fact that no ransom could be paid to recover infected systems suggested that NotPetya was not the work of cybercriminals intent on extorting companies for financial gain, but a state-sponsored group, most likely aligned with Russia. Moreover, NotPetya remained dormant for five days until the eve of Ukrainian Constitution Day, a celebration of independence from Russia and one of the republic's most important holidays.[35]

When this ticking time bomb finally exploded on the morning of June 27, it spread through infected networks at an unprecedented speed. A major Ukrainian bank saw its entire network destroyed in 45 seconds. It started with an unscheduled reboot of computers, followed by encoding of the master boot record that controlled how programs were loaded onto computers. A warning then appeared on the screen that the file system was being "repaired." "DO NOT TURN OFF YOUR PC!" it read. In fact, the only way to save the data from permanent destruction was to shut off power before the files could be encrypted. If one followed the attacker's instructions, the computer would reboot a second time and display fake ransomware payment "instructions." By this time, company files had been lost forever.[36]

More than 300 Ukrainian companies, banks, and hospitals were compromised, representing roughly 10 per cent of the country's computers.[37] Although NotPetya had targeted Ukraine specifically, multinational corporations doing business in the region often used MeDoc for local tax filing. Once computers had been compromised, the malware also spread throughout their global networks. One of those firms was A. P. Møller-Maersk.

MAERSK'S MESS

> Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds; and be stolen without your knowledge.
>
> Bruce Schneier, chief technology officer of IBM Resilient[38]

On June 27, Pawel Szczecki, CEO of Predica, a Polish analytics company that provided support to Maersk, was meeting with his Maersk counterparts in London, England, where the company's information technology (IT) support was headquartered. He recalled:

> It was . . . a nice summer day. The morning started out like any other. The planned meeting began and discussions about the *new Managed Service operations* had just commenced, when a large commotion spread across the office. Suddenly, the monitoring screens started to show all systems turning to red, and not long after all laptops started to reboot.[39]

Similar events were happening across the company's global network. As a systems engineer in Copenhagen prepared to deliver an update for the company's 80,000 personal computers (PCs), his computer spontaneously rebooted. When he rose from his desk, he noticed "a wave of screens turning black" as all the PCs began simultaneously rebooting.[40]

Back in London, systems administrators took nearly 30 minutes to realize what was happening before they began shouting to everyone to unplug their machines. The entire network took more than two hours to shut down, primarily because email, messaging, and phone systems were also down as employees resorted to WhatsApp and personal phones to communicate. By then the damage had been done.

Maersk's senior system administrators had warned the company that its network was vulnerable to attack. In 2016, they had complained that the company's ancient Windows 2000 server software was overdue for a complete overhaul. Additionally, because Microsoft had long discontinued support for Windows 2000 and Windows XP, both of which were still used on many of the company's PC terminals, any PCs running those outdated operating systems did not receive security patches. The senior system administrators had warned that, unless something was done, the entire infrastructure could face a

crippling attack. Maersk's senior leadership team had approved the upgrades, but the systems administrators—whose bonuses depended on current infrastructure uptime, not installing upgrades—had never implemented them.[41]

Good computer hygiene involved not only keeping software up to date but also providing regular backups. In this area, Maersk followed best practice, making backups of its data every few days and keeping those backups off-line at various locations across its global network. However, a central piece was missing, the domain controllers that mapped the company's network and allowed access to authorized users.

A domain controller was a Microsoft Windows server that authenticated users and provided access to computer resources. It was essentially the central nervous system of the computer network, consisting of an "active directory" of multiple master controllers. Maersk operated a network of 150 domain controllers, each of which could act as a backup for the entire network. If one failed, it could easily be restored from any one of the other 149 controllers. What the company hadn't accounted for was all 150 nodes being hit by the same malware simultaneously, wiping out the entire network in one foray. It meant that the company's entire network structure would be lost—*forever*—unless a controller somewhere in the company had been off-line during the attack. "The primary and key objective was to reestablish the Active Directory for identity management," recalled Szczecki. "This was necessary to reenable resource access which was the first step towards switching back to automated operations."[42]

