WILL **AIR CARGO'S LAX CYBERSECURITY MEASURES** BE ITS **UNDOING?**

In the last two years, logistics and aviation industries have faced numerous cyberattacks that have brought their operations to a standstill for weeks and created huge losses. As the air cargo and global supply chain industry moves rapidly towards a complete digital transformation, cybersecurity needs to be embedded into the basic DNA of its systems to protect against a range of cyberattacks being witnessed these days.

Lakshmi Ajay

In the last few years, logistics and aviation industries have faced numerous cyberattacks that have brought their operations to a standstill for weeks. The air cargo industry which is embracing digitalisation with a vigor, has also been a victim of cyberattacks as some recent incidents of cyberattacks against ports, airports, and critical logistics infrastructure have shown.

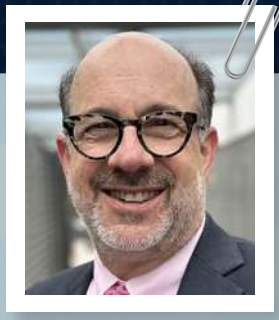
Last February saw US-based logistics giant Expeditors International announce a disruption of its global systems owing to a cyberattack. Leading cargo, ground handling, and airport services company Swissport notified its customers last February that its cargo services division had become the target of a ransomware attack. Hackers had also reportedly targeted several German airport websites last year which affected operations at Dusseldorf, Nuremberg, and Dortmund airports. Speculation is rife that the Federal Aviation Administration (FAA) system outage in the US that grounded all US departing flights in January this year could have been triggered by a possible cyberattack.

Some of the common forms of cyber attacks against organisations globally have been malware attacks, phishing attacks, ransomware attacks, distributed denial of service (DDoS) attacks, password attacks, man-in-the-middle attacks, spam, SQL injection attacks, insider threats, cryptojacking, and corporate account takeover (CATO).

Brandon Fried, Executive Director of, Airforwarders Association said, "Cybercriminals are not only targeting the big freight forwarders. The primary targets are the small-to-medium-sized forwarders with fewer resources to repel these attacks. The cyber-loss stories of these smaller forwarders may not appear in headline news, but our association hears about these attacks frequently."

While nation-state attacks once focused on infrastructure, think tanks, and governments; now they attack supply chains including vendors, software, and networks that government organisations rely upon as entry points to primary targets. The intellectual property of governments and organisations is also targeted.

Sean Lee, Director, Cyber Risk Advisory, at Heron Technology said, "What we could see happening in the future is a potential decoupling of the global



> *Cybercriminals are not only targeting the big freight forwarders. The primary targets are the small to medium-sized forwarders with fewer resources to repel these attacks.*
>
> **Brandon Fried**
> Airforwarders Association

economy into a West and East economic bloc and more countries strengthening resilience within their supply chain. There would be fragmentation of the global supply chain into smaller 'supply chain blocs'. This means that disrupting the smaller supply chain blocs, or either the West or East economic supply chains, to achieve political or criminal aims by attackers can become more attractive and prevalent."

Cybersecurity has become a growing concern for the aviation and transportation industry, reveals Eileen Rubiera, Director, Technology Operations, Cyber Technology & Innovation at Canada's Edmonton International Airport (EIA).

Rubiera told *The STAT Trade Times*, "Today's supply chains are highly interconnected. A threat to one partner in the chain constitutes a threat to the entire supply chain. When one supplier is hacked, it can disrupt transport across the planet. The transportation and logistics industry is a particularly tempting target because it is global. Hackers look for weak links in the chain and easy ways to access large amounts of data and money. Protecting the global supply chain with enhanced cybersecurity to guarantee the integrity of data and product is of utmost importance."

Even as the air cargo and global supply chain industry is rapidly moving towards a complete digital transformation, cybersecurity needs to be embedded into the basic DNA of its systems.

