SIMMS·SHOWERS LLP

INTERNATIONAL PRACTICE. PERSONAL COMMITMENT.

The IBIA Annual Convention – Cancun – 3-5 November, 2015

CYBERCRIME – The Legal Issues

J. Stephen Simms

jssimms@simmsshowers.com

+1.410.783.5795

IBIA INTERNATIONAL BUNKER INDUSTRY ASSOCIATION

Welcome to Cyber-Holics Anonymous

Group Therapy

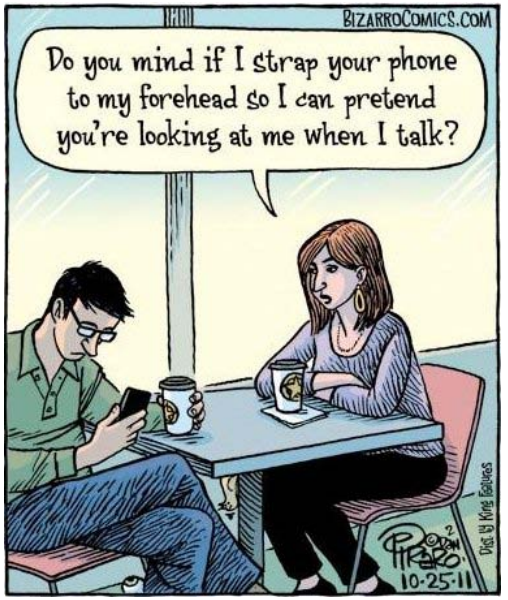
To Start our meeting:

Hi, my name is

_____

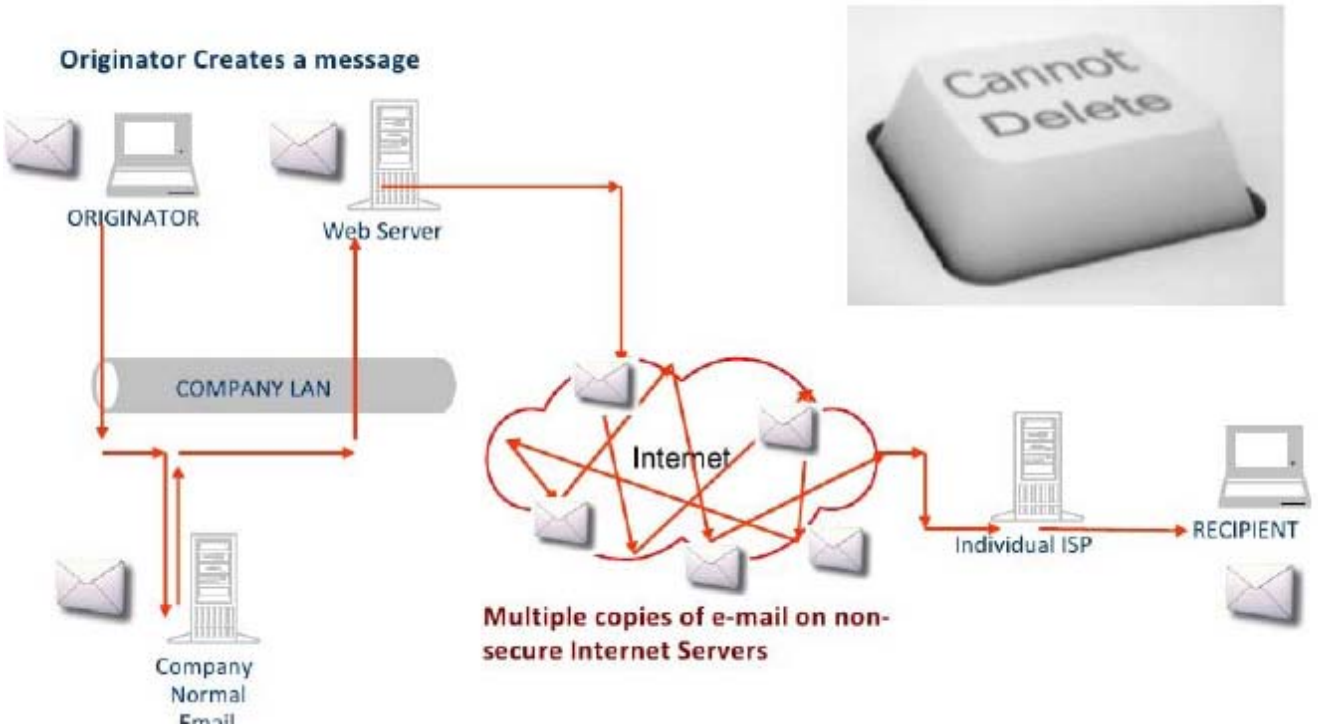
and I'm a cyber addict

("Hi _____")



Not sure?