Normally, conducting a search of company resources would have simply involved emails or phone calls to key IT staff at each of the company's 150 domain controller sites. However, with the email and phone lines knocked out by the same cyberattack, the emergency-response centre had resorted to communicating through personal emails and phone numbers, not all of which were readily accessible without the HR (human resources) personnel database. Maersk brought in consultants from Deloitte to manage the recovery effort, along with smaller IT firms such as Predica. The company booked all the hotels in the area to house the recovery team, but many were working such long hours that they chose to sleep in the office.[43]

As status updates rolled in from the various sites, the team became increasingly disillusioned. Everyone had been hit. It began to appear that the network directory was lost forever, when word arrived that one site may have survived—in Ghana. The West African country was in the midst of a longstanding energy crisis that had led to the demise of numerous businesses. The nation was often plunged into total darkness for up to 24 hours at a time, and generator prices in the country soared. The unreliable power situation also had economic consequence, and "Morgan Stanley . . . cut its 2015 growth forecast for Ghana from 5 per cent to 3 per cent due to the power cuts."[44]

For most Ghanaians, the power outage on June 27 was yet another reason to curse the government. For Maersk however, it seemed like divine intervention, as "joyous whoops" filled the London command centre.[45] The ecstasy was short-lived, however, because the company needed to find a way to recover the data.

The domain controller could not be connected to the Internet, as Ghana's network bandwidth was so slow it would have taken days to transmit. Moreover, connecting it to the internet risked infecting the last known controller and the company's last hope of restoring its network. Instead, the company instructed its administrator in Ghana to deliver the hard drive to London for examination. But there was one problem. No one in the Ghana office had a travel visa for the United Kingdom and Europe, and it would take weeks to get one. Instead, an employee from Ghana would need to travel to Nigeria and hand the hard drive to

an employee in that country, who would then transport the hard drive to London. For a time, it became the most valuable hard drive in the world.

MANAGING A GLOBAL SHIPPING COMPANY WITH PEN AND PAPER

As the London Emergency Response Centre worked furiously to restore Maersk's IT infrastructure, shipping terminals around the world were becoming hopelessly backlogged. Maersk operated the largest terminal in the Port of Los Angeles, commonly known as America's port because of its importance to U.S. trade. Not only was the Port of Los Angeles the largest container port in the United States, but, as a part of the San Pedro Bay Port Complex, and together with the neighbouring Port of Long Beach, it supported one in nine jobs in the five-county Southern California region.[46] As Maersk shut down its global computer network, it was left with no choice but to close the terminal.[47]

A similar story was unfolding at Maersk's terminal in Port Elizabeth, New Jersey, the largest port on the east coast. Three thousand trucks arrived daily at the port to load and unload hulking containers loaded with furniture, electronics, bananas, and almost every other imaginable product. On the morning of June 27, more than 800 trucks lined the road for more than a mile to the port, unable to move. Some sat for as long as six hours before police told them to turn around and leave the area.[48] One trucker explained how he received an incomprehensible email about the attack from a Gmail account. It offered no explanation and no information about when the port would reopen. His only recourse was to find somewhere to store his cargo and await word.[49]

Normally, 90 per cent of Maersk's shipping orders were placed through the company's online system. The company had no choice but to manage shipments manually. Many companies with tight supply chains could not wait for orders to be processed manually. Instead, they sought out alternative shippers, in many cases resorting to costly air freight. Maersk offered to compensate customers for the added expenses, which amounted to millions of dollars per customer. Overall, Maersk saw its shipping volume decline by 20 per cent.

Customers that remained with Maersk during the cyberattack and its aftermath were often forced to resort to pen and paper, pasting sticky notes onto packages and then tracking them in Excel. Coordination was done on WhatsApp, which at the time became, in effect, Maersk's instant messenger outside of the United States.

Maersk's ships were mostly disconnected from the network during the attack and therefore had not been infected. Moreover, ships were required to have procedures in place to handle adverse conditions, such as natural disasters, and were able to function independently. For ships that were already loaded, the impact was minimal. Søren Meyer of Maersk Tankers explained that although his division was also hit by the attack, it was able to function without the IT system. "It comes back to the craftsmanship of our people and the hard work of our people being able to do things with a pen and paper," he explained.[50]

Once the network restoration began, online ordering and tracking was prioritized to allow shipping services to return to normal. On July 25, 2017, Maersk announced that its online quoting system was back online and that it was working toward clearing the backlog of delayed shipments (see Exhibit 5).

