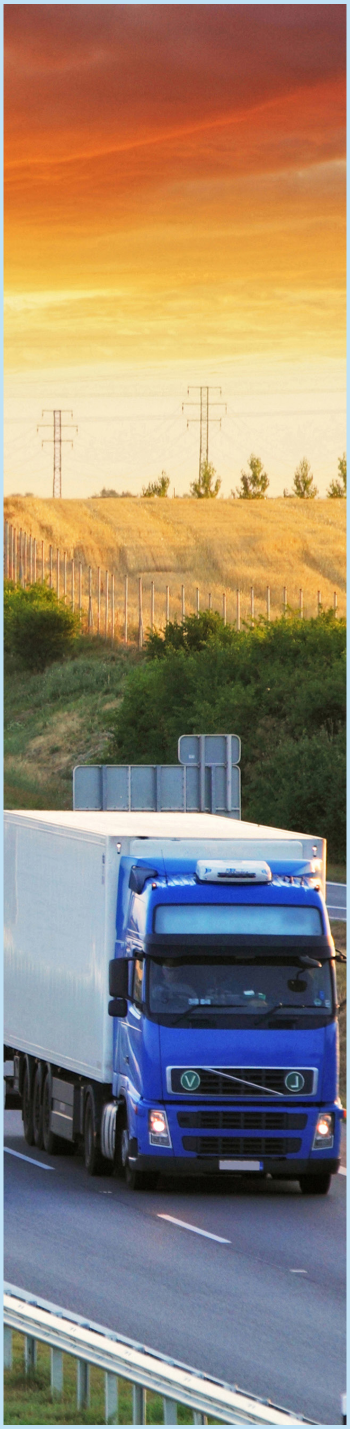
VIEW POINT



CYBERSECURITY FOR TRANSPORT AND LOGISTICS INDUSTRY

Infosys®

Navigate your next

Table of Contents

Transport and logistics industry overview

The world economic forum indicates that digitalization could unlock business opportunities worth $1.5 trillion approximately for logistics players over the next decade (to 2025). Digital transformation has rendered the supply chain to grow circular – utilizing the existing technologies with less cost, apt raw materials, transport management and execution. There are machine driven process changes – warehousing robotizations, electro-mobility, high speed rail, last mile optimization, software based process change - intelligent transportation systems, predictive maintenance and drone supervision, block chain solution and artificial intelligence solutions.

As a result, the logistics industry has begun generating huge amounts of structured and unstructured data that can be strategically dealt with only by advanced technologies like IoT and artificial intelligence. Businesses can achieve greater supply chain transparency and extensively reduce operating expenses by mapping information generated through connected equipment and logistics software to machine learning models implemented in the cloud.

Equipped with IoT solutions; manufacturing, retail and transportation companies can monitor goods' whereabouts in real time and ensure they arrive at the right time and place and in appropriate condition. Furthermore, IoT solutions enable businesses to assess demand based on historical data and automate inventory replenishment.

These technologies are in fact the key drivers of digital transformation in the transport and logistics (T & L) industry that increase operational efficiency and customer satisfaction.

Cyber risk in the T & L industry – Current state

Although digital transformation and automation of the transport and logistics sector is proving to be a boon, it also means that this industry, too, has become an easy target for cybercrime. As all levels of the supply chain are rapidly integrating with the cloud, there is an emergence of significant risk with regards to cybersecurity. According to Gartner, the number of internet-connected devices is expected to reach 50 billion by 2020. By integrating traditional IT environment with unconnected OT (Operational Technology) systems and expanding connected endpoints via IoT, the amount of security risks that consumers and businesses are prone to face will increase exponentially. Also, with the existence of many stakeholders and third party vendors in the logistics chain, this sector is particularly rendered vulnerable. Many companies currently lack a full picture of how to manage the risks that come hand in-hand with digital rewards. In a recent survey by PwC it was discovered that 38% of logistics companies have significant unresolved questions surrounding data privacy and security.

Cybersecurity drivers for the T & L industry

The State of Logistics Technology Report: 2019, EFT states that a bulk of the logistics industry's IT investment remains focused on four areas: business intelligence, transportation management, warehouse management, and supply chain visibility. Their findings also stated that:

- Only 35 % of solutions/service providers in the industry have a Chief Information Security Officer (CISO) in place
- Only 43 % of shipping companies have a CISO
- Only 21 % of the logistics companies believe they even need a CISO
- At least 55 % of logistics employees feel they are ill-equipped to identify or handle a significant cyberattack

The findings prove that the state of awareness in organizations with regard to cybersecurity in the logistics industry is very low.