Intervention: Let's send an email - -



A "Typical" Bunker Stem

1 Inquiry to purchase

2 Enquiry acknowledged

3 Enquiry to Suppliers

4 Quotation or refusal

5 Optimum price option

6 Counter or accept quotation, delivery details, agents name

7 Further possible price negotiations

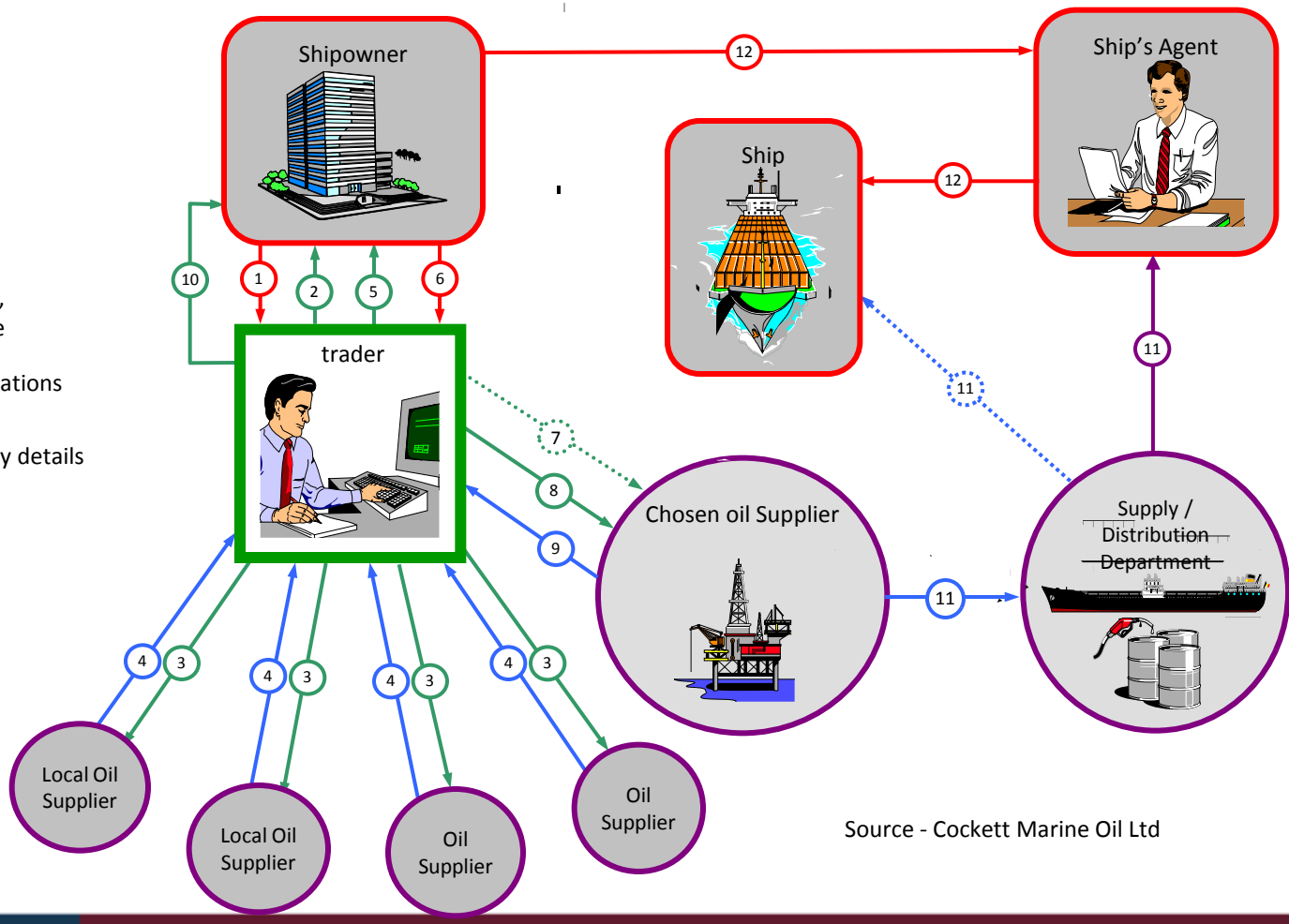
8 Firm nomination plus delivery details

9 Acceptance of nomination

10 Confirmation: nomination placed and accepted

11 Instructions to supply ship, liaise with ship's agent

12 Instructions to ship/ships agent and vessel



Source - Cockett Marine Oil Ltd

CYBERCRIME - - The Legal Issues

From: Monjasa Accounts Dept. <accounts@monjasa.com>
Sent: Wednesday, October 07, 2015 7:53 AM
To: Recipients
Subject: Re:INVOICE FOR MV MY VINASHIP GOLD BUNKER SUPPLIED

Hello,

Attn: Accounts Department
Good day,

We are pleased to attach the following documents for your attention:
- Invoice
- Bunker Delivery Note

The original invoice & BDN will be send out once available.

