Best practices as proposed by FIATA

PREVENTION OF CYBERCRIME

fiata.com

DISCLAIMER

It should be borne in mind that this document does NOT include any legal advice. It is suggested that readers seek advice from legal professionals if they have any question about data-protection laws or other legal-related topics.

It should be noted that these best practices mainly include general guidelines from a risk-management perspective, not technical advice. Companies should adjust and implement the recommended measures based on its specific corporate structure, business models and risk management requirements, as well as seek advice from national authorities, FIATA Association Members or technical experts for technical assistance.

FIATA accepts no responsibility whatsoever for the consequences of the use of the information contained in this document.

For further information about the activities of FIATA Advisory Body Legal Matters or to make comments about this guide, please contact the FIATA Secretariat info@fiata.com

Best practices as proposed by FIATA

PREVENTION OF CYBERCRIME

FIATA Advisory Body Legal Matters (ABLM) has produced this best practice guide to assist both FIATA Association Members and Individual Members as well as the global logistics and freight forwarding industry at large.

Legal issues are key for those operating in the area of freight forwarding whether in their own jurisdiction or internationally. Keeping forwarders advised of legal developments around the world is therefore of prime importance for ABLM as is advising the association of action it may take in relation to legal developments to protect the interests of its members.

ABLM has 12 members and many co-opted members from around the globe, all of whom are experienced law practitioners, professors or active freight forwarders. ABLM meets two times a year at the HQ Session in Zurich and at the Annual World Congress, both are open sessions welcoming the participation of global forwarders.

Issue experts in ABLM have reported to FIATA members in the past several ABLM sessions the increase of cybercrimes in the industry. Participants in the sessions showed great interests to the topic and requested advices in lowering risks for cyber-attacks.

The risk of cybercrime to the international transport and logistics industry is increasing in conjunction with the growing application of information technology. Customer-, price-, and transport-data are being stored increasingly digitally today as logistics service providers are becoming data-driven organisations, which however also increases the likelihood of an attack on the digital infrastructure.

The past years witnessed a series of reports on cyber-attacks to leading enterprises in the industry, causing severe delay in the supply chain and financial loss. It should be noted that most of these enterprises are not direct targets of these attacks, but random victims. In case the attack breaks through, the enterprises need to devote substantial amounts of time and capital to stop the attack, inform clients, rearrange the supply chain and make up for other consequences.

Legislation in many jurisdictions now expressly stipulates that enterprises should protect confidential data and/or personal data. For instance, the EU General Data Protection Regulation (GDPR) requires holders of personal data of EU citizens to take certain measures in processing and transferring data, and to notify customers and authorities in case of serious data breaches. International logistics providers and freight forwarders are very likely to fall within the application scope of this legislation as they hold data on customers and shipments.

In view of requests from FIATA membership, the threats brought by cybercrime and requirements from new government policies and legislation, ABLM has prepared this document to raise awareness among FIATA members and the industry regarding the threats and risks of cybercrime, to recommend measures for assessing and mitigating the risk exposure and to suggest best practices in prevention of cybercrime.

FIATA's special thanks go to Mr Michael Yarwood of TT Club who made fundamental contributions to this paper.

EXECUTIVE SUMMARY

Cybercrime is a risk from of failure of information technology systems. It may take various forms, such as phishing, spear fishing, malware, mandate fraud or ransomware.

There have been many cyber-related incidents reported in the last 5 years, with a smaller number of very high profile cases within the logistics and freight forwarding sector.

With current business relying substantively on IT systems, disruption in or suspended operation of IT systems, breach in customer and shipment database can dramatically disrupt shipment operations, communication with clients, carriers and sub-contractors, resulting in monetary losses and possible legal liabilities.

Logistics service providers and freight forwarders are advised to:

- **Assess the risk exposure**: identify areas potentially exposed to a cyber-attack and operational vulnerability, in both information technology (IT) systems and operational technology (OT) systems
- **Adopt technical standards** such as ISO/IEC 27000-series standard or any national standards on information security for the logistics industry
- **Adopt general prevention measures** if any specific technical standard is unable to be implemented, such as:
  - ✓ Implementing layers of defence, such as physical security of hardware, management procedures, firewalls and architecture, computer policies, account management, security updates and antivirus solutions
  - ✓ Limit access to information within a company to a need-to-know basis
  - ✓ Adopt segregation and protocol-aware filtering techniques to protect critical systems
  - ✓ Employ network hardening measures, ensure patch management is adequate and proactively reviewed
  - ✓ Employ a removable device policy, for access and use of devices like USBs
  - ✓ Vet third party providers to ensure cyber security compliance
- **Develop business continuity plans** in the event of the need to respond to an attack
- **Implement measures to detect a cyber-attack** as quickly as possible
- **Form an emergency response team** with key personnel nominated
- **Organize constant training of the staff**: conduct frequent awareness briefings and training programmes to educate all employees on best practices, ensure that the regulatory requirements are known, understood and addressed
- **Ensure suitable insurance is in place** to provide business with a degree of protection

WHAT IS CYBERCRIME?

Cybercrime is defined by the Institute of Risk Management as "any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems."

The scope of the risk exposures related to cybercrime is far reaching, including persons infiltrating an organisation's IT systems, weaknesses in an organisation's procedures and people. Cyber-attacks may take any number of forms, common examples are phishing, spear fishing, malware, mandate fraud and ransomware.

Cyber-attacks can be extremely harmful for an organisation and results not only in large financial losses but also irreparable reputational damage and, through denial of access to services. They also can prevent a business from operating effectively to meet its customers' needs.

THE THREAT IS REAL

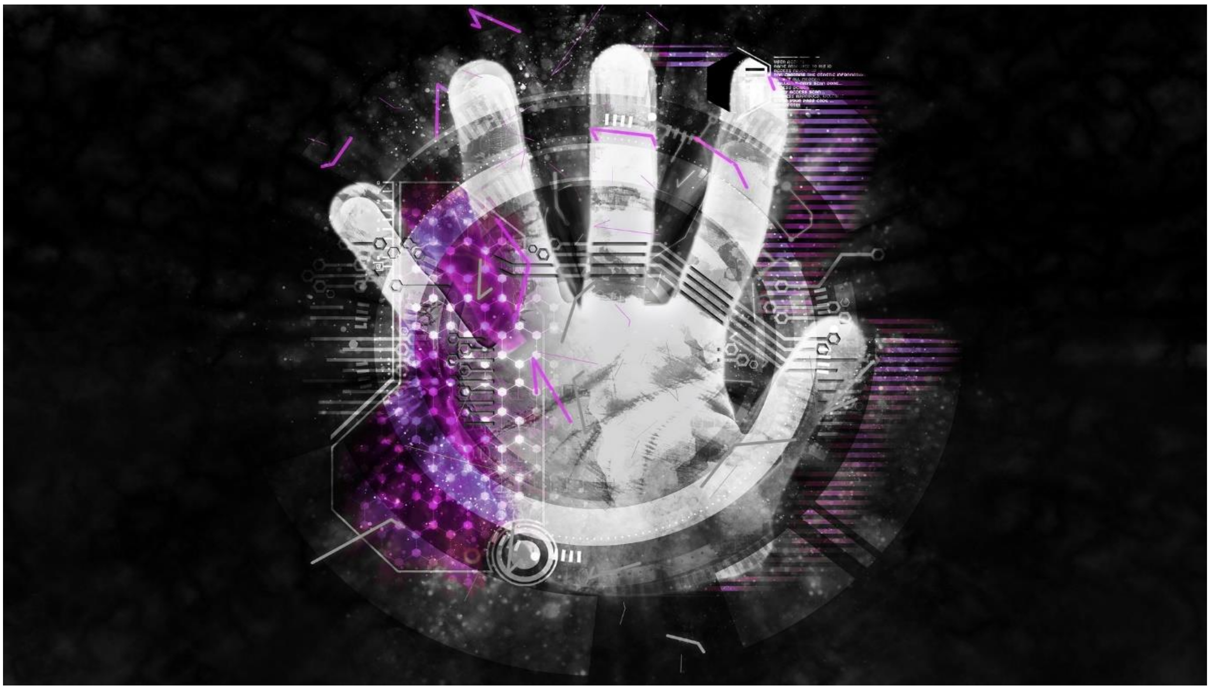
There have been many cyber-related incidents reported in the last 5 years, with a smaller number of very high profile cases within the logistics and freight forwarding sector.

Cyber incidents vary from unsophisticated mandate fraud scams through ransomware attacks to targeted attacks on specific IT infrastructure. There is no one-size-fits-all solution to this risk exposure. It should be highlighted that the majority of cases to date have not been targeted attacks.