The following facts need to be acknowledged and addressed:

- The threat to logistics, in particular is due to lack of security awareness within all layers – It's a board room challenge – typically wherein the CEO, CFO, board members should know, that cyber-attacks can prove to be grave issues. The traditional IT perimeter has changed to IT + OT+ smart products + services across supply chains.
- Security products are mainly focused on traditional IT and not on OT – the integrations will need lot of revamp in processes and tools. The dangerous cocktail of new, poorly secured IoT devices and old, poorly updated systems that exist in many companies present a golden opportunity for hackers to carry out attacks.
- Finding and mapping right talent to leverage advance tools and technologies is imperative

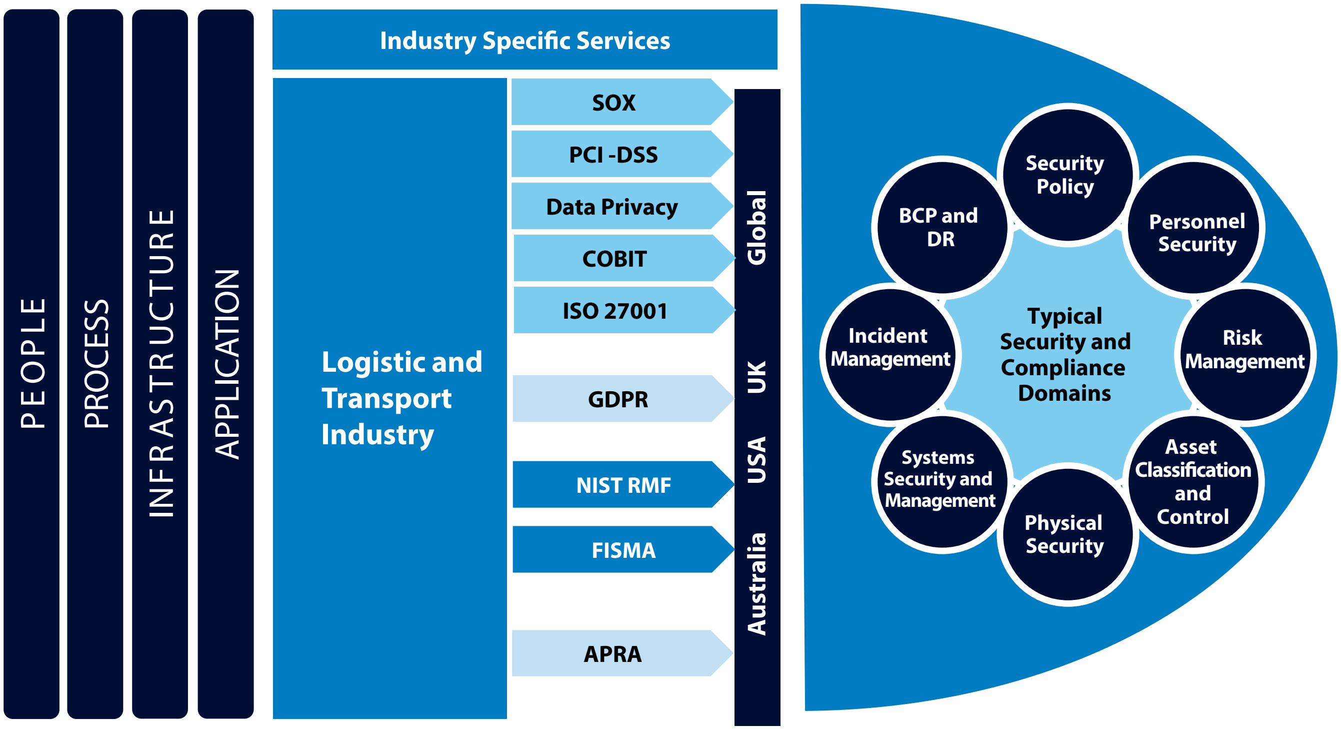
Building blocks for cybersecurity in the T & L industry

As digitalization will continue to reshape the T & L industry, it's important to have wise investments in security tools and technologies. Organizations should have complete transparency and visibility to manage risks within their environment. Long term security strategies and measures like the following should be implemented to reduce cyber risks significantly.

Risk based approach (Top Down)

To understand the gaps and future steps for a strong cybersecurity strategy, environments should have transparency and visibility and should manage risks with regard to people, processes and technologies.

A comprehensive risk assessment and discovery of all devices within an environment should include audit of the network, applications, and security protocols to mitigate threats. The assessment should also categorize and list the number of devices within the network, their particular risk, and how sensitive the data is that is produced by each device.



