ThreatQ for Transportation

The transportation industry consists of air, rail, marine, trucking, and warehousing sectors, all interwoven with physical and digital elements, rendering them susceptible to cyber threats. For instance, essential systems like traffic lights and air traffic control towers heavily rely on technology. Cyber attackers utilize tactics such as phishing to obtain sensitive data, malware or ransomware to disrupt or destroy data, and breaching cloud-based systems to steal information.

Cyber criminals target their victims for the purpose of gaining sensitive information, such as credit card details, through phishing tactics, inflicting data loss or system failure using malware or ransomware and/or gaining unauthorized access to cloud-based data leading to data breaches and theft.

KEY CHALLENGES

The transportation industry encounters diverse challenges and considerations, contingent upon the mode of transportation (air, rail, marine, trucking) and the specific region or country. Here are some prevalent concerns across different segments of the transportation industry with a focus on cybersecurity:

REGULATORY COMPLIANCE

The transportation sector is subject to numerous regulations and standards that vary across regions. Complying with these regulations, including those related to cybersecurity measures, is imperative. Adhering to cybersecurity standards ensures the protection of sensitive data, critical infrastructure, and the overall resilience of transportation systems. Cybersecurity training and awareness programs become essential to prevent human errors leading to cybersecurity breaches. Attracting and retaining qualified personnel with cybersecurity expertise is vital for ensuring the overall security of transportation services.

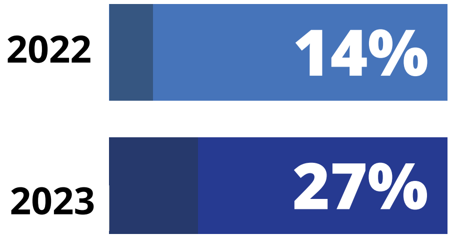
TECHNOLOGICAL ADVANCEMENTS

The rapid integration of technologies such as automation, artificial intelligence, and digitalization presents opportunities and challenges. Transportation companies must adapt to these innovations while prioritizing cybersecurity measures. Safeguarding against potential cyber threats is essential to maintain the integrity and security of advanced transportation technologies.

GLOBAL SUPPLY CHAIN MANAGEMENT

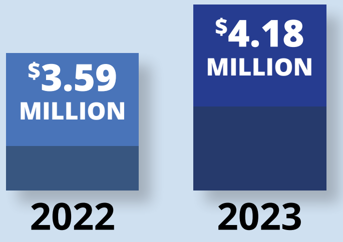
Events like natural disasters, geopolitical tensions, or global health crises can

PHISHING SCAMS NEARLY DOUBLED IN THE PAST YEAR



Source: Travelers Risk Index[1]

AVERAGE COST OF A DATA BREACH



Source: IBM[2]

Ransomware incident reports

INCREASED FROM 13%

of the total in 2021 to 25% in 2022.[3]

Source: Infosecurity Magazine [3]

disrupt supply chains, impacting the movement of goods and passengers. Cybersecurity measures are crucial to mitigate the risks of cyber attacks on interconnected supply chain systems, ensuring the secure and uninterrupted flow of transportation operations.

Addressing these concerns in the transportation industry requires collaborative efforts between governments, industry stakeholders, and cybersecurity experts. The focus on integrating cybersecurity into all facets of transportation operations is essential for building resilient and secure transportation systems.

CREATING A LEADING DATA-DRIVEN SECURITY OPERATIONS

Serving as the hub of intelligence operations for many industries, the ThreatQ Platform aggregates and combines unstructured and structured data from any source, internal and external. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with the ThreatQ open architecture. No code / low code automation eliminates repetitive, time-consuming tasks so analysts can focus on high-priority and strategic work. The platform also provides flexibility to share curated threat intelligence, advisories and reports with a range of internal and external stakeholders, including transportation sectors, quickly.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** external (e.g., ISAC) & internal (e.g., SIEM) threat intelligence & vulnerability data in a central repository.
- **ELIMINATE** noise & easily navigate through vast amounts of threat data to focus on critical assets & vulnerabilities.
- **PRIORITIZE** what matters most for the transportation system environment.
- **INTEGRATE** only relevant indicators into your transportation security policies.
- **PROACTIVELY HUNT** for malicious activity which may cause significant harm to transportation organizations.
- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status.
- **ACCELERATE ANALYSIS** and response to attacks against multiple targets including network-connected devices.
- **AUTOMATICALLY** push threat intelligence to detection and response tools.

Sources:

1. **Travelers Risk Index:** https://investor.travelers.com/newsroom/press-releases/news-details/2023/Travelers-Risk-Index-Amid-Fluctuating-and-Emerging-Business-Risks-Cyber-Threats-Remain-a-Leading-Concern/default.aspx (2023)
2. **IBM Security, Cost of a Data Breach Report 2023:** https://www.ibm.com/reports/threat-intelligence
3. **Infosecurity Magazine:** https://www.infosecurity-magazine.com/news/ransomware-double-europes/

Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at www.threatq.com/demo.

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection, investigation and response (TDIR). ThreatQ is the first purpose-built, data-driven threat intelligence platform that helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading integration marketplace, data management, orchestration and automation (SOAR) capabilities support multiple use cases including threat intelligence management and sharing, incident response, threat hunting, spear phishing, alert triage and vulnerability management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.