The means to undertake such an attack is also now becoming less expensive and more accessible. Cyber criminals are able to purchase from the dark web Cyber-crime-as-a-service products, which act as an enabler where the criminal has limited technical capability.

In June 2017, A.P. Moller Maersk became a victim of an untargeted global malware attack known as "NotPetya". The impact on business activities was wide spread, impacting online cargo booking, general email correspondence and the ability to communicate with customers as well as operational challenges at as many as 76 port terminal operations globally. Whilst Maersk was able to recover quickly from the attack, it was reported to have had a financial impact of several hundred million dollars.

Businesses in the 21st Century are heavily reliant on their IT infrastructure. Many personnel have never known the former manual operation and so are entirely reliant upon the automation and efficiencies the IT infrastructure brings. The logistics and freight forwarding sector is a potentially vulnerable target given its service-based global nature and reliance on IT systems.



PERPETRATORS: MOTIVATIONS AND OBJECTIVES

There are a number of perpetrators of cybercrimes, all of whom have personal motivations and objectives. It is useful to outline these groups and their motivations to better consider the threat of cyber-attacks posed to your business.

Group	Motivation	Objective
Activists (including disgruntled employees)	• Reputational damage • Disruption of operations	• Destruction of data • Publication of sensitive data • Media attention • Denial of access to IT systems
Criminals	• Financial gain • Commercial espionage • Industrial espionage	• Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transport of cargo • Gathering intelligence for more sophisticated crime (theft)
Opportunists	• The challenge/ kudos	• Getting through cyber security defences • Financial gain
States/ state sponsored organisations/ terrorists	• Political gain • Espionage	• Gaining knowledge • Disruption to economies and critical national infrastructure

THE PRIMARY RISKS

Business disruption

This is arguably the largest risk in relation to a cyber-attack. Such attacks can prove to be extremely disruptive where complex business activities are concerned. Denial of services and access to customer information, email systems, phone systems, the internet, information databases, booking software, tracking software and EDI services can quickly cause great operational difficulties. A denial of services attack could also negatively impact your sub-contractors or tenants where they are afforded access to your systems. This highlights the importance of having a robust business continuity plan in place.

Cost

There will inevitably be an upfront financial cost in managing a cyber-attack. Whether replacing or updating computers and systems or having to pay for experts to assist in overcoming the challenges faced, the upfront costs can be unexpected and high.

Financial loss

The motivation of many untargeted cyber-attacks is to extort money. Using denial of service ransomware, an attacker is able to leverage a ransom payment in return for granting access back to IT services. Internet enabled mandate fraud can also result in large financial losses to a business.

Reputational damage

A cyber-attack on your business will undoubtedly have an impact on your customers. The effect could be direct in terms of the impact on the services that you are able to provide in the immediate aftermath, through to the potential of the attack infecting your customers' systems. Whilst overcoming the practical impact of a cyber-attack may take a matter of days or weeks, reputational damage and loss of confidence in your business has the potential to last for many years.

Loss of Intellectual Property

Businesses digitally retain a huge volume of IP, ranging from confidential customer information and commercially sensitive data to product specific information. Theft of such information as a result of a cyber-attack is a real threat.

RELATIVE REGULATIONS

National, regional and international regulations to protect businesses from cyber-attacks continue to develop, for instance:

- EU General Data Protection Regulation (GDPR) *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en*
- EU Directive on the security of network and information systems (NIS Directive) *https://www.ncsc.gov.uk/topics/nis-directive*
- IMO Resolution MSC.428 (98) *http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf*

WHAT TO DO?

The International Maritime Organization (IMO) framework suggests that the cyber-attack risk should be approached using the following framework:

- **Identify**: define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that pose risks to operations if disrupted.
- **Protect**: implement risk-control processes and contingency planning to protect against a cyber event and ensure continuity of operations.
- **Detect**: develop and implement activities necessary to detect a cyber-attack as quickly as possible.
- **Respond**: develop and implement activities and plans to provide resilience and to restore systems necessary for continued operations.
- **Recover**: identify measures to back up and restore systems necessary for any affected operations. A proactive approach should be taken when considering this particular risk exposure.

Assess the risk exposure

As highlighted by recent cases, the logistics and freight forwarding industry is not immune from cyber-attacks. When they do occur, they have the potential to inflict high consequences on a business. It is essential therefore to give due consideration to assess this risk and prepare your business accordingly.

