

BUNKERSPOT

CYBER STORM HOW SECURE ARE YOUR BUNKER DEALS?

INSIDE:
FUEL TESTING
REGULATORY COMPLIANCE
VESSEL MONITORING
ALTERNATIVE FUELS



NEWS

Financial outlook 8
 Europe10
 Americas18
 Asia Pacific 25
 Africa and Mideast 29

Features

Cybercrime

Cyber hackers are targeting the bunker industry – and the financial implications can be huge. Steve Simms offers a counter-offensive to this growing threat 30

LNG

LNG America is designing a ‘hub and spoke’ architecture for the distribution of LNG to the major US Gulf Coast ports. CEO Keith Meyer explains the company’s vision 34
 Innovative solutions invariably require market ‘pioneers’ to prove their viability. Sam Lowrey spoke to Ed de Jong about Deen Shipping’s commitment to LNG..... 36
 Regulations and supply structures governing the use of marine LNG are being implemented. However, as Sam Lowrey discusses, pricing LNG as a fuel is far less clear cut 40

Alternative Fuels

New research shows that glycerine has clear potential as a niche bunker fuel. Rebecca Byers discovers more42

ECA Regulations

Much work remains to be done on the ‘policing’ of sulphur emissions regulations in Europe after 2015. Lesley Bankes-Hughes takes a closer look at the problem..... 46

Environment

Researchers at the Tyndall Centre believe that the shipping sector has yet to wake up to the problem of CO₂ emissions. Rebecca Byers finds out more 50

Trade Focus

The US Administration is under increasing pressure to lift the ban on US crude oil exports. However, as Melanie Wold explains, this long-standing legislation continues to polarise opinion52

Finance

Innovations in exchange platforms have provided the transparency that is required for commodity derivatives to evolve. Chris Thorpe takes a closer look at this dynamic marketplace..... 54

Regional Focus: Russian Far East

The opening up of the North Sea Route will have a major effect on cargo transit schedules. As Rebecca Byers finds out, RFE suppliers are gearing up for new business opportunities..... 58

Regional Focus: Latin America

Pedro Gomez of OW Bunker Latin America explores the region’s changing bunker market and explains why ECA regulations are bolstering the market for LSFO supply at gateway locations..... 62

Fuel Issues

As the Arctic Ocean opens up to increasing maritime trade, Albert Leyson of Drew Marine urges operators to reassess fuel flow parameters for distillate fuel oil..... 64

Fuel Cell Technology

An innovative fuel cell technology project for the maritime sector is poised to move to the next level, as Mike Janes of Sandia National Laboratories explains.....67

Vessel Monitoring

Peter Mantel of BMT SMART discusses how performance monitoring systems can be effective drivers towards vessel efficiency70

Scupper Plug

Mark Bell, General Manager of the Society for Gas as a Marine Fuel, outlines the key points on the agenda of its newly-formed technical committee.....72

Event focus74
 Networking 76
 Bunkerspotted 77
 Conference Diary78

page 30



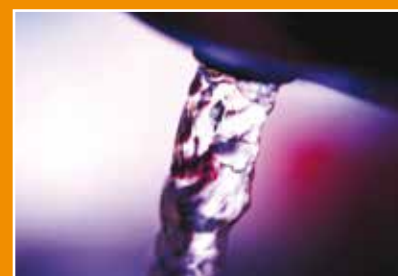
Steve Simms shows how cybercrime is impacting the bunkering industry – with huge financial implications

page 42



Rebecca Byers investigates glycerine’s potential as a niche bunker fuel

page 64



Albert Leyson flags up some key distillate fuel flow parameters for vessels on Arctic Ocean transits

bunkerspotted... on page 77



Safe house

Cyber hackers are targeting the bunker industry – and the financial implications can be huge. Steve Simms offers a counter-offensive to this growing threat

Most of the world's bunker quotations, and sale and payment transactions, now take place electronically. An email arrives, sometimes from a customer the trader believes he or she knows, but often not. The email requests a quote, and the trader uses the email address on the customer's (or supposed customer's) email to quote back, including (following best practices) the trader's sales terms and conditions. An email returns accepting the quote, and the trader emails back a stem (again incorporating sales terms and conditions) and also confirms the purchase with a physical supplier, who also emails back confirmation incorporating its own sales terms and conditions. The bunkers are loaded, the trader emails an invoice with wire payment instructions, and the physical supplier also emails the trader wire payment instructions.