Best Regards,

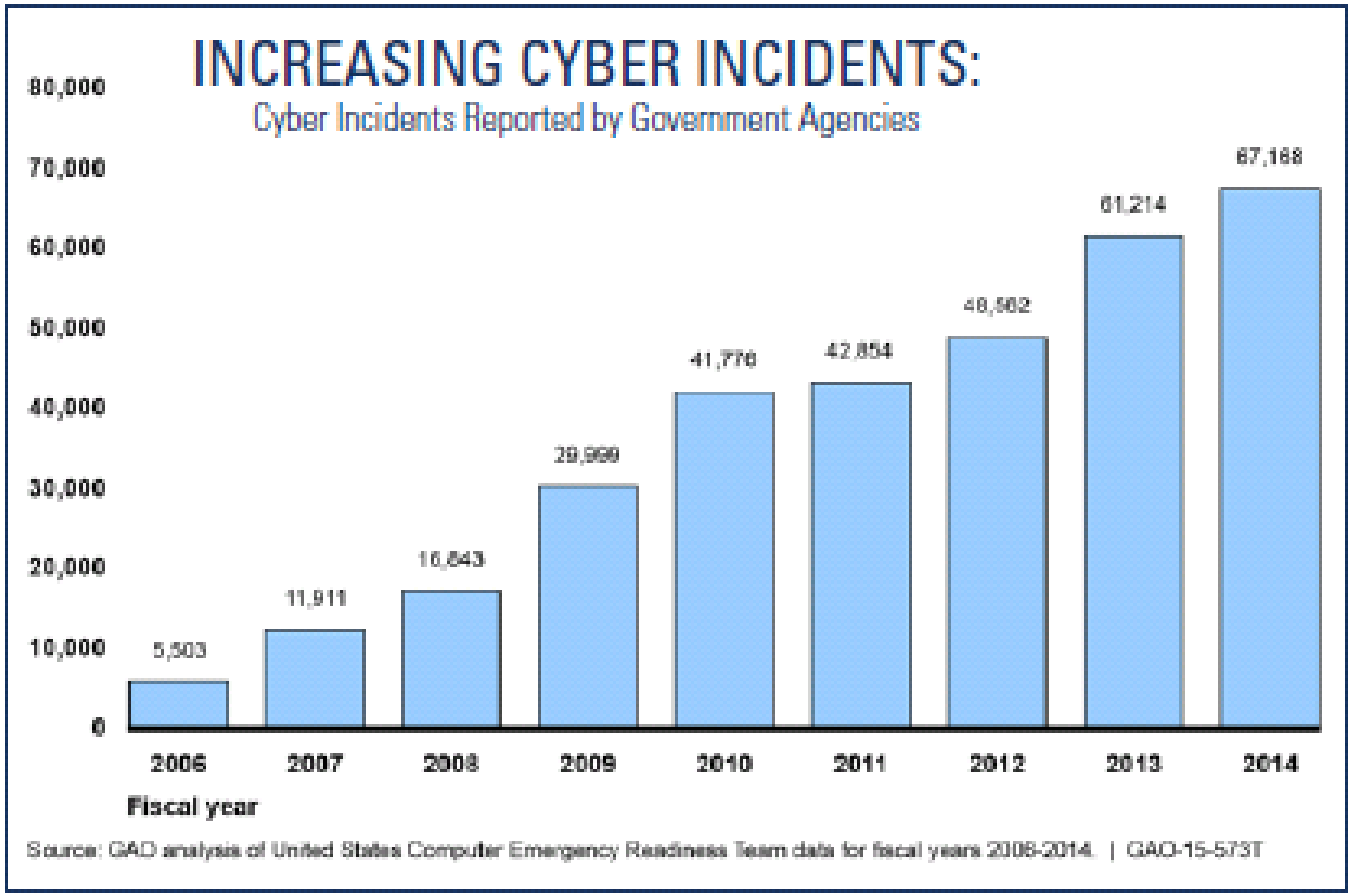
Jeng Wong
Accountant

Direct tel :+65 64 38 4483
Direct email:wj@monjasa.com
Mobile tel :+65 96 189 336
Yahoo ID :soeng_monjasa
Webpage :www.monjasa.com

