

Airport Cyber Security- A Boon or Bane

“Technology is going to disrupt the future of work, perhaps sooner than we thought”

~ Brian cornell

Since last 2 decades the world has witnessed, technological advancement and digitization which came as a revolution that made the systems error free and reducing the error of human terror. Artificial intelligence is marking its presence almost in every sector. Robotics on the other hand is taking over human jobs, all the way from intricate chores to heavy mental physical activities. Be it cleaning the house, cooking in the kitchen, or passenger facilitation at the airports by moving around and answering questions, controlling air traffic, controlling movement of trains, driver less cars and so on, it has taken control over major segments.

Keeping in view of terror attacks after world trade center episode 26/11 in US, the emphasis is on security of various installation and public utility services. When it comes to the airport cyber security, we need to first know what exactly it is in order to analyze the threat perceptions. Cyber in literal sense denotes computer and electronics. We are here talking about e-offices, paper less work. At airports, passengers can simply walk in with their mobile phones or i-pads with no physical tickets or boarding pass, neither id proof because when we talk about “cyber enabled”, every single piece of information is already available in the system. Recently, Mumbai Airport undertook a trial run for the air crew to reach up to the Aircraft with face identification. Being cyber enabled can save a lot of resources, from manpower to time to money, but it doesn't come that easy. There is a gigantic amount of threat perception, thus immense need to secure the systems, especially in terms of Aviation. This is where Cyber Security becomes a mandate in today's scenario, where we intend to depend on technology almost, entirely!

Aviation industry has been witnessing growth as open trade policies, foreign investments, multi stake holder collaboration and increasing air traffic. Artificial intelligence has led to dependence on cyber gadgets for comforts and quick mobility as a part of e-governance. Digital literacy and mobile devices are indispensable for air passengers, it is a matter of great concern that cyber threats are growing faster than their mitigation measures.

European Union has forecasted 248 million broadband subscribers by year 2025 and by the same period, India is expected to reach more than 700 million broadband subscribers. We can envisage that this explosion of digital land will greatly impact not only exports, but every growth sector as the supplier spectrum shall be worldwide, even for a small user segment.

Cyber security in Aviation sector needs to be given priority because of advanced persistence threat campaigns targeting airports, say for instance, malicious traffic for 2 nations state, result of a phished email, public document used as an email. The international airports are also being targeted by cyber attacks and passport control

system can get affected due to the result of malware. These attacks may culminate significant delays in departure.

Let us talk about some of the aviation attacks. An Islamic state message was displayed on an airport website that got hacked; it was defaced with statements supporting Islam and thus, led to the website shutdown. Airport private network baggage systems have experienced the intrusion by malware. Zombie army was introduced by the contractor managing the system. The airline attacks can affect ground operating systems that are related to flight planning. Suspecting distributive denial of service attack vector, often blocking the resources by unwanted data, suspensions of systems due to huge deliberate created traffic are some examples of varied attacks that take place almost every single day. Not just the information within the airport, but passenger's personal data too are prone to great risk elements, be it biometrics, photos or identifications. Frequent flyer accounts are first targeted, forcing the airlines to freeze their loyalty accounts, thereby quashing their marketing strategies, revenue and goodwill.

The World Economic Forum has identified cyber threat as a global risk. In a survey in 2018, San Diego International Airport had the threat index as 10 which meant devices and network was most vulnerable as compared to others posing higher risk of cyber attacks. Recently in September 2018, a Cyber attack at Bristol Airport caused flight display screen fall for 2 days. In the month of May 2019, another spoofing attack at Calcutta airport spread malware that by passed the network access controls resulting in release of unwanted data that clogged the core switches in the main data center and triggered LAN shut down.

The examples of Aviation attacks are innumerable, even the US customs and border protection disclosed an alarming data breach in the end of May 2019 wherein photos, license plates and sensitive biometrics of the travelers were stolen by the way of malicious cyber attack, that too by a subcontractor's network. The threats on cyber security at the airports from outsiders are dangerous but inside threats are treacherous, it directly amounts to immense continual loss if not pondered. Inside threats are usually unnoticed, unseen, un-anticipated and therefore neglected. Of course, the integrity of personnel should not be doubted, but seldom, the negative motivation leading to an emotional turmoil can force to act against the truthful law of nature. Two different persons undergoing a similar situation of being guilty, let down, or on a slip up may act differently. One may learn from the past mistake, whereas the other may haplessly choose to seek revenge.