Amar More, CEO of Kale Logistics Solutions outlines the size of the beast as he says, "Cyberattacks have been on the rise. As per Eurocontrol, there have been 52 cyber-attacks in 2020 and 48 in 2021 against the aviation industry. Until the end of August 2022, there have been 50 attacks. This means that cyberattacks in 2022 have reached the same average as in 2020 and 2021 within three-quarters of the time. We have seen recently that USA-based aviation websites were taken offline by what is believed to be a Russian-based attack. Although no airport operations were affected, the attack underscores the deep vulnerabilities that exist »

in the aviation industry. One of the major factors contributing to aviation threats is the large attack surface of the aviation industry. Free Wi-fi in airports and on planes, digital apps, reservation/booking systems, IoT devices, and a host of other disparate but sophisticated systems increase the total attack surface."

The Covid-19 pandemic also forced people to work remotely and accelerated the digital transformation of workplace systems and work practices, which also massively increased the risk and threat landscape for cybersecurity. However, the cargo industry needs to be better prepared to protect digital cargo operational infrastructure at the API (application programming interface), hardware device, IoT, data, network, and application layers.

Giving a real picture of why cybersecurity is still a stumbling block for many in the air cargo industry, Marcus Campbell, Chief Technology Officer (CTO), of Hermes Logistics Technologies explains, "The economic pressures force us to look very closely at our cost of doing business and look for ways of reducing spending. Cybersecurity is an expensive business both in terms of implementation and operation. For a cargo business the challenges of fluctuating cargo volumes, slowing cargo demand and the economic performance in Europe, the impact of the Ukraine war and geo-political tensions between the US and China, and tech layoffs soon lead to cost-cutting measures that can result in a lowering of the cybersecurity barriers that are there to protect a business from cybercrime. However, it's the responsibility of everyone but more so the leadership to ensure the business has the necessary protection and governance in place at a cost to the business that is compatible with their revenues and risk appetite."

Today, there are many sources of intelligence and the intelligence information itself must be prioritized and correlated and therefore requires some human interaction too.

Tony Velleca
UST

Types of cyberattacks

In light of the ongoing Russia-Ukraine war, many countries are becoming increasingly vigilant in defending themselves against cyberattacks.

Fried added, "Over the last year, logistics companies including several AfA members, were forced to pay significant sums to cyber criminals who crippled operational information systems while demanding a ransom to restore service. These attacks continue to cost millions of dollars in cash and lost productivity. One common type of cyberattack is ransomware, which encrypts data on a computer system and demands payment to decrypt the data. Ransomware can cripple businesses and individuals when it locks them. Understanding that employees are the weakest link in any company's network security, we knew from the beginning that we needed to provide expert training to get our staff vigilant, keeping cyber security at the forefront."

Rubiera recalled, "The websites of major airports in the U.S. were hacked in October 2022, leaving them temporarily inaccessible. The cyber-attack hit websites at 14 airports. The cyber-attack, called denial of service (DoS), was designed to disrupt systems people use, to check flight timings and other information. In this specific case, the cyber criminal's objective was to cause disruptions to passengers and airlines. The websites were back online in a few hours. However other cyber-attacks can be more harmful and difficult to recover from, like ransomware or supply chain attacks, because they can have a large impact on systems making it more difficult and time-consuming to recover from."

Managing data is key

One might argue that data sharing is the future of the air cargo industry and will actively mitigate the supply chain against disruption or another Black Swan event in the future.

However data is becoming an increasingly valuable asset and it is essential that stakeholders in the air cargo industry continually implement updated cybersecurity measures to protect data in all its forms, including rates and operational data.

Vitaly Smilianets, Founder and CEO, of Awery Aviation Software explains, "Firstly, it is important to understand the difference between data sharing and cybersecurity. Data sharing between industry stakeholders, as advocated by Awery, improves the efficiency and reliability of the supply chain. Participating in selective data sharing with trusted providers does not impact cybersecurity. By partnering with a trusted

software provider like Awery, clients benefit from the selective sharing of essential information along the supply chain, which improves connectivity and efficiency."

Cyber-attacks also happen because of the multiple data transfers through different computer technologies, and insufficient cyber threat/event information-sharing amongst logistics stakeholders. So how can aviation and logistics companies mitigate against this risk?