COUNTING THE COST

"We had to install 4,000 new servers, 45,000 new PCs, 2,500 applications," Snabe noted. "And that was done in a heroic effort over ten days. Normally—I come from the IT industry—I would say it's going to

take six months. It took ten days and was a heroic effort."[51] Nevertheless, those 10 days cost the company some $300 million in expenses and lost earnings. And it would take weeks to re-image and upgrade every computer in the company.

Any locally stored information on infected PCs that had not been backed up prior to the attack was forever lost, including contacts, orders, and any personal files, such as family photos. Moreover, because hackers had gained access to compromised networks for weeks or months prior to the attack, they may have siphoned valuable business and personal data from victim PCs. Given that the drives were destroyed by NotPetya, it would be impossible to determine what, if any, information had been stolen.

For Snabe it was a wake-up call. "It is time to stop being naïve when it comes to cybersecurity," he said, vowing to transform Maersk into a world leader in network and supply-chain security. "Many companies will be caught if they are naïve. I think that it is important that we are not just reactive but proactive."[52]

EXHIBIT 1: MAERSK INCOME STATEMENTS, 2013–2016 (IN US$ MILLIONS)

Income statement	2016	2015	2014	2013
Revenue	27,266	30,161	34,806	33,908
Profit before depreciation, amortization and impairment losses, etc.	2,475	4,365	5,284	4,398
Depreciation, amortization and impairment	2,495	2,391	2,730	2,226
Gain on sale of non-current assets, etc., net	190	391	505	128
Share of profit/loss in joint ventures	130	147	29	134
Share of profit/loss in associated companies	–55	97	416	337
Profit/loss before financial items	245	2,610	3,505	2,771
Financial items, net	–543	–452	–727	–636
Profit/loss before tax	–298	2,158	2,778	2,134
Tax	171	225	509	134
Profit/loss for the year – continuing operations	–469	1,934	2,269	2,000
Profit/loss for the year – discontinued operations[1]	–1,428	–1,009	2,925	1,777
Profit/loss for the year	–1,897	925	5,195	3,777
A.P. Møller - Mærsk share	–1,939	791	5,015	3,450
Underlying profit/loss – continuing operations	–496	1,553	2,580	1,837

Notes: [1] Discontinued operations comprise Maersk Oil, Maersk Tankers, Maersk Drilling and Maersk Supply Service. Comparative figures have been restated for the income statement and cash-flow statement.
Source: *Maersk 2017 Annual Report*, accessed September 19, 2018, http://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf.

EXHIBIT 2: MAERSK BALANCE SHEETS, 2013–2016 (IN US$ MILLIONS)

Balance sheet	2016	2015	2014	2013
Total assets	61,118	62,408	68,844	74,509
Total equity	32,090	35,739	42,225	42,513
Invested capital	42,808	43,509	49,927	54,630
Net interest-bearing debt	10,737	7,770	7,698	11,642
Investments in property, plant and equipment, and intangible assets – continuing operations	4,585	3,597	3,552	3,070
Cash flow statement				
Cash flow from operating activities (from continuing operations	1,264	4,267	4,914	4,332
Cash flow used for capital expenditure (from continuing operations)	–2,073	–1,852	–2,279	–2,340
Net cash flow from discontinued operations	503	226	1,806	150
Financial ratios				
Return on invested capital after tax – continuing operations[1]	0.5%	8.2%	8.4%	7.6%
Return on equity after tax	–5.6%	2.4%	12.3%	9.2%
Equity ratio	52.5%	57.3%	61.3%	57.1%