Let us learn about the various cyber security systems which are prone to threats. Access control systems, perimeter intrusion system, radars, biometric data, network enabled baggage system, various electronic utilities, E - enabled aircraft system supported by Airport network services, face detection, digital identification systems, most vital and vulnerable database management systems and even core internal daily planning, working and implementation. The diversified attack vectors prone to cyber threats are devices and systems which become defenseless to any attack, fraud, misuse or data steal once a hacker gains access. Any digital media be it laptops, tablets, smart phones, pen drives, hard disks, even USB enabled charging stations, cloud computing, etc. Cyber attacks can be attempted by any amongst hackers, criminals, terrorists and insiders too.

Adverse Effects of Cyber Attack

We have been talking about cyber security measures and threat perception but the most important aspect of this problem is coming in the form of adverse effects to all stake holders, first & foremost the cost of repair damage, incalculable revenue loss and difficulty in sharing critical information. The shared information definitely creates awareness but it also serves as outline maps for attackers to target loop holes making them hit the iron when it hot. In most of the cases, the cyber attacks are not reported to the public or spoken about for the fear of reputation loss. The revenue loss is taken as a closely guarded secret. Cathay Pacific airline suffered major loss in the form of leakage of data over 9 lac passengers. Their passport details, personal data, photographs, telephone numbers etc were hacked creating an irreparable loss to the airlines in terms of reputation as well as revenue.

The Wi-Fi systems is the most dangerous facility in regards to data leakage, a better way out would be having our own monitoring system walled Wi-Fi to protect the data leakage because the information being passed can always be scanned and then assigned OK flags. The USB charging stations at airports are at a higher risk, for passengers as well as the working staff. They can be hacked, since USB is meant for data and power transfer, it can be misused and the information can be leaked once you used the device for charging purposes. Criminals can easily modify the USB to gain access to the connected devices. More because USB transfers data, all your privacy is in the hands of the attacker. To prevent such unauthorized data transfer, jack defenders should be used that are attached to the charging cord. They prevent the transfer of any data and pass only voltage. Also, let there be shielding systems to protect data theft, by enabling power pins and disabling data pins in the sockets.

Measures to secure systems are a mandate because the most vital asset of any organization is Data, which can broadly be misused by attackers. Outsourcing activities at the airports by airlines and other agencies are a major cause of concern coming in the form of cyber security threat, for instance the airlines do not employ their own people on checking counters and in their place, it is the people on contract basis who have accesses to all details of passengers. Imagine a situation where the intruders use them by giving the pen drive to copy the data, we normally suspect only the boarding pass, QR enabled but how many passengers are aware that a simple boarding pass thrown by them can be the biggest source of data leakage.

Alexandre de Juniac, Chief Executive Officer of the airline's global trade group, International Air Transport Association expressed, "Beyond biometric security measures, airlines are working on new data standards for traveler records, called ONE ID, to "liberate the industry from a century of accumulated legacies". With ONE ID, passengers will no longer be subject to repetitive document checks from check-in to the departure gate. He also mentioned that Air travelers have told us that they are willing to share personal information if it removes some of the hassle from the air travel, as long as that information is kept secured and not misused.

The travel industry is moving ahead with biometric identification to speed up the processes. We can have a single journey token that can be saved and used for a single trip, Gloria Guevera said, the World Travel and Tourism council's president and chief executive officer. Of course concern were being expressed by people for their privacy, but here both the sides of the coin must be seen, if there are risks, there are benefits as well. She also mentioned that increasing security is critical for the industry which is expecting passenger growth from 4.6 billion this year to 8.2 billion in 2037. Lack of global standards hamper the enforcement of security and privacy protocols worldwide.

World over, efforts have been and are being made by various agencies to have preventive measures for cyber security attacks. The bottle neck comes in the form of diverse international laws, airport size and community expertise. The funding availability for cyber security is also a big issue. What can we do if we are talking in global sense, the airport community needs a common sense and attainable approach to cyber security which is feasible to implement globally. We must set some common goals. An alternative approach in my view to curb data theft would be to prioritize data. In megabytes of data, only a part of it contains sensitive information. An easier way would be to secure the most sensitive information by means of prioritizing it (highest priority). Enforcing encryption standards, anti theft data protocols on every bit of data is not feasible, but yes the highest priority data can be kept in the farthest vault, even unseen so that it is not susceptible to any malicious attack. Even if intruders manage to reach our safest farthest data check point, we will have time to curb it as breach alerts and already have been sent and now instead of witnessing a cyber attack, we are in a state of counteraction and closely monitoring the hacker even before the attack has taken place.