Batting for modern Airport Community Systems or Cargo Community Systems (CCS) to save the day, More added, "With next generation CCS, which are built on technologies like blockchain,user-based access, and secured clouds like Microsoft Azure with third-party audits, these risks can be significantly mitigated. In order to respond to some of these threats, the aviation industry will need to adopt policies for managing vulnerabilities and preventing attacks. First, sophisticated multi-layer systems must become more secure to ensure their continued operation. 'Zero-trust' principles can easily be applied to airline industry systems and help prevent attackers from spreading their reach, once a system is penetrated."

Disrupting the smaller supply chain blocs, or either the West or East economic supply chains, to achieve political or criminal aims by attackers can become more attractive and prevalent.

Sean Lee
Heron Technology

Chua Eng Hock, Director, Cybersecurity Ops & Engineering, Heron Technology told the publication that the company offers a suite of offerings including consultancy services, data protection, and Managed SOC(Security Operations Center) services for its customers.

"With our consultancy services, we support companies to comply with the latest standards specified within their industries and regulations by relevant authorities. We also provide red teaming and vulnerability assessment services to test and audit companies' cybersecurity readiness and maturity. With our 'Data Protection' services, we offer a unique data leak protection (DLP) solution that incorporates digital rights management (DRM) and user entity behavioral analytics (UEBA) functionalities that enable companies to classify and manage access to their data across their companies and supply chain. We also offer a data diode solution that optimises data management in segregated networks, which are relevant to the air cargo industry that operates diverse information and operational technologies across public and private networks. With our managed SOC services, we provide for early detection and response to cyber-attacks by proactively monitoring our clients' IT network and user endpoints," Eng Hock said.

From reactive to proactive

In the digital era, supply chains are deeply integrated digitally with information being shared to track and trace the real-time conditions of shipments and cargo. The amount and importance of the data being tracked are enabling many new means of disruptions and the weakest link therein makes the entire chain vulnerable.

Tony Velleca, Chief Information Security Officer at UST and CEO of CyberProof told the publication that the burden is shifting to detection and response. "CyberProof uses our CyberProof Defense Center (CDC) platform to provide a single set of responses for monitoring potential threats to the organization. Our focus is on automation, not just to be able to handle more with less, but most importantly to respond faster to contain a potential threat and meet today's faster reporting requirements. Our »

CDC platform includes SeeMo – our virtual analyst, who automates up to 85% of threat response activities. From alert monitoring and enrichment to triage, investigation, and issue containment, this combination of an always-available virtual analyst and expert human analysts ensures false positives and duplicate alerts are ruled out faster, and our clients are then able to respond faster to reduce the business impact of real attacks."

Velleca added that as most of their clients become more digital, the technology landscape is moving to the public cloud. He says, "This shift fundamentally changes the way information flows between third parties in the supply chain and their solutions. For example, data flows between applications running in the public cloud (versus data centers). As the public cloud generally has a solid infrastructure layer, the threat moves to the APIs. The security of these APIs requires a knowledge of not just the network layer but also of the business logic and the potential means of conducting fraud or tampering with data."

Deploying threat intelligence

Threat intelligence is becoming more important these days in understanding these new types of potential attacks, their targets, and their motivation. It offers a means of identifying and therefore focusing on what is important to an organization.

Velleca shared, "Most large organisations have their own threat intelligence teams and if they don't, they can leverage an advanced MDR (Managed detection and response) service provider like CyberProof to help them. CyberProof integrates and automates cyber threat intelligence (CTI), ingesting CTI updates as alerts, and correlating these alerts with vulnerabilities and system alerts into a potential incident that can be prioritized. Today, there are many sources of intelligence and as with alerts, it can be overwhelming. The intelligence information itself must be prioritized and correlated and therefore requires some human interaction too."

Speaking about how AfA is safeguarding its members' cybersecurity, Fried added, "The Airforwarders Association now offers a cyber insurance program to its members. This initiative is also an extensive cyber risk management suite that includes risk prevention and loss response services as well. AfA has partnered with Roanoke Insurance Group to provide this complete cyber risk management program. This integrated solutions program offers cyber risk training and support to help you mitigate your risks. Members will also gain access to logistics cyber suite insurance coverage, loss projection and prevention tools, deep cyber data resources, and cyber recovery expertise. In addition, the program includes an exclusive cyber loss prevention and recovery portal complete with a breach coach and a 24/7 hotline in the event of an attack."