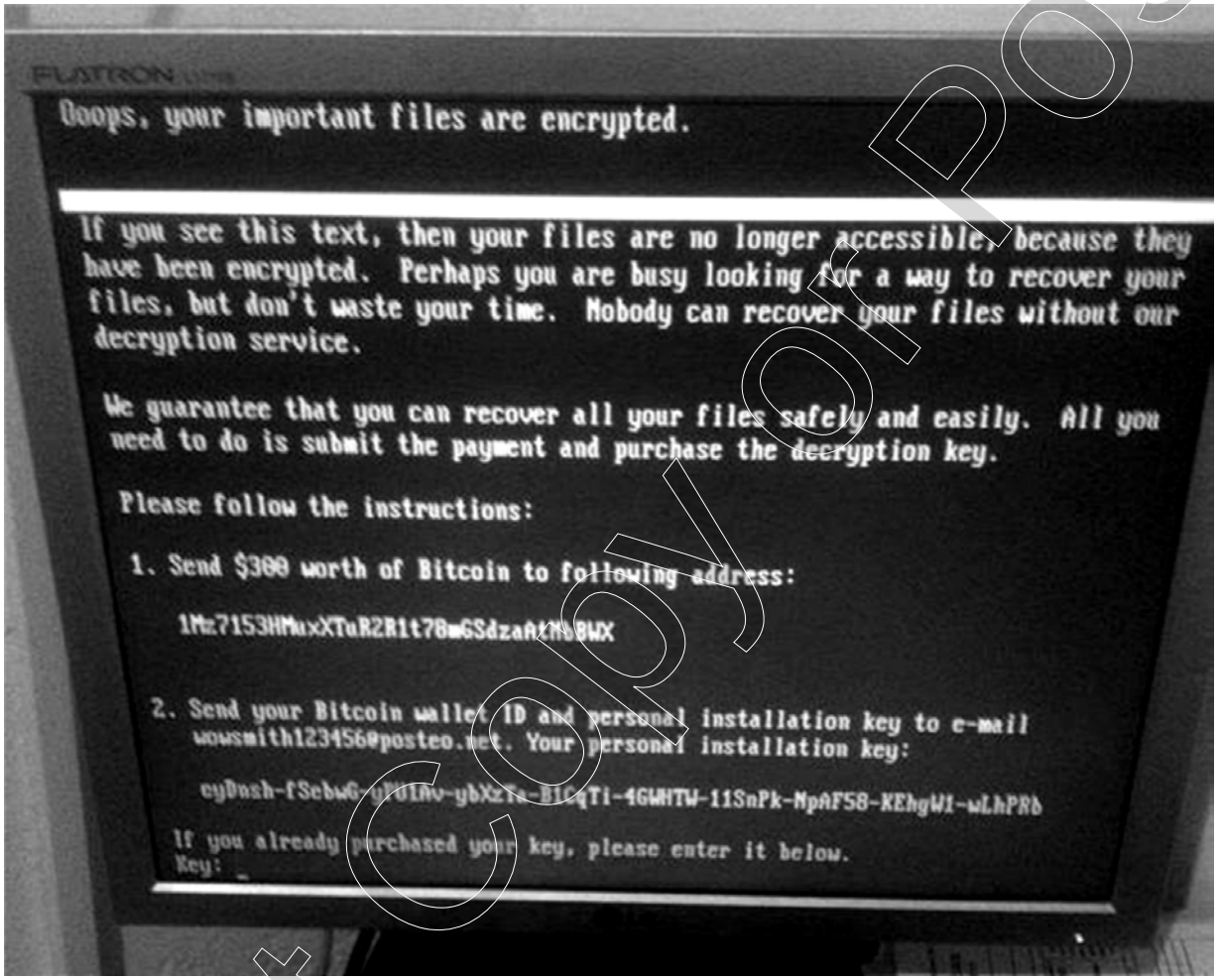
Notes: [1] Excluding Hamburg Süd for comparison purposes.
Source: *Maersk 2017 Annual Report*, accessed September 19, 2018, http://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf.

EXHIBIT 3: MAERSK STOCK MARKET RATIOS AND BUSINESS DRIVERS, 2013–2016

Stock market ratios	**2016**	**2015**	**2014**	**2013**
Earnings per share – continuing operations, USD	–25	84	97	84
Diluted earnings per share – continuing operations, USD	–25	84	97	84
Cash flow from operating activities per share, USD	61	199	225	198
Ordinary dividend per share, DKK	150	300	3004	280
Ordinary dividend per share, USD	21	44	494	52
Share price (B share), end of year, DKK	11,270	8,975	12,370	11,770
Share price (B share), end of year, USD	1,597	1,314	2,021	2,175
Total market capitalization, end of year, USD millions	32,215	27,587	42,848	46,305
Business drivers				
Maersk Line[1]				
Transported volumes (FFE in '000)	10,415	9,522	9,442	8,839
Average freight rate (USD per FFE)	1,795	2,209	2,630	2,674
Unit cost (USD per FFE including VSA income)	1,982	2,288	2,584	2,731
Average fuel price (USD per tonne)	223	315	562	595
Maersk Line fleet, owned	292	285	274	275
Maersk Line fleet, chartered	347	305	336	299
Fleet capacity (TEU in '000)	3,239	2,962	2,946	2,631
APM Terminals				
Containers handled (measured in million TEU and weighted with ownership share)	37.3	36.0	38.3	36.3
Number of terminals	73	63	64	65

Notes: USD = U.S. dollars; DKK = Danish krone; FFE = forty-foot equivalent units; VSA = Vessel Sharing Agreement; TEU = twenty-foot equivalent units; [1] excluding Hamburg Süd for comparison purposes.
Source: *Maersk 2017 Annual Report*, accessed September 19, 2018, http://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf.