Throughout this process there are at least eight email communications, three of which confirm contractual sales conditions, and two of which transmit bank account wire information. Some are only text with graphics, others have text with .pdf attachments, including invoices, loading receipts or testing results.

Those in the bunkering industry execute literally thousands of transactions like this each day. But aside from the traders, customers and physical suppliers themselves, how many people are involved with, and could have access to, these transactions?

The answer is thousands, if not more.

Before reaching the intended recipient, an email travels across a

variety of public servers and can be intercepted at any point. The use of web-based access to emails, for off-network and out of office email access typically needed by travelling employees, further increases interception possibilities.

In our worldwide legal practice representing bunker suppliers, brokers and traders, we have seen increasing numbers of criminals gaining access to bunker suppliers', brokers' and traders' electronic communications. These criminals know how the bunker industry works, they use the language and means of communication familiar to the industry, and they are adept at intercepting communications, creating fake email accounts, modifying .pdf documents, and forging invoices and receipts.

Because of the industry knowledge they demonstrate, we believe that many may have at one time worked in an area of the bunkering industry. Insiders still in the industry, such as lower level personnel with access to email, customer and bank account information, may also be assisting them. They target particular transactions, where they seem to know that the supplier, broker or trader, or their customer, may not be attentive to changes of bank account, email or other information.

In rare instances, bunker suppliers, brokers and traders detect the potential crime before it happens – perhaps via their customers who receive what seem to be out-of-ordinary documents and emails. More often, however, the crime is uncovered after the bunker parties involved have wired funds to a fictitious bank account which the criminal has set up in the broker's, supplier's or trader's name. Only then will email exchanges be examined and the subtle email address changes and modified documents picked up.

The bunker supplier, broker or trader, or customer who fall victim to this electronic theft may lose a significant amount of money. The criminal theft of individuals' credit card information by hacking or internet web site 'phishing' is well known, but given typical card credit limits, the monetary losses are relatively low. The credit card industry itself has also created elaborate security approaches to deter fraud. This is not the case with most bunker suppliers, brokers, traders or their customers who undertake enquiries and transactions via unsecured and unencrypted email and then send wires to accounts which those unsecure emails have specified.

Many bunker suppliers, traders, brokers and their customers could be seen as 'low hanging fruit' for cyber criminals. Diverting just one wire concerning a bunker transaction can instantly net an on-line criminal hundreds

'These criminals know how the bunker industry works, they use the language and means of communication familiar to the industry, and they are adept at intercepting communications'

of thousands of dollars with little chance of detection. The magnitude of gain from such criminal diversion also leaves ample funds for incentive payments to lower level personnel in the bunker industry who have access to sensitive electronic information and for whom such payment may well exceed their honestly-earned pay.

The embarrassment over the discovery of such criminal fraud can also prevent reporting to authorities, which further emboldens the criminals. The fraud, once discovered, is usually one that, had there been more careful oversight of emails, could have been discovered. Questions are then raised over who is responsible and what should be done about it.

Reporting to authorities could bring investigators into a company to inspect its electronic systems and perhaps look into areas that the company would prefer to keep private. Then, there is the question of how to replace the stolen funds. If the customer has paid on fraudulent wire advice, generated arguably because of a broker's, trader's or supplier's lack of diligence, must the customer pay twice, once to the criminal and again to the real seller? Even if the customer, reluctantly, pays (again) into a genuine account, he is unlikely to engage in repeat business.

Let's now look at three types of electronic theft – or attempted theft – which our bunker clients have been subjected to. Some resulted in the theft of hundreds of thousands of dollars, never to be recovered, and others, with our intervention, were detected before they could occur.

In one example, the trader confirmed a stem and then placed a delivery order with a physical supplier. The physical supplier was one who the trader did not ordinarily use, but who offered a below market price for the delivery. The physical supplier provided bunkers to the customer's vessel, and the trader received an emailed invoice which appeared to be from the physical supplier. As he had done hundreds of times before,

the trader forwarded the emailed invoice to the trader's book-keeping staff, who quickly executed a wire to the instructions from the supposed physical supplier. Not long afterwards, the trader received another email from the physical supplier – this was a genuine one with an invoice attached which stated the supplier's real wire information. The supplier identified the first wire instructions as fraudulent; the trader protested against paying again to the supplier's authentic account. The supplier threatened to arrest the customer's ship for non-payment. Reluctantly, the trader paid (again).