Identifying vulnerabilities within the environment

Due to the rapid adoption of IoT and IT solutions, the T & L sector is facing an increase in new threat vectors and an unprecedented level of cyber risk. IoT end points that are physically deployed at global scale and are also connected to the internet through many different protocols, make data privacy, confidentiality and assurance of key protection aspects and transactions vulnerable. Organizations should conduct rigorous vulnerability scans and pen test to detect potential threats and existing breaches.

Also, static and dynamic testing for IoT-connected devices should be done to establish minimum security baseline. Dynamic testing captures and exposes code weaknesses and any underlying defects or vulnerabilities introduced by hardware. This plays a pivotal role in identifying vulnerabilities that are created specially when a new code is used on old processors.

Network segmentation and centralized management

Once an organization has established a complete visibility of the environment through the two steps stated above, it can review its network layer. Network segmentation and zero trust are keys to a secured network layer.

A network needs to be partitioned into secure segments, or zones, so that IoT devices can be isolated from the traditional IT devices. One benefit of segmenting the IoT endpoints is that OT can continue to manage all of its devices without IT support. In case a device is breached, the devices in that segment are the only ones that are impacted. The zone can be quarantined and remediation steps can be taken without incurring the risk of other systems, IT or OT, being infected.

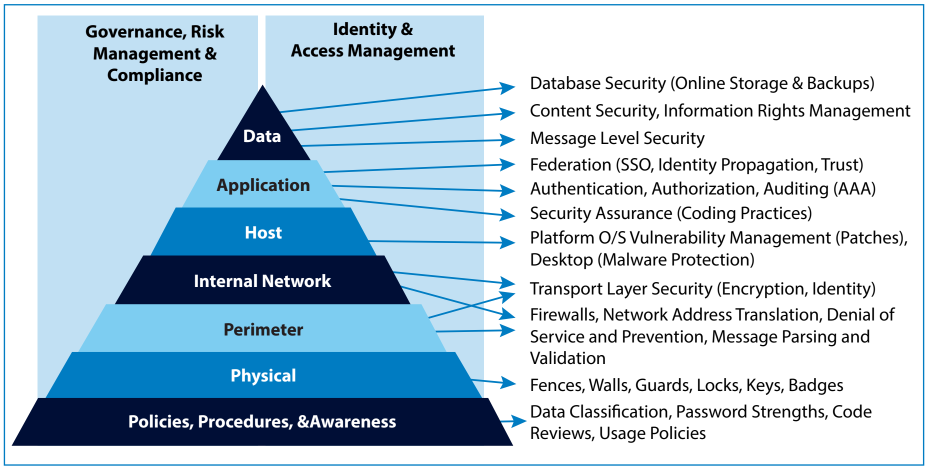
Centralized management is required to establish controls to protect the expanding IoT attack surface. An essential component of these controls involves the intelligent and automated segmentation of IoT devices and communication solutions into secured network zones that are protected by customized and dynamically updated policies. This allows the network to automatically grant and enforce baseline privileges for each IoT device risk profile, enabling the distribution and collection of critical data without compromising on the integrity of systems.

Also, in order to prevent DoS, Man-in-the-Middle and storage attacks, there needs to be a strong encryption mechanism and identity authentication control in place.

Multilayered IT security (Defense in depth)

It's also recommended to plan countermeasure strategies by implementing multiple layers of defense against any risks (defense in depth) with additional compensation and operational controls. At a basic level, all systems should have regular security updates. Network design strategies with proper zoning, micro-segmentation that involve isolation, should be implemented. The use of artificial intelligence should be increased so as to rapidly sort and analyze incoming data - allowing security professionals to spend more time detecting and containing threats.

The following diagram depicts security measures to be undertaken at each layer.


Governance, Risk Management & Compliance
Identity & Access Management
Data
Application
Host
Internal Network
Perimeter
Physical
Policies, Procedures, &Awareness
Database Security (Online Storage & Backups)
Content Security, Information Rights Management
Message Level Security
Federation (SSO, Identity Propagation, Trust)
Authentication, Authorization, Auditing (AAA)
Security Assurance (Coding Practices)
Platform O/S Vulnerability Management (Patches), Desktop (Malware Protection)
Transport Layer Security (Encryption, Identity)
Firewalls, Network Address Translation, Denial of Service and Prevention, Message Parsing and Validation
Fences, Walls, Guards, Locks, Keys, Badges
Data Classification, Password Strengths, Code Reviews, Usage Policies

A well-established change management and ITIL process for integration of new technologies and processes can reduce vulnerabilities within the environment.

Also, cybersecurity awareness should be made mandatory for all staff so as to avoid social engineering attacks.