EXHIBIT 4: RANSOMWARE EXAMPLE



Source: User:Jbuket, "File: PetyaA.jpg," Wikimedia Commons, June 27, 2017, accessed October 19, 2018, https://commons.wikimedia.org/wiki/File:PetyaA.jpg. Used with permission.

EXHIBIT 5: MAERSK GLOBAL UPDATE, JULY 25, 2017

Dear customer,

We hope your workweek is off to a great start. As we continue our last sprint toward full recovery, we would like to share the final global update on some of the items that are of interest to you; going forward, these updates will be handled by your local Maersk Line team because, while all global applications are up and running, there are some local variances. This ensures you get frequent regional information that is relevant to your business.

When we reflect on the activities of the last four weeks, we have conducted extensive work on our IT infrastructure. Concurrently, we have worked hard to clear the backlog and make sure the impact on your business has been as minimal as possible. During this process, our local teams have been required to handle lots of manual work, and everyone is looking forward to returning to servicing your business in a seamless and efficient manner. We thank you once again for your patience and support.
With that, let us get to today's updates:

Online Quote

We are pleased to announce that the quote request form for short-term rates is now back online—available globally. This means we will once again be able to give you quick and relevant shipping rates online. You can submit your quote request here: https://my.maerskline.com/onlinequote/. We strive to provide you with a rate within just a few hours, but also anticipate that the increased number of requests this week might result in slightly longer response times.

We know that some of you have asked for spot quotes over the last few weeks. We want to make sure that you get the most relevant and latest rate offering at hand, which means we have opted to focus on your new requests coming in through the online form. We hope you will resubmit your quote request and look forward to supporting your business. Our short-term rate sheets and long term contracting are running normally as previously advised.

Submission of Advanced Manifest

We can confirm that we are in full compliance with both U.S. and EU regulations related to Advanced Manifest process. It is of great importance that Shipping Instructions are submitted in due time in order to comply with Advanced Manifest deadlines. Submission deadlines will be listed on your Booking Confirmation as usual.

General global status

The majority of our global applications is back up and running which enables us to execute the processes to move your cargo. We are open for all your quotations. Our website is working with all functionalities; we are handling bookings through the various normal channels and processing shipping instructions, including advanced manifest submissions to relevant authorities.

Our import releases and inland deliveries are also flowing, although we acknowledge we still have some challenges in certain locations due to manual processing and capacity restrictions. Lastly, we are issuing invoices online but still have a few remaining items to progress on local invoicing applications which we continue to work on over the next period.

As we clear the last parts of the backlog and serve your new business, we acknowledge that you may still encounter some data quality inconsistencies and delays in response times in some locations. We assure you that we are fully committed to returning to our normal standards as soon as possible.

We understand that this journey has been inconvenient and sometimes frustrating for you and we would like to thank you once again for your patience and trust in us. The kind gestures that many of you have offered our local teams—ranging from offering office space and laptops, to sending cakes and encouraging words—are truly humbling and we sincerely appreciate all the support.

Thank you
The Maersk team

Note: IT = information technology; EU = European Union
Source: Maersk, 25 July Global Update, July 25, 2017, accessed October 24, 2018, www.maersk.com/news/2017/07/25/25th-july-global-update.