In another situation, the broker completed the delivery to the customer though the physical supplier. Again using email, the broker emailed an invoice to the physical supplier, including wiring information for payment. A criminal intercepted the email and forged a 'corrected' invoice (appearing in layout and design almost identical to the authentic invoice) which stated 'new' wiring instructions, and in a covering email, with an address almost identical to the broker's, even offered a discount for immediate payment to the 'corrected' invoice details. The customer, however, sensed something amiss and contacted the broker who immediately uncovered the fraud. The customer made one payment, to the broker's correct account (without even expecting the 'discount!').

In our third example, the supplier was involved in a quality dispute with the customer and the customer refused to pay. This resulted in lengthy email exchanges, including detailed testing information and each side's position on the claims. Finally, the supplier and the customer agreed to settle the dispute, and the supplier emailed the customer with a letter in .pdf format including the imaged, physical signature of the supplier's managing director, stating the settlement terms and wiring instructions for the settlement amount. The customer insists that it never received this email.

Instead, the customer received a

forged letter, which included an image of the managing director's signature, stating a fraudulent bank account opened in the supplier's name. The customer signed the letter to acknowledge settlement, wired funds to the fraudulent bank account, and then returned the signed/acknowledged letter, imaged in .pdf, by email to what it thought was the supplier's email address. The supplier then received a copy of its authentic letter (with authentic wiring instructions) and the customer's imaged acknowledging signature. The supplier, however, never received the wired settlement funds (which went to a fraudulently-opened account).

The supplier learned of the fraud when it contacted the customer about the missing funds – and the customer sent the forged letter. An examination of emails showed slight alterations of some of the 'cc' copies of the emails. Evidently, the criminals (with apparent 'inside' assistance) had opened fraudulent, similar email accounts to the customer's account. They intercepted the supplier's letter, altered it (leaving the managing director's signature), and then sent that on to the customer who returned its letter to a fraudulent email similar to the supplier's.

The criminals then transferred the customer signature to the original supplier letter, and, using an email address similar to the customer's, returned what the supplier thought was its original letter, with an acknowledgment. The supplier contacted the bank where the criminals had opened the fraudulent account. The criminals, who had presented documents showing that they were the supplier's officers, opened the account. The intercepted wire was for \$200,000. In conclusion, only \$500 remained in the account; the criminals were long gone, and the supplier and customer were left to contend, once again, over payment – above and beyond the original quality dispute.

In each of these situations, diligence could have stopped the problem. There also was a question about whether to report to the authorities (no report ever has resulted in successful prosecution). In addition, there was a significant loss of funds, except for one customer's vigilance in one situation, and legitimate questions were also raised about whether a company insider had facilitated part of the theft. Decisions had also to be taken as to whether other customers should be notified of the scams, in case the criminals (having knowledge of the client's operations) targeted other transactions with the client's customers.

How can you then take steps to ensure that your company does not fall prey

'A further benefit of using these email encryption programs is that they provide evidence admissible in court or arbitration that your correspondent actually has received the transmission'

to electronically-based criminal theft?

Consider using email encryption with digital signature for transmitting quotes, receiving all confirmations, and sending invoices. This is the only way to safely take advantage of secure email communication with customers, partners and employees, and there are a number of email encryption programs available which enable authentication of emails and provide assurance that the emails reach and are read by the person(s) you are sending them to.

A further benefit of using these programs is that they provide evidence admissible in court or arbitration that your correspondent actually has received the transmission. Often, disputes over whether a bunker supply incorporates sales terms and conditions, or whether the supplier has received 'no lien' notice, turns on proof that emailed incorporated terms and conditions, or the terms referring to those sales terms, actually reached the customer. Email encryption programs provide means that courts and arbitrators should recognise, confirming that you have sent your terms and that your customer has received them. They will also provide you with a better defence against customers who

later claim that they have responded with acceptances which negate your sales terms. We have seen such responses intentionally directed to lower-level employees, who do not know to report the responses. The responses are raised later, of course, as reason for non-payment or non-compliance with terms for payment or for reporting supposed quality or quantity disputes.

You should also include in your sales terms and conditions express terms for payment, which should include specific bank account wiring information. Although this may initially seem to be offering 'private' information, your banking information will be well known within any customer or supplier organisation you have done any business with, as well as to their bank. It is up to your bank to ensure that no one, with that information, withdraws your funds without authorisation (and the bank is liable to you if they do). Post your sales terms and conditions on your website, and in your sale confirmation and invoices. You should also ensure, of course, that you are using a web provider with adequate security against hackers and who will report back to you quickly about any attempts to modify the website.