d0c_scan_2339288.pdf
238K View Download

d0c_scan_2339288.pdf
238K View Download

CYBERCRIME - - The Legal Issues



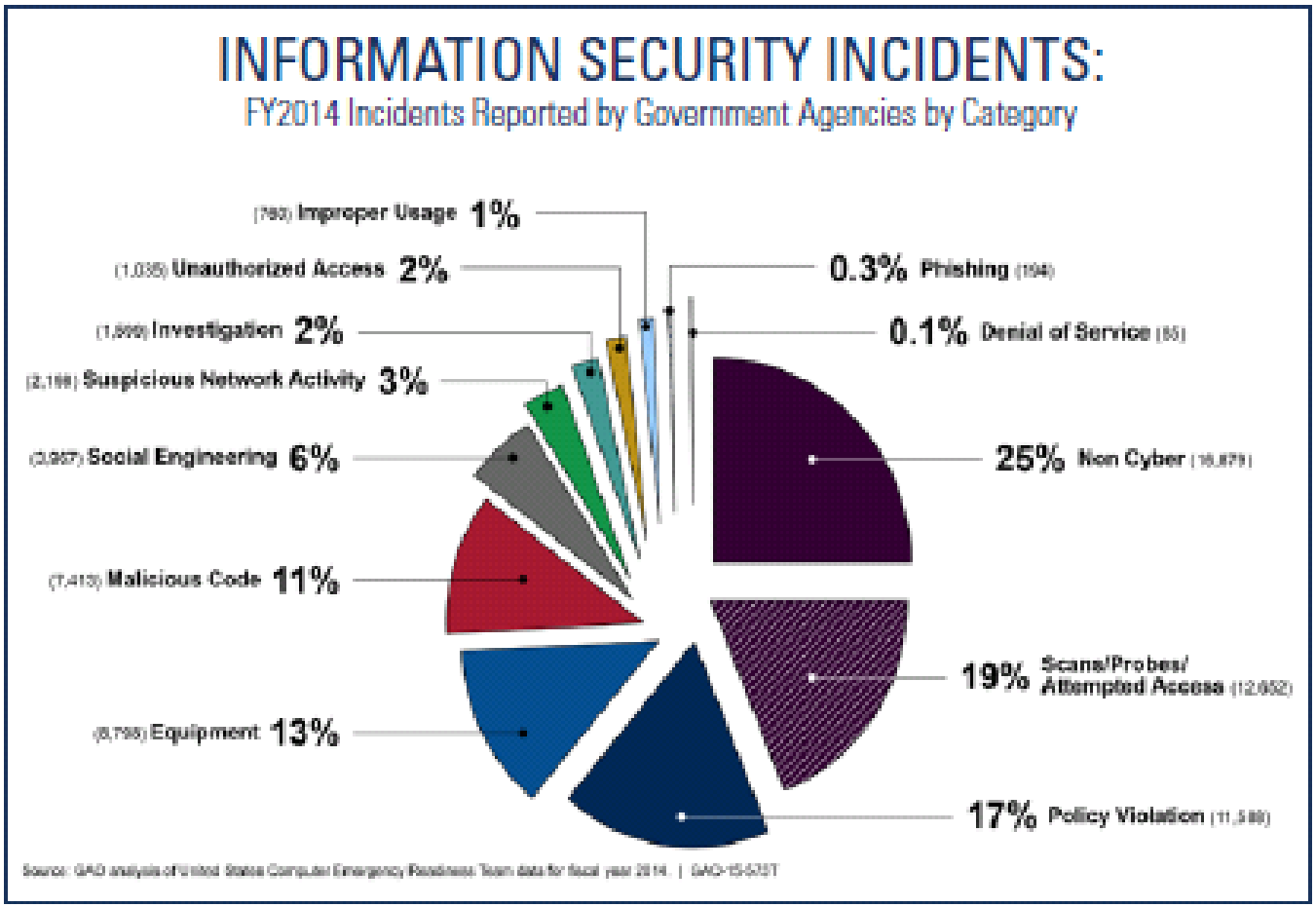
UNITED STATES COAST GUARD

CYBER STRATEGY

JUNE 2015

WASHINGTON, D.C.

