UNECE-OSCE

Inland Transport Security Discussion Forum
"Securing Global Transport Chains".
Session 1a - Cyber crime against transport

Geneva, 17.6.2016

Dr. Juha Hintsa
Cross-border Research Association
Lausanne, Switzerland
juha@cross-border.org, tel +41-76-5890967

Cyber risks are inextricably linked to the Confidentiality (C), the Integrity (I) and/or the Availability (A) of data – the so-called CIA triad.

- The Confidentiality of the information ensures that the only persons who can access the information are those for whom it is intended.
- The Integrity of the data is ensued if the right data are linked to the right records.
- The stored data must be Available when required.

Source: Vanbreda 201x

Typical actors and motivations behind Cybercrime

- Criminals / organized criminal groups

- Terrorists

- Hacktivists

- Malice

- Nation states

Source: Marsh 2015

Examples of potential Cyberattacks in the transport sector

- Hacking a freight forwarder's system;
- A Distributed Denial of Service (DDOS) attack;
- Installation of ransomware;
- 'Portables' (mobile phones, tablets etc.);
- Espionage and competition.

Source: Vanbreda 201x

Examples of key Cybercrime risks in the transport sector

- Physical asset damage and associated loss of use.
- Unavailability of IT systems and networks.
- Loss or deletion of data.
- Data corruption or loss of data integrity.
- Data breach leading to the compromise of third-party confidential information, including personal data.
- Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information.
- Extortion demands to cease a cyber attack.
- Direct financial loss as a result of theft.
- Damage to reputation.

Source: Marsh 2015

Road cargo transport market in the EU

- €300 Billion EU road transportation market
- 2 Million trucks and 3 Million workforce
- 600.000 transport companies, most smaller than 10 people
- 72% of all inland transport is done on trucks

Source: Palleter 2016

14.8.2010 - Fraud via electronic freight exchange systems, EU

By Wim Dekeyser, International Loss Adjusters, the Netherlands

- *The last weeks we have been confronted again with a new wave of fraudulent practices by the use of online freight exchange systems, this time in Eastern and Central Europe (with fake Slovakian carriers)*
- *Unidentified persons try by the use of the name of several carriers in good faith to obtain transport orders via on line freight exchange systems.*
- *The shipments are subsequently collected and disappear.*
- *We can only advice you to not entrust transports to companies using exclusively mobile phone numbers and anonymous e-mail accounts (such as gmail, hotmail or live); but to check always with their official coordinates.*
- *Extra vigilance is required as at the occasion of the last wave one goes one step further producing falsified letterheads, transport licenses, insurance certificates etc.*

http://eb-iaati.org/news/entry/fraud_via_electronic_freight_exchange_systems

Aug.2012: Research into freight exchange fraud in the Netherlands (1/2)

The consequences of freight exchange fraud are numerous:

- When goods are lost insurance companies try to recover the losses by approaching the carrier.
- Because of the low margins in road haulage a small carrier will not be able to pay the compensation claims which might lead to bankruptcy.
- Economically, loss of goods can lead to delayed production.
- Furthermore trust within the sector will diminish creating high barriers for new entrants.
- Current trends show that insurance companies consider excluding insurance of losses caused by usage of the freight exchange.

Aug.2012: Research into freight exchange fraud in the Netherlands (2/2)

For a criminal organization the existence of the freight exchange makes high value/ low risk criminal activities possible:

- Governments do not prioritize this type of criminal behavior and therefore police attention stays limited as consequence which is a stimulus for criminals to continue this type of crime.
- Criminals are able to improve their working methods and keep up with the latest trends, which is enhanced by the low priority given to this type of crime.
- Modern techniques such as access via mobile apps to the freight exchange hinder the, slightly lagging behind, police in identifying the perpetrator.

27.6.2014: Insurance specialist warns of fast-growing trend for criminals to target carriers, terminals and other transport operators, EU

- *The freight transport sector is increasingly at risk from cyber-criminals targeting carriers, terminals and other operators to access data on high-value cargo and susceptible loads.*
- *TT Club's Mike Yarwood told the conference: "We see incidents which at first appear to be a petty break-in at office facilities… post incident investigations, however, reveal that the 'thieves' were actually installing spyware within the operator's IT network."*
- *More commonly targets are individuals' personal devices, where cyber security is less adequate, he observed.*
- *"Awareness is often the first step," commented Yarwood. "Education of employees across all disciplines of the organisation is crucial… Often the level of threat is dependent on an organisations' own culture," he concluded.*

https://www.securecargo.org/news/freight-increasingly-at-risk-from-cyber-crime

29.7.2015: 'It fell off the back of the Internet': Freight thieves are becoming cybercriminals, US

- A new generation of tech-savvy truck thieves are innovating on old methods.
- "One of the M.O.'s that's on the increase is in a sense identity theft—impersonating another company," says Nick Erdmann
- The tactic is known as a fictitious pickup… canny thieves can spot the valuable ones based on certain details: Loads requiring high insurance minimums, loads requiring a team of drivers, or loads coming out of particular locales, such as technology corridors.
- Then, using falsified credentials to pose as legitimate truckers, criminals contract to carry the load, drive their own truck to a warehouse or distribution center, and simply pick it up.
- "People just hand it over," says Detective Eric Dice, who heads a cargo theft task force in Florida. "It's amazing."
- The average value of a load lost to a fictitious pickup was more than $140,000 in 2014.

http://fortune.com/2015/07/29/cargo-freight-thieves-cybercriminals/

18.9.2015: Cyber Risks on the Rise for Transportation – What to do about it? (Canada)

Where trucking is concerned, Descartes's Foroughi offers some IT security tips for trucking companies:

- *Always run supported software, operating systems and hardware and apply patches in a timely manner with a tool that can automate the process and provide compliance reporting;*
- *Train your staff in security concepts;*
- *Run a centrally-managed antivirus program that updates signatures frequently and protect all Operating systems;*
- *Collect and correlate your log sources for global awareness is essential;*
- *Have frequent backups and disaster recovery plans;*
- *Scan your environment for vulnerabilities frequently, and remediate the findings.*

http://cantruck.ca/cyber-risks-on-the-rise-for-transportation/

Insurance policies in the context of transport Cybercrime

Professional Indemnity / General Liability – Crime – Property insurance coverage

Coverage	None	Partial	Cover
Management assistant in an insured event	X		
Notification and communication costs	X		
PR costs (reputational protection)	X		
Cost of reconstructing own and 3rd party data		X	
Investigation and tracking costs	X		
Loss of profits + additional costs		X	
Legal cost with a supervisory body	X		
Defense + damages (liability)			X
Compensation			X
Ransom money in case of extortion			X
Cyber theft			X
Telephone switchboard hacking			X

Source: Vanbreda 201x