Managing Cyber Risk
Webinar on Cybersecurity and Data Protection in Cross-Border Paperless Trade

Bangkok, Thailand
June 13, 2024
Key Challenge: Ports and Terminals are Aggressively Targeted

- **Cybercriminals**' primary motive is financial gain, often stealing data or demanding ransom.
- **Hackers-for-hire** sell their services to people who do not have the skills or capabilities to do so.
- **State-sponsored** actors target organisations to compromise, steal, change, or destroy information. These groups are usually affiliated with a nation state.¹⁶
- **Hacktivists** are politically, socially, or ideologically motivated and target victims for publicity or to effect change.

**Threats**

- Ransomware: 27%
- Data-related threats: 20%
- Malware: 20%
- Phishing: 13%
- Breach/Intrusion: 7%
- Credential Harvesting: 7%
- DDoS: 7%
- Spoofing: 7%
- Supply Chain Attacks: 7%
- Vulnerability Exploits: 7%

**Threat Actors**

- Individual Actor: 7%
- State-Sponsored: 15%
- Espionage: 7%
- Operational Disruption: 20%
- Hacktivist: 23%
- Criminal: 55%
- Financial Gain: 38%
- Unknown: 29%

**Motivation**

- Financial Gain: 38%
- Criminal: 55%
- Hacktivist: 23%
- Unknown: 29%

ENISA Threat Landscape: Transport Sector (Jan 2021-Oct 2022); Published March 2023

© 2024 HudsonAnalytix, Inc.
Key Challenge in Cross-Border Data Exchange: Ports and Terminals are Aggressively Targeted

Transportation Sector Comparison

<table>
<thead>
<tr>
<th>Sector</th>
<th>Port authorities and bodies</th>
<th>Infrastructure and rail</th>
<th>Port operators</th>
<th>Airlines</th>
<th>Service providers</th>
<th>OEM</th>
<th>Airport operators</th>
<th>Public transport operators</th>
<th>Supply chain</th>
<th>Tier X suppliers</th>
<th>Surface transport operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port authorities and bodies</td>
<td>5</td>
<td>6</td>
<td>11</td>
<td>7</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure and rail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port operators</td>
<td></td>
<td></td>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Airlines</td>
<td></td>
<td></td>
<td></td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service providers</td>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OEM</td>
<td></td>
<td></td>
<td>9</td>
<td></td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Airport operators</td>
<td></td>
<td></td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public transport operators</td>
<td></td>
<td></td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply chain</td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>2</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier X suppliers</td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surface transport operators</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All subsectors had authorities and bodies that were being targeted, in fact 38% of the incidents targeted transport authorities. In the railway sector, incidents almost exclusively targeted railway undertakings and infrastructure managers. Similarly, port operators were the most affected entities in the maritime sector. These two sectors had only a few incidents targeting supply chain or service providers. This was not the case in the road sector, where OEM tier-X suppliers and service providers were targeted, along with public transport operators. In the aviation sector, airlines and airport operators are the main targets, followed by service providers, surface transport operators and the supply chain.

*ENISA Threat Landscape: Transport Sector (Jan 2021-Oct 2022); Published March 2023

© 2024 HudsonAnalytix, Inc.
Top 10 Emerging Cybersecurity Threats: 2024 – 2030

1. **Supply Chain Compromise** (e.g., software dependencies)
2. Advanced **disinformation** campaigns. (e.g., elections)
3. Rise of **digital surveillance**; loss of privacy (rise of authoritarianism)
4. Human error and **exploited legacy systems within cyber—physical ecosystems**
5. **Targeted attacks** enhanced by smart device data
6. Lack of analysis and control of **space-based infrastructure** and objects.
7. Rise of advanced **hybrid threats**
8. **Skills shortage**
9. **Cross border ICT service providers as a single point of failure**
10. **Artificial intelligence** abuse (e.g., deepfake videos/audio)
Enterprise Resource Planning (ERP) Systems offer virtual windows into an organization’s activities as it relates to people, resources, goods, and money.

ERP Systems integrate core business processes and leverage shared databases to support multiple functions used by different business units.

Systems affected include:

- Port Community System Applications
- Financial (re: Fraud, Payment info)
- Cargo Handling & Management
- Taxes (e.g., VAT)
- Customs
- Banking
- Aviation and Shipping

Impacts

- Data integrity
- Financial loss
- Liability exposure
- Operational delays
What You Can Do Right Now

**ORGANIZE!** Establish multi-disciplined cyber working group that meets regularly. Grant authorities!

- **ENTERPRISE ASSESSMENT**
  Perform an enterprise level cybersecurity capability assessment. Identify capability strengths and weaknesses.

- **DEVELOP AN INVENTORY**
  Develop an inventory of your assets. Classify critical systems.

- **QUANTIFY YOUR CYBER RISK EXPOSURE**
  Identify your most valuable assets, determine values and develop loss scenarios. Prioritize.

- **STRESS TEST YOUR INSURANCE**
  Review all policies for gaps/exclusions. How do they perform against the loss scenarios? Engage your broker!

- **PREPARE**
  Establish a Cyber Incident Response (IR) plan. Update Data Loss Prevention (DLP), Disaster Recovery (DR) and Business Continuity (BC) Plans.

- **TRAIN**
  Train! Deliver awareness training to executives (first) then staff, including operations and drivers. Exercise plans.

- **SUSTAIN RESOURCES**
  Develop and sustain resources (people, processes, tools) with a budget.
Thank You!

1800 Chapel Avenue West
Suite 360
Cherry Hill, NJ 08002

Max Bobys
VP & Practice Director

Office: +1.856.342.7500
Mobile: +1.301.922.5618
Email: max.bobys@hudsonanalytix.com

https://www.linkedin.com/in/maxbobys/