CYBERCRIME - - The Legal Issues



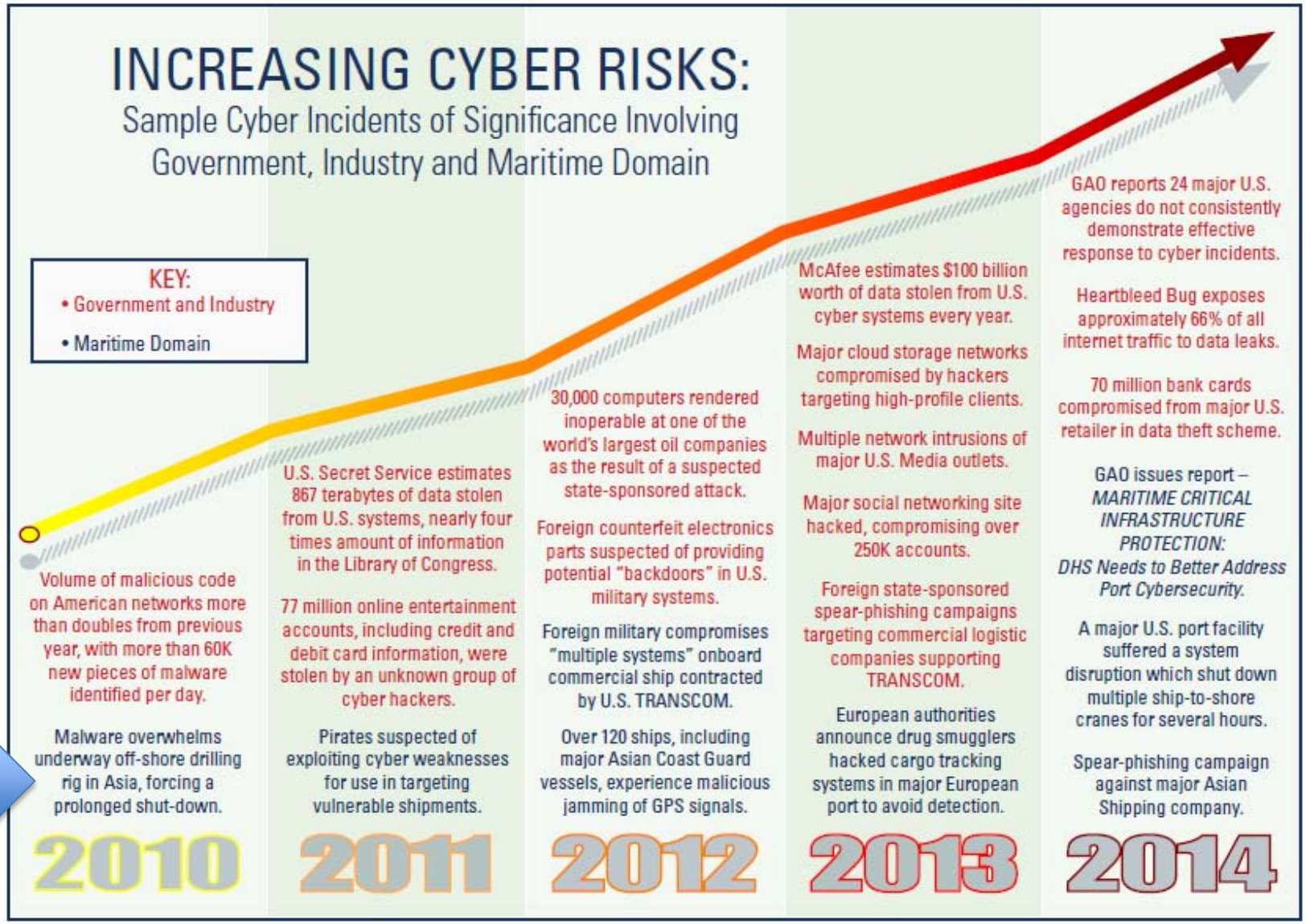
UNITED STATES COAST GUARD

CYBER STRATEGY

JUNE 2015

WASHINGTON, D.C.

CYBERCRIME - - The Legal Issues



As of April, 2015 - - BIMCO, ICS, Intercargo and INTERTANKO are developing standards and guidelines to address the major cyber security issues faced by the shipping industry.

https://www.bimco.org/en/News/2015/04/15_cyber_security_guidance.aspx

The European Network and Information Security Agency published the first comprehensive report on maritime security, in 2011

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts

Case 1:14-cv-05902-PAE Document 1 Filed 07/30/14 Page 1 of 69

JUDGE ENGELMAYER

14 CV 5902

John A.V. Nicoletti
Nooshin Namazi
Kevin J.B. O'Malley
NICOLETTI HORNIG & SWEENEY
Attorneys for Plaintiff
Wall Street Plaza
88 Pine Street, Seventh Floor
New York, New York 10005
(212) 220-3830

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AGCS MARINE INSURANCE COMPANY,

Plaintiff,

vs.

WORLD FUEL SERVICES, INC. and
SERVICES EUROPE, LTD.,

RECEIVED
JUL 30 2014
U.S.D.C. S.D. N.Y.
CASHIERS

COMPLAINT

In good company.
.. UPDATE

September 18, 2015

World Fuel lost more than $17 million worth of marine gasoil ("MGO") to thieves who successfully impersonated the U.S. Defense Logistics Agency. The perpetrators contracted with World Fuel to purchase the MGO, and using a series of fraudulent shipping documents, stole it as it was being delivered off the coast of Lome, Togo to a vessel (the "Ocean Pearl") the perpetrators had "designated." AGCS Marine Insurance Company/Allianz ("AGCS") issued to World Fuel a marine open cargo "all risk" insurance policy (the "Policy") which insured all cargos in which World Fuel entities and affiliates "have an interest." The Policy covers physical loss of the MGO, which AGCS admits occurred here.