ENDNOTES

[1] This case has been written on the basis of published sources only. Consequently, the interpretation and perspectives presented in this case are not necessarily those of A. P. Møller-Maersk A/S or any of its employees.
[2] Catalin Cimpanu, "Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover from NotPetya Attack," BleepingComputer.com, January 25, 2018, accessed September 13, 2018, www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/.
[3] Marcus Rohwetter, "SAP-Chef Snabe: Nur beinahe ein Nerd," [in German], *Zeit Online*, July 5, 2012, accessed September 17, 2018, www.zeit.de/2012/28/P-Snabe/komplettansicht.
[4] Ibid.
[5] Michael Schrøder, "BSS Alumni Reach the Top," Aarhus University, March 22, 2017, accessed September 17, 2018, https://medarbejdere.au.dk/en/faculties/business-and-social-sciences/news/news-article/artikel/bss-alumni-reach-the-top/.
[6] Rohwetter, op. cit.
[7] "Chefwechsel bei SAP: Snabe geht 2014, McDermott wird alleiniger CEO," [in German], *Computerwoche.de*, July 22, 2013, accessed September 18, 2018, www.computerwoche.de/a/snabe-geht-2014-mcdermott-wird-alleiniger-ceo,2542885.
[8] Derek du Preez, "Outgoing SAP co-CEO to join Siemens," *ComputerworldUK*, September 18, 2013, accessed September 18, 2018, www.computerworlduk.com/it-vendors/outgoing-sap-co-ceo-join-siemens-3469346/.
[9] Andrea Diederichs, "Interview with Former SAP Co-CEO Jim Hagemann Snabe: 'I'm a Concerned Optimist'," SAP News Center, November 6, 2017, accessed September 18, 2018, https://news.sap.com/2017/11/interview-with-former-sap-co-ceo-jim-hagemenn-snabe-im-a-concerned-optimist/.
[10] "Jim Hagemann Snabe Elected New Supervisory Board Chairman," Siemens Global, press release, January 31, 2018, accessed September 18, 2018, www.siemens.com/press/en/pressrelease/?press=/en/pressrelease/2018/corporate/2018-q1/pr2018010147coen.htm.
[11] P. McGee, "Jim Hagemann Snabe steps up as Europe's top industrialist", *Financial Times*, February 10, 2017, accessed February 28, 2018, www.ft.com/content/605a392c-eed6-11e6-930f-061b01e23655.
[12] Richard Milne, "Jim Hagemann Snabe Steps Up as Europe's top industrialist," *Financial Times*, February 10, 2017, accessed September 13, 2018, www.ft.com/content/605a392c-eed6-11e6-930f-061b01e23655.
[13] Much of this section on Maersk's history is based on "Explore Our History: Go back in Time with A.P. Moller—Maersk," Maersk, accessed September 19, 2018, www.maersk.com/about/our-history/explore-our-history.
[14] "TEU stands for Twenty-Foot Equivalent Unit which can be used to measure a ship's cargo carrying capacity. The dimensions of one TEU are equal to that of a standard 20' shipping container. 20 feet long, 8 feet tall. Usually 9–11 pallets are able to fit in one TEU. Two TEUs are equal to one FEU (forty-foot-equivalent unit)." EJ, "What Is a TEU?" Dedola Global Logistics, October 13, 2011, accessed September 19, 2018, https://dedola.com/2011/10/what-is-a-teu/.
[15] "Securing a Common Future in Cyberspace," YouTube video, 59:06, posted by World Economic Forum, January 24, 2018, accessed September 13, 2018, www.youtube.com/watch?time_continue=224&v=Tqe3K3D7TnI.
[16] *Maersk 2017 Annual Report*, 5, 2018, accessed September 19, 2018, http://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf.
[17] Ibid.
[18] All currency amounts are shown in US$ unless otherwise specified.
[19] Wolf Richter, "World's Largest Container Carrier 'Unexpectedly' Has Big Loss in Crushed Industry. Now Trade War with China Looms," *Wolf Street*, February 8, 2017, accessed September 21, 2018, https://wolfstreet.com/2017/02/08/maersk-worlds-largest-container-carrier-has-big-loss-in-crushed-industry-trade-war-with-china-looms/.
[20] DC Velocity Starr, "Maersk Posts Massive 2016 Loss; Company Sees Better Days Ahead," *DC Velocity*, February 8, 2017, accessed September 21, 2018, www.dcvelocity.com/articles/20170208-maersk-posts-massive-2016-loss-company-sees-better-days-ahead/.
[21] Richter, op. cit.
[22] Keith Lowe, *Savage Continent: Europe in the Aftermath of World War II* (New York: Picador, 2013).
[23] Paul Robert Magocsi, *A History of Ukraine: The Land and Its Peoples* (Toronto: University of Toronto Press, 2012).
[24] Paul J. J. Welfens and Evgeny Gavrilenkov, *Restructuring, Stabilizing and Modernizing the New Russia: Economic and Institutional Issues* (Berlin: Springer, 2000).
[25] Jonathan Roessler, *Can Annexation Be Justified? Analysing Russia's Annexation of Crimea* (Munich: GRIN Publishing, 2017).
[26] Gillaume Van der Loo, *The EU-Ukraine Association Agreement and Deep and Comprehensive Free Trade Area: A New Legal Instrument for EU Integration without Membership* (Leiden, Belgium: Brill Nijhoff, 2016).
[27] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (2016): 141–165.
[28] Ibid.
[29] Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica CA: RAND Corporation, 2017).
[30] Gaoqi Liang, Steven R. Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," *IEEE Transactions on Power Systems* 32, no. 4 (2017): 3317–3318.
[31] Dan Goodin, "NSA-Leaking Shadow Brokers Just Dumped Its Most Damaging Release Yet," *Ars Technica*, April 14, 2017, accessed October 16, 2018, https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/.
[32] Robert Hackett, "This Ukrainian Company Is Likely Behind the Ransomware Wave," *Fortune*, June 27, 2017, accessed October 15, 2018, fortune.com/2017/06/27/petya-ransomware-ukraine-medoc/.