Problem Needs to Be Realised

The cyber threats must not be addressed today but it needs to be reviewed to ensure that defenses are adequate for new threats for that education at all levels is critical.

Government Agencies Must Be Involved

Airport personnel should work with the government to ensure that airport cyber security concerns are discussed. The U.S. government has determined that the air transport industry is one amongst the 18 critical national infrastructures. Government everywhere must work with industry to meet the challenges.

Cyber Security to Be Given Priority

Airport personnel must not bury technology issues only with IT director and techno experts. Cyber threats not only need the top management attention, but also needs to be shared with all the stakeholders. Legal councils, risk management facilities, law enforcement must be involved for cyber defense.

DATA PRIVACY – AN ALTERNATIVE APPROACH TO SECURITY

In cyber space the prima concern and the most valuable asset of any organization is DATA. If we can keep the data secured, we continue to win. But, in an attacking scenario, our entire system stands lapsed. Is there a way whereby data can be completely secured? Yes, where data privacy steps in. If the data

private to you, it is secured already. If an attacker is unaware of the existence of your confidential data, how and from where would the imposter steal?

Even at airports, the internal data as well as data of all the passengers is very important. They not only hold all the relevant chief information, but also biometrics. In case it is hacked, the security and privacy of all the passengers including the airports is at stake. The key data must be kept private in order to save it from eavesdropping. Also, when free WI-FI is enabled, all care must be taken that any connected device doesn't breach into the system. One open pathway, access, or a gateway is enough for a big leak, which must be avoided, pondered upon and quashed.

Aviation Information Sharing and Analysis Centre

The airports need a greater presence in A-ISAC , since it is unique focal point for security information sharing across aviation sector to enhance ability to prepare for threats. A-ISAC is largely lead by aircraft manufactures and airlines. Cost prohibitive for even category X-airports which are busiest for volume of passengers traffic. Either amend A-ISAC cost approach or find an airport alternative.

Aviation is a Growing Industry

The airport community cannot assume that by protecting their own airport they are safe. All airports must work together to ensure a comprehensive defensive approach to cyber security.

Risk Assessment is a Must

Following areas are prone to risk

- Communication network
- USB Charging stations
- Wi-Fi in terminals
- Point of sale for concessions
- Supervisory control and data acquisition
- Law enforcement system
- Websites, parking systems
- Third party vendors, contractors and consultants etc.

Entire Network Not to Be Defended

Risk assessment will indicate most immediate vulnerability to vigorously defend the most likely threat vector. Follow demining cycle – predict, prevent , detect, respond.

Worst Case Scenario

- If you are cyber attacked, what is your response?
- Airports routinely practice emergency response on a variety of issues, but rarely on a cyber attacks.
- Immediate response or wait until you can determine the full threat?
- Are emergency response teams ready to have the IT take front and center after a cyber attack ?

- What is the continuity of operations plan (COOP) and disaster recovery plan (DR)?

STRATEGY TO BE FRAMED

The African proverb “it takes a village” applies in cyber security. Government, ICAO, NGO’s, IATA, ACI, industry leaders, contractors, especially airports must develop an industry wide strategy-the leading airports assist trailing airports. Organizations such as SITA (international society for international telecommunications) can play prominent role. Anything that is digital, can be hacked. Utmost care should be taken not just on preventive measures but also on building an airport level hierarchy data model where confidential information stays in the farthest accessible path.

What to Do?

- A long to go to understand and mitigate the cyber threat. • Airports have fewer resources than other players
- A common approach is critical.
- Start with education and information sharing
- Proceed to mitigation and defense techniques
- Airports need to work as a community, led by ACI and supported by major industry players such as SITA

The key to save oneself from a cyber attack, not just at airports but in daily living is to learn to use technology, not be used by the technology. If you stay smarter and alert, don’t be entirely dependent on a device even to remind you to drink water and switch off the A.C. or even speak your spouse’s name for you, you are on the safer side. Only if computers knew how to think, we would have lost our world to technology long back. After years of research and advancement in technology, this is very thin line that is stopping artificial intelligence to widen its horizons because it’s extremely difficult to figure out where the line of control needs to be drawn.

Be it aviation, defense, government, or private sector, I believe wherever there is digital media, it is prone to hacking, unless we can smartly secure it. This will always be a continuous evolution, new breaching techniques will keep peeping in and defensive measures shall keep defending.

TECHNOLOGY IS NOT DANGEROUS, THE WAY WE USE IT, IS.

TECHNOLOGY CAN’T HARM YOU, UNLESS YOU GIVE IT THE CONTROL TO DO SO.