NOTE: It is necessary for The Assured to give prompt notice to This Assurer when the Risk Manager or equivalent become aware of an event for which they are "held covered" under this policy and the right to such cover is dependent on. compliance with this obligation.

UNDERLYING FACTS – THE INSURANCE CLAIM

25. Willis submitted a New Marine Claim/Loss Report to AGCS' office in New York on January 31, 2014 describing the nature of the claimed loss as follows:

> WFS [World Fuel] was informed that it was the victim of a scam in which someone impersonated the U.S. Defense Logistics Agency ("DLA") and set up a fake tender/bid offer for the supply of a large cargo of fuel. Believing the bid/tender was legitimate, WFS unknowingly supplied the cargo, and when it sent the invoice to the DLA for payment, they advised that WFS' invoice did not match any official DLA tender. The value of the now mssing [*sic*] cargo is approximately $18M USD.

26. The fake tender referred to by Willis is a Request for Quote that was purportedly issued by DLA Energy PEA on October 28, 2013 seeking a quote for, among other items, one

Present status – still in court – summary judgment

AS AND FOR A SECOND CAUSE OF ACTION

53. AGCS repeats and realleges each and every allegation set forth in paragraphs "1" through "52" of this Complaint with the same force and effect as if

54. The nature of the compl

purported buy

wo here. Nor was there "delivery" to a legitimate purchaser or "destination." In any event, World Fuel believes undisputed facts will establish that the loss occurred before the MGO was "delivered in tanks" on the Ocean Pearl as the bulk liquid clause states. In fact, the MGO was lost the moment it crossed the flanges of the supplier vessels to enter the hoses between those vessels and the Ocean Pearl. Thus, it was lost before it reached the Ocean Pearl tanks. E.g., Int'l Multifoods Corp., 309 F.3d at 84 ("'loss' if never remedied is the loss of control that occurs upon a dispossession")

resu

for th

$18,000,000?

CYBERCRIME - - The Legal Issues

Bunker Suppliers / Traders / Brokers are Targets!

- Bunker Case Studies
- Prevention – and Potential Liability
- Detection
- Conclusion

Case Studies -

(Friends') Experiences to share?

Case: Trader confirmed a stem . . . placed a delivery order with a physical supplier, which the trader did not ordinarily use . . . **Offering a below-market price for the delivery.**

Trader received an emailed invoice from what appeared to be the physical supplier. As the trader had done hundreds of times before, the **trader forwarded the emailed invoice to the trader's bookkeeping staff** - - who quickly executed a wire to the instructions from the supposed physical supplier.

Not long afterwards, the trader received another email, **which was an authentic one** from the actual physical supplier, including an authentic invoice containing the physical supplier's correct wire information. The supplier identified the first wire instructions as fraudulent, but the trader protested against paying again to the supplier's authentic account.

When **the supplier threatened to arrest the customer's ship for non-payment**, the trader reluctantly paid again to the physical supplier's correct account.

$80,000

Case: The broker completed the delivery to the customer though the physical supplier.

Again using email, the broker emailed an invoice to the customer, 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 detected the fraud. The customer made one payment, to the broker's correct account, not even expecting the discount.

Diligent Customer – No Loss

Case: In a third and most sophisticated version, the supplier was involved in a quality dispute with the customer and the customer refused to pay. There was an extended set of **email exchanges** between the parties, including of detailed testing information and each side's position on the claims.

Finally, the supplier and customer agreed to settle the dispute, and the supplier emailed the customer with a letter in PDF format stating the settlement terms and wiring instructions for the settlement amount, which included the imaged, physical signature of the supplier's Managing Director. The customer insisted 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 forged letter to acknowledge settlement, wired funds to the fraudulent bank account, and then returned the signed, forged letter in PDF format via email to what it thought was the supplier's email address.

(Case, contd.)

This letter, too, was **intercepted**, and the bank account information changed to reflect the correct wiring instructions, and not the fraudulent bank account, before it was received by the supplier.

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 the 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. Examination of emails showed slight alterations of some of the "cc" copies of the emails.

Evidently, criminals (with likely "inside" assistance) had created fraudulent email accounts using domains similar to the supplier's and the customer's. They intercepted the supplier's letter before it reached the customer, altered the wiring instructions, and sent through the forged letter to the customer.

(Case, contd.)