[33] Lily Hay Newman, "The Leaked NSA Spy Tool That Hacked the World," *Wired*, March 7, 2018, accessed October 15, 2018, www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.
[34] Elia Florio, "Windows Defender ATP Thwarts Operation WilySupply Software Supply Chain Cyberattack," Microsoft Secure, May 4, 2017, accessed October 15, 2018, https://cloudblogs.microsoft.com/microsoftsecure/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/?source=mmpc.
[35] Hackett, op. cit.
[36] Karen Sood and Shaun Hurley, "NotPetya Technical Analysis—A Triple Threat: File Encryption, MFT Encryption, Credentail Theft," *CrowdStrike* (blog), June 29, 2017, accessed October 16, 2018, www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/.
[37] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 24, 2018, accessed October 16, 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[38] Bruce Schneier, *Protect Your Macintosh* (Berkeley, CA: Peachpit Press, 1994), 1
[39] "Conquering NotPetya: Two Weeks on the Front Line," Predica, June 15, 2018, accessed September 14, 2018, https://predica.pl/blog/conquering-notpetya/.
[40] Greenberg, op. cit.
[41] Ibid.
[42] "Conquering NotPetya," op. cit.
[43] Greenburg, op. cit.
[44] Matthew Mpoke Bigg and Kwasi Kpodo, "Ghana Power Blackouts Add to Nation's Economic Woes," *Reuters*, May 13, 2015, accessed October 16, 2018, www.reuters.com/article/ghana-power/ghana-power-blackouts-add-to-nations-economic-woes-idUSL3N0Y26JX20150513.
[45] Greenburg, op. cit.
[46] "About the Port of Los Angeles," The Port of Los Angeles, accessed October 19, 2018, www.portoflosangeles.org/.
[47] Jill Leovy and Alexa D'Angelo, "Maersk's L.A. Port Terminal Remains Closed after Global Cyberattack," *Los Angeles Times*, June 29, 2017, accessed October 19, 2018, www.latimes.com/business/technology/la-fi-maersk-cyber-attack-20170629-story.html.
[48] Hugh R. Morley, "NY-NJ's APMT Terminal Aims for Full Operations Come Wednesday," *Journal of Commerce*, July 10, 2017, accessed October 19, 2018, www.joc.com/port-news/port-productivity/ny-nj's-apmt-terminal-aims-full-operations-come-wednesday_20170710.html.
[49] Greenburg, op. cit.
[50] Mfame Team, "Maersk: 'Pen and Paper' Kept Business Running During Cyber Attack," Mfame.guru, November 16, 2017, accessed October 24, 2018, http://mfame.guru/maersk-pen-paper-kept-business-running-cyber-attack/.
[51] Catalin Cimpanu, "Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover from NotPetya Attack," BleepingComputer, January 25, 2018, accessed September 13, 2018, www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/.
[52] Pete Donahue, "To Serve and Protect: Cybersecurity Tips for PR Pros and Clients," *Strategy & Tactics*, October 2, 2018, accessed October 19, 2018, https://apps.prsa.org/StrategiesTactics/Articles/view/12349/1162/To_Serve_and_Protect_Cybersecurity_Tips_for_PR_Pro.