Cybersecurity and Data Protection Issues in Cross-border Paperless Trade

Dr. Gizem Kayisoglu
Maritime Cyber Security
Istanbul Technical University
Why is the cybersecurity of port infrastructure important?

Case 1: Port of Antwerp

Between 2011 and 2013, Dutch drug traffickers employed hackers to hide cocaine in containers bound for the Port of Antwerp by infiltrating the networks responsible for managing the goods contained within each container.

According to CyberKeel, the hackers managed to gain remote access to the terminal systems and thus had their own truckers load the containers without the knowledge of the port or shipping line officials. The Antwerp incident is the first known cyber drug incident.

Case 2: Australian Customs

A similar incident happened to Australian Customs in 2012. The criminals hacked into Australian customs' logistics software to see if they were tracking their containers, and when they realized their containers were diagnosed as suspicious, they abandoned the containers and fled.
What are the threat scenarios?

1. **Data Breach**
   - invoices
   - bills of lading
   - customs declarations

2. **Ransomware Attack**
   - shipping
   - payments
   - custom clearance

3. **Phishing Scam**
   - login credentials
   - financial details
   - trade-related email accounts

4. **Denial-of-Service (DoS) Attack**
   - critical trade documents
   - transaction processing systems
   - network infrastructure

5. **Insider Threat**
   - trade documents
   - transaction records
   - operational infrastructure

6. **Supply Chain Attack**
   - trade documents
   - operational systems within the supply chain
What are the international standards for cybersecurity and data protection?

International Standards for Cybersecurity and Data Protection

- EU General Data Protection Regulation
- APEC Data Privacy Pathfinder
- CETS 108
- ISO/IEC 27001 Information Security Management System
What are the cybersecurity strategies for cross-border paperless trade systems?

<table>
<thead>
<tr>
<th>1. Data Assets:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Trade Documents: Includes invoices, bills of lading, customs declarations, and other trade-related documents.</td>
</tr>
<tr>
<td>• Personal Identifiable Information (PII): Information about individuals involved in trade transactions, such as names, addresses, and financial details.</td>
</tr>
<tr>
<td>• Financial Records: Transactional data, payment records, and financial statements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. Infrastructure Assets:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Network Infrastructure: Includes routers, switches, firewalls, and other networking equipment.</td>
</tr>
<tr>
<td>• Servers and Databases: Hosts trade applications and databases storing trade data.</td>
</tr>
<tr>
<td>• Cloud Services: Platforms and services used for storing and processing trade-related information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Application Assets:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Trade Management Systems: Software applications used for managing trade processes, document exchange, and transaction tracking.</td>
</tr>
<tr>
<td>• Communication Platforms: Email, messaging, and collaboration tools used for communication within the trade ecosystem.</td>
</tr>
<tr>
<td>• Customs and Regulatory Systems: Applications used for complying with customs regulations and trade laws.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. Personnel Assets:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Employees and Partners: Individuals involved in trade operations, including traders, logistics providers, and customs agents.</td>
</tr>
<tr>
<td>• IT Staff: Personnel responsible for managing and securing trade systems and infrastructure.</td>
</tr>
</tbody>
</table>
What are the conclusion and suggestions?

International Collaboration:
• ESCAP and other international organizations should foster greater collaboration between nations to develop unified cybersecurity standards and practices.

Capacity Building:
• Providing training and resources to developing countries to enhance their cybersecurity capabilities and infrastructure.

Public-Private Partnerships:
• Encouraging cooperation between governments and private sector entities to share threat intelligence and best practices.

Research and Development:
• Investing in R&D to develop advanced cybersecurity technologies and solutions tailored for the trade sector.

Regulatory Harmonization:
• Working towards harmonizing cybersecurity regulations across different jurisdictions to ensure a cohesive and comprehensive approach to data protection.

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

OECD Privacy Principles

C5:2020 - Cloud Computing Compliance Criteria Catalogue
Thank you for listening

Dr. Gizem Kayisoglu
yukselg@itu.edu.tr