After the customer executed the forged letter, it was sent to a fraudulent email address where the **criminals transferred the customer signature to the original supplier's letter**, and using an email address similar to the customer's, returned what the supplier thought was its original letter, with acknowledgment.

The supplier contacted the bank where the criminals had opened the fraudulent account and **learned that criminals presenting documents showing that they were the supplier's officers had opened the account with $50,000**.

The intercepted wire was for $200,000; only $500 remained in the account, the criminals were long gone, **and the supplier and customer left to contend, once again, over payment**, this time with an issue in addition to the original quality dispute.

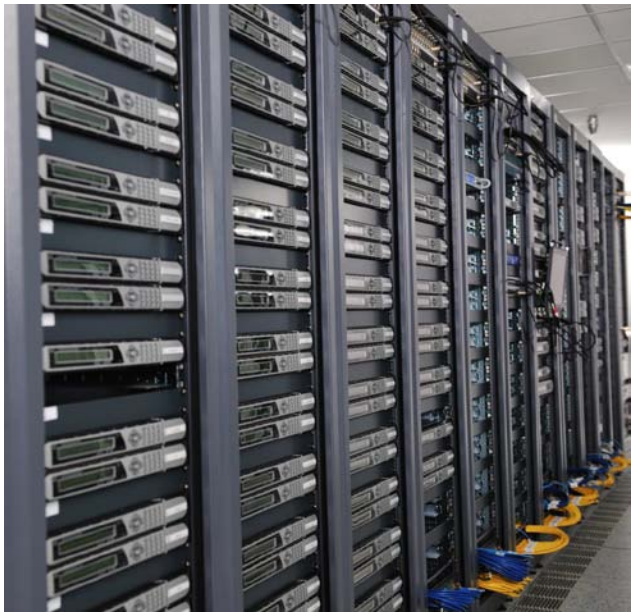
Loss - $200,000

Definitions

- Cyber Security – protecting computers, networks, and data from unauthorized access and other vulnerabilities through prevention and detection
- Cyber Crime – any crime involving a computer or network, such as:
  - Illegal access / interference
  - Theft of data
  - Identify theft / fraud

Areas of Risk

- Individual Computers
- Internal Network
- Servers
- Mobile Devices
- Email Communications
- Websites

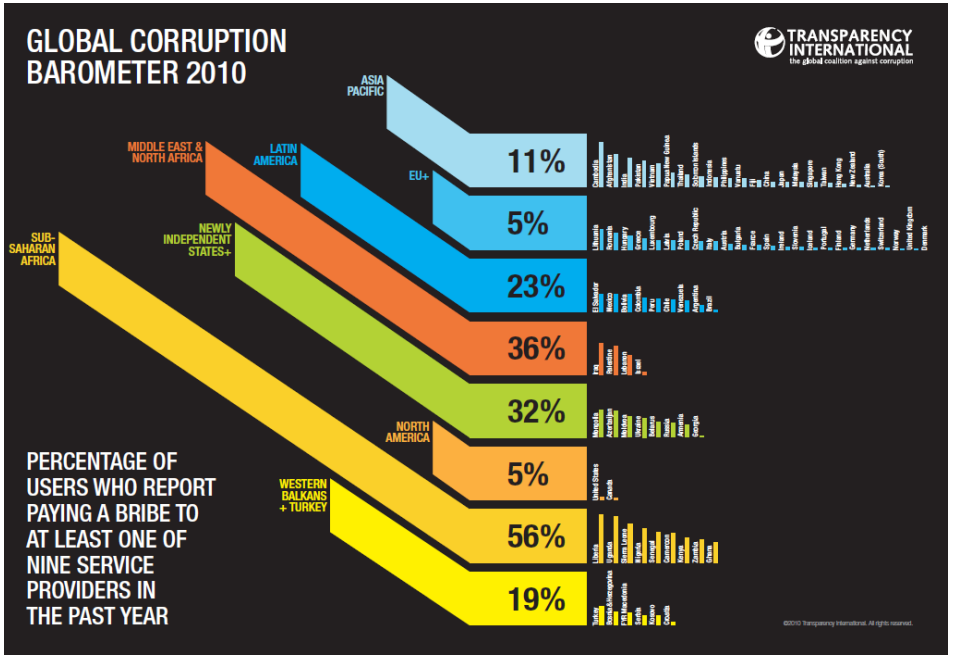


Types of Threats

- Viruses / Worms / Trojan Horses
- Identity Thieves
- Spyware
- Hackers
- Web Jacking

Bunker Suppliers / Traders / Brokers as Targets

- Volume of Transactions
- Amounts at Stake
- Parties Involved
- Geography



CYBERCRIME - - The Legal Issues

Federal Trade Commission v. *Wyndham Worldwide Corporation, United States Court of Appeals, Third Circuit, August 24, 2015*