Cyberattacks have been on the rise. As per Eurocontrol, there have been 52 cyber-attacks in 2020 and 48 in 2021 against the aviation industry.

Amar More
Kale Logistics Solutions

Fried shared that in the United States, the Transportation Security Administration (TSA) had in fact issued a cyber security directive for pipeline owners under its emergency authority last year following the Colonial Pipeline ransomware attack in May 2021.

Fried added, "Since other transportation industry segments outside the pipeline industry were not immune from risk, the TSA issued similar directives for different segments, including the indirect air carrier community. As a result, a similar operational framework is in place for our members, with many of the exact requirements instituted for the pipeline sector. Meanwhile, the White House is also taking notice of the cyber security threat in our industry with a recent initiative designed to promote the sharing of critical information between different supply chain participants. The objective is to reduce disruptions and to guard against interference through cyber security, vulnerabilities, and other threat."

Rubiera added, "For detection and response, we have engaged a specialized cyber firm that provides 24/7 cyber monitoring and threat intelligence for our operating environment. For prevention, we have a vulnerability management program

in place. It is essential to highlight the importance of the recovery phase as well and to have secure backups that enable recovery in case of a disaster."

Prevention is better than cure

Preventing cyber-attacks relies heavily on the ability of every organisation to share information and data about threats and their activity so that the cybercrime experiences of one organisation can help protect another. Ensuring an organisation has a catalogue of incidents is key to continued learning and reapplication of proven remediation measures.

Campbell added, "Our SaaS managed service is a Software-as-a-Service solution that aims to focus the customer on the business of running their cargo operation while Hermes Logistics Technologies (HLT) takes care of running their CMS infrastructure. A component of this service is that we work with a number of partners who provide a combined managed security service. The security partner's objective is to deliver specialist security services to protect our systems from data breaches, monitor for threats, and monitor our Hermes CMS infrastructure at the application, server, network, and Operating System, and all components of the cloud infrastructure layers. We follow and implement a secure software development lifecycle for our Hermes CMS managed service and this ensures that security is designed and built-in at the start and is not just added on to the solution like so many other systems."

In the current geopolitical climate, it is also becoming known that state-sponsored actors target critical infrastructure to collect information through espionage and as a form of positioning and intimidation. As a result, global supply chains today are also targeted because of being a potential vehicle to cause massive disruptions to the ecosystem.

Giving details of the work being done on cybersecurity by leading agencies, Sean Lee told the publication, "The aviation industry is currently developing standards and guidelines for cybersecurity to cover various systems, such as air traffic management systems, aircraft systems, airport management systems, etc. ICAO's work includes developing Standards and Recommended Practices (SARPs) Standard 4.9.1 and Recommended Practice 4.9.2 in Annex 17 – Aviation Security to the Convention on International Civil Aviation (the Chicago Convention), procedures and guidance material."

Lee added, "Leading regulatory bodies like FAA and EASA are continuously developing guidance and opinions for cybersecurity. Under the Singapore Cybersecurity Act, the Singapore aviation sector was designated one of eleven critical information infrastructure (CII) sectors in 2018. Since then, several infrastructure owners, including airport operators and air cargo depot operators, have been required to comply with the Cybersecurity Codes of Practice (CCoP) issued by the Commissioner of Cybersecurity."

More suggests a three-pronged strategy involving people, processes, and technology and following a standard compliance-driven approach to do the job.

"Organisational silos where people do not speak to one another is one weakness that hackers can exploit. IATA estimates that more than 70 percent of hacks begin with interaction between staff and the hacker. So a compliance-driven approach, around regulation and standardisation, ensuring best practices when it comes to policy and procedure is a must. It is important for countries and global bodies to have strong cybersecurity laws that have the same level of harmonisation. Protecting today's complex infrastructure requires a fundamental change in how the industry approaches security. Airlines can't stop all malware from getting in, but they can stop damage to infrastructure and data theft using very secure technology," he added. ■