Continuous monitoring

This should be an ongoing process to spot vulnerabilities and threats in order to support organizational risk management. The NIST (National Institute of Standards and Technology) framework provides a clear roadmap for compliance and continual improvements. The following should be adhered to:

- Categorize the underlying criticality and asset values of specific IT systems and data
- Select baseline security controls and apply device policies
- Implement and validate effective controls via SOPs (standard operating procedures), standard practices and run books
- Continuous assessment to check effectiveness at ground level
- Automation to monitor all security controls

If utilized wisely, these solutions can help companies to protect reputational damage, loss of competitive advantage, possible harm to passengers/employees, especially from OT attacks or regulatory impact on their brand, and also possibly generate increased revenues.

Conclusion

The logistics industry has introduced digital innovations at a slower pace compared to other industries that are revolutionized by digital technology. In such a scenario, early detection of vulnerabilities and the ability to monitor systems will help to have quick and efficient response to breaches. Cybersecurity should be a strategic decision that organizations must implement to maintain high safety standards across the T & L industry.

References

https://www.pwc.nl/en/industries/transport-and-logistics/digital-transformation.html

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

https://globalmaritimehub.com/wp-content/uploads/2018/05/Cybersecurity-and-the-threat-to-logistics.pdf

https://www.brighttalk.com/webcast/17106/376446?utm_campaign=user_webcast_register&utm_medium=email&utm_source=brighttalk-transact&utm_content=title

https://www.morethanshipping.com/importance-cyber-security-logistics/

https://www.oliverwyman.com/our-expertise/insights/2017/jun/time-for-transportation-and-logistics-to-up-its-cybersecurity.html

https://www.vanbreda.be/vrb-custom/uploads/2016/03/whitepaper_cyber_en.pdf

https://www.securitysolutionsmedia.com/2015/10/15/security-in-the-transportlogistics-industry/

https://www.bilogistik.com/en/blog/cybersecurity-logistics-transport/

https://www.forbes.com/sites/oliverwyman/2017/06/28/time-for-transportation-logistics-to-up-its-cybersecurity-as-hackers-put-it-on-target-list/#6141a5fa6fb9

https://www.supplychain247.com/article/the_top_2019_logistics_trends_shippers_should_know_about

https://cerasis.com/transportation-technology/transportation-reports-business-intelligence/

https://beyondsecurity.com/blog/security-testing-the-internet-of-things-iot.html

https://www.csoonline.com/article/3234915/3-must-haves-for-iot-security-learn-segment-and-protect.html

http://blog.cipher.com/mitigating-and-managing-iot-security-challenges

Abbreviations

Abbreviations	Details
T & L	Transport and Logistics
SAAS	Software as service
IoT	Internet of things
IAAS	Infrastructure as service
CISO	Chief Information Security Officer
API	Application programming interface
AI	Artificial intelligence
VA	Vulnerability Assessment
SOPs	Standard operating procedures

Annexures

Annex 1 : Real world cyber-attacks

The massive cyber-attack in May 2017 with the Wannacry virus jeopardised the world economy, affecting both small companies and large corporations. This threw many sectors including the logistics sector into a turmoil. Since 2017, logistics companies have found themselves thrown unexpectedly into the centre of this new threat landscape with the following high-profile incidents resulting in complete shutdown.

Not Petya	Perhaps the most infamous global ransomware campaign after WannaCry. Global shipper Maersk was badly hit: the malware required a complete infrastructure reinstall of 4,000 new servers, 45,000 new PCs and 2,500 applications. In the meantime, shipment delays had a huge knock-on effect on the supply chain. Maersk lost an estimated $310m as a result. FedEx is said to have lost a similar amount.
Ransomware	A ransomware attack on Bristol airport in September 2018 resulted in a total blackout of flight information, forcing staff to hand-write regular updates on whiteboards. A more targeted attack would have caused even more damage
Clarkson's breach	The global shipper suffered an unauthorized intrusion in 2017 which compromised a wide range of lucrative information including insurance, passport, bank account, national insurance and payment card data. Attackers got in via a "single and isolated user account", meaning a phishing attack was likely to have been the cause.
Ransomware	In the same year- diverse targets such as Deutsche Bahn in Germany, Cadbury's chocolate factory in Australia and the UK's National Health Service fell victim to ransomware attacks.
Pirate Attack	Greek shipping co had pirated attack at Somalia, Pirates gained access to systems easily because user names and passwords were never changed by the organisations.

Author

Arati Prabhughate – Principal Consultant

Arati possesses over 17 years of experience in data security , risk/compliance and cloud security domains. In addition to these, Arati has been a security architect and subject matter expert for multiple security products. She has also been involved in consulting, designing, transforming projects, program and service delivery across verticals within cybersecurity.

For more information, contact askus@infosys.com

Infosys®
Navigate your next