It is recommended that businesses should check:

- ✓ Any areas where they are potentially exposed to a cyber-attack and any consequent operational vulnerability.

- Vulnerability assessments of all systems should be conducted to identify those systems critical to the business, understand the potential exposures faced by each and the impact on overall business continuity in the event of a cyber-attack.
- Businesses should consider to check both information technology (IT) systems and operational technology (OT) systems.

> IT systems refer to the technology used for information processing that include software, hardware and communications software. OT systems however refer to hardware and software used to detect or cause a change through monitoring and control of physical devices and processes. This is found in cyber-physical systems including RF communications, navigation systems, cargo handling and terminal operating systems.

- Businesses may take reference from ISO/IEC TS 27008, *Information technology – Security techniques – Guidelines for the assessment of information security controls*, which provides guidance on assessing the controls in place to ensure they are fit for purpose, effective and efficient, and in line with company objectives.
- Conduct comprehensive threat assessments to determine the threat landscape and understand the potential attack surface faced by logistics facilities.

✓ Whether business continuity plans are in place in the event of the need to respond to such an attack.

✓ Whether key personnel are nominated to be in charge of daily maintenance of the IT systems and OT systems, detection of cyber-attacks and, in case of attacks, to form an emergency response team.

✓ Whether both key personnel and staff are suitably trained and aware of their responsibilities in terms of cyber security measures, the immediate response and the escalation procedure within the business in order to trigger a timely response.

✓ Whether the regulatory requirements are known, understood and addressed in order to protect the business.

✓ Whether suitable insurance is in place to provide the business with a degree of protection.

Prevention measures

Whilst not exhaustive, below is a list of preventative strategies that could be considered by businesses. Businesses are suggested to adopt relevant technical standards, national or international, to establish a relatively high protection level. For companies that may not have sufficient technical or financial capacities at present, the general prevention measures below are advised.

- **Adopt technical standards on information security management:**

  1) ISO/IEC 27000-series
     ISO/IEC 27000-series comprise information security management system (ISMS) standards published by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

The series lay out the specifications for management systems that intend to bring information security under explicit management control. Best practice recommendations on information security management included in the series can help an organisation in managing the security of assets, such as financial information, intellectual property, employee details or third-party information.

2) National standards for information systems

Some states have developed technical standards for information systems, or more specifically for logistics enterprises. Business may seek assistance from FIATA Association Members[1], authorities or technical experts, in implementing such standards.

- **Adopt general prevention measures:**

  ✓ Implementing layers of defence, starting with the outermost layer of physical security, followed by management-level procedures and policies, firewalls and architecture, computer policies, account management, security updates and finally antivirus solutions.

  ✓ Operating a least-privileged principle, where information and access is limited to a need-to-know basis.

  ✓ Employing network-hardening measures, ensuring patch management is adequate and proactively reviewed.

  ✓ Employing segregation and protocol-aware filtering techniques to protect against cyber threats that might affect critical systems.

  ✓ Employing a sound removable device (e.g., USBs, laptops) policy with provisions to ensure all USBs are encrypted and tested for viruses prior to being used with other devices.

  ✓ Developing business continuity plans, identifying key personnel and establishing processes from both technical and commercial perspectives to prevent the negative impact of a cyber-attack from further expanding and recover business operation.

  ✓ Organizing frequent awareness briefings and training programmes to educate all employees on best practices. These can cover installation and maintenance software while avoiding infection and propagation, safeguarding user information and the treatment of cyber physical threats such as the presence of any third party.

  ✓ Vetting of third party providers to ensure cyber security compliance.

Useful documents for further reading:

- *The Guidelines on Cyber Security Onboard Ships*, BIMCO, https://www.bimco.org/news/priority-news/20181207-industry-publishes-improved-cyber-guidelines
- *Guidelines on Maritime Cyber Risk Management,* IMO, http://www.imo.org/en/Our-Work/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx
- *Risk Focus Cyber*, NYA, Thomas Miller P&L Ltd and Through Transport Mutual Services https://www.ttclub.com/fileadmin/uploads/tt-club/Publications___Resources/Document_store/UK_NYA_TT_Risk_Focus_-_Cyber_WEB.pdf

[1] List of FIATA Association Members is available at https://fiata.com/home.html