- Lack of firewalls and other cyber security measures may be an unfair business practice by a hotel chain in violation of the Federal Trade Commission Act (FTCA)

- The Court acknowledged the agency's interpretation of its authority under that statute

Potential Civil (Monetary Fines) Liability:

Federal Trade Commission v. *Wyndham Worldwide Corporation, United States Court of Appeals, Third Circuit, August 24, 2015*

Wyndham:

- **allowed its hotels to store payment card information in clear readable text;**
- **Permitted employees to use easy-to-guess passwords to access its property management systems;**
- **Failed to use firewalls and other "adequate information security policies and procedures";**

Potential Civil (Monetary Fines) Liability:

Federal Trade Commission v. *Wyndham Worldwide Corporation,*
United States Court of Appeals, Third Circuit, August 24, 2015

- **Inadequately restricted third-party vendors' access to its network and servers;**
- **Failed to take "reasonable measures to detect and prevent unauthorized access" to its computer network; and**
- **Did not follow "proper incident response procedures," allowing hackers to use similar methods in each attack**

Potential Civil (Monetary Fines) or Criminal Liability: U.S. Maritime Transportation Security Act of 2002 (MTSA) - - enacted following 9/11:

Grants the United States Coast Guard broad jurisdiction and authority over any "incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area."

CYBERCRIME - - The Legal Issues

The USCG, however, may soon formulate a Navigation and Vessel Inspection Circular (NVIC) offering "guidance" as to how cyber risk management fits into MTSA.

- **Noncompliance could serve as a basis for imposing civil or perhaps even criminal penalties, in addition to the liabilities or losses incurred from the underlying event.**

Now, the USCG views cyber risk "prevention" and "response" as operational responsibilities of management

- **Maritime companies may be expected to establish an effective cyber risk management program: continuous assessment, coordinated planning, investment, training**

Prevention

- Networks / Servers / Computers / Devices
  - Firewalls (networks)
  - Antivirus / Antimalware
  - Restricted Access
  - Security Settings
  - Strong Passwords
  - Backup Data
  - Operating System / Software Updates
    - Windows XP / Office 2003

Prevention (cont.)

- Email Communications

  - Encryption
  - Distribution List
  - Telephone / Facsimile Confirmation

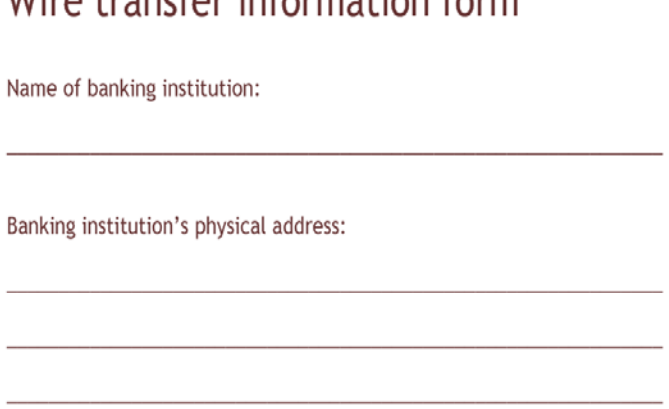
Prevention (cont.)

- Websites / Browsers
  - Browser Settings / Cookies
  - Personal Information
  - Pop-up Blockers
  - Anti-Phishing
  - Privacy Policies

SIMMS·SHOWERS LLP
INTERNATIONAL PRACTICE. PERSONAL COMMITMENT.

Prevention (cont.)

- Terms and Conditions
  - Express Payment Terms
  - Bank / Wiring Information
  - Website
  - Single Point of Contact
  - Notice to Customers
- Legal / Security Audit


Wire transfer information form

Name of banking institution:

Banking institution's physical address:

Detection

- Networks / Servers / Computers / Devices
  - Virus / Malware Detection
  - Suspicious Computer Activity
- Email Communications
  - Email Addresses
  - Banking / Wire Information Notices

Responding to Cyber Crime

- Engage Competent Legal Counsel
- Preserving Evidence
- Criminal Investigation
- Recovery Stolen Funds
- Customer Notification

Conclusion

- Evolving Nature of Threats
- Current Technology / Policies
- Adaptable Prevention / Detection Strategies

Simms Showers LLP has assisted their clients to recover over U.S. $100 million in assets in successful maritime recovery actions throughout the United States and abroad. The Firm arrests vessels and proceeds on maritime attachments and garnishments, and possessory actions, in jurisdictions throughout the world, and its attorneys are available to clients on a 365 day, 24 hour basis to serve its clients with that. Further information about Simms Showers LLP is at www.simmsshowers.com.

Steve Simms
jssimms@simmsshowers.com
Office 410-783-5795
Mobile 410-365-6131