Your sales terms and conditions should state expressly that there must be no other payment than by wire to the specific account which your sales terms and conditions specify. You should repeat this both in your stem and in all of your invoices (always remembering that criminals may forge your invoice, as explained above).

Make sure that educate yourself and your employees to spot potential frauds. Look for email addresses or signatures which appear different from known customer emails. A 'spoofer' will write an email appearing to be from an authentic source (perhaps after intercepting a prior email), attempting to gain a response which will reveal information about your mail system and business style. This may be, for example, by way of a request from what seems to be a potential customer, with which you have never done business.

Essentially, train your employees and yourself to be suspicious, particularly at the critical time when the customer wires funds to you, or when you wire funds to a supplier. Not only confirm the wire instructions for your wire receipt, or the address to which you're wiring, but also confirm the identity of the person with whom you are confirming the instructions. Keep in mind that not only are emails 'spoofed', but that telephone numbers, through 'voice over internet protocol', can be hijacked too.

Consider engaging a security and legal audit of your quotation, stem, invoicing,

'More often, however, the crime is uncovered after the bunker parties involved have wired funds to a fictitious bank account which the criminal has set up in the broker's, supplier's or trader's name'

and wire transfer and receipt systems. Cyber criminals are very determined: Norton, the Internet security company, has estimated that cyber criminals steal from one million people each day, and stole from 431 million people in the past year, with an extraordinary \$114 billion either stolen or spent on prosecuting cybercrime in 2013 (these statistics can be found at <http://uk.norton.com/cybercrimereport>).

A legal and security audit will also help identify internal information flows, which may tempt employees to be part of criminal

schemes resulting in electronically-facilitated theft. It will further evaluate your sales terms and procedures for security and enforceability if there is a fraud. Such an audit can include an educational programme for you and your employees about how to detect and deter electronic commerce fraud. Our law firm does, and your insurers may, provide services for such a legal audit and educational programme.

If your company is the victim or attempted victim of an electronic fraud, engage competent legal counsel immediately. That counsel can advise about a proper response,

including how to secure your computer systems and preserve evidence of breach, and about how to detect the source of the theft. Legal counsel also can advise about how to recover funds which have been stolen, including any grounds for claim against a bank which has opened an account to receive a fraudulently-directed wired, or an internet service provider (ISP) which has facilitated the opening of a fraudulent internet email account. Legal counsel also can advise how (and whether) to notify law enforcement officials, and how to notify those customers (and potential customers) which criminals may also be targeting about the fraud and avoiding the fraud. They can also advise on whether a customer who has wired funds to a fraudulent account must still wire funds to your authentic account (and double pay).

There are many legal systems which may be involved in the question of how to respond to a cyber fraud involving payments for a bunker supply, and some may conflict. Competent legal counsel can help sort through those many legal systems to figure out how to respond, and recover from a fraud.

Of course, an investment for prevention is worth far more for a cure. Significant electronically-related fraud is occurring in the bunker industry and, given the international nature of this sector and the frequency and size of transactions involved, it is certain to escalate.

In the early 1930s, during the Depression in the United States, there was a pair of celebrated bank robbers, Clyde Barrow and Bonnie Parker. 'Bonnie and Clyde', like the pirates of the *Maersk Alabama*, even had a movie made about them. While there may never be a movie made about cybercrime and the bunker industry, these criminals and Clyde Barrow do have something in common. After his capture, someone asked Barrow, 'why do you rob banks?' He responded: 'because that's where the money is.'


Make sure cyber criminals don't see your company as 'where the money is'. As this article outlines, you can take a number of relatively straightforward measures to safeguard your business from prying 'cyber' eyes.

STANLEY SERVICES LTD

Suppliers of IFO's and MGO. Your South Atlantic fuelling station for Bunker Fuels to cruise, fishing, oil exploration and research vessels. Available by pipeline at dockside and by tanker-barge. Marine lubricants also supplied.



Stanley Services Ltd
 Port Stanley, Falkland Islands, South Atlantic Ocean
 Phone: 500-22622 | Fax: 500-22623
 Email: rowlands@stanley-services.co.fk

 Steve Simms is a Principal of Simms Showers LLP.

Simms Showers LLP provides customised legal services in the areas of vessel arrest, attachment, bunkers quality and quantity disputes, as well as cybersecurity, to bunker suppliers, traders and brokers worldwide

 Email: jssimms@simmsshowers.com
 Tel: +1 410 783 5795