Extending the airport boundary: Connecting physical security and cybersecurity

Received (in revised form): 2nd February, 2018

BERT WILLEMSEN
is EVP Security at Scarabee Aviation Group. Bert is consulting airports on security challenges in the field of airside, landside, security and cybersecurity. He is a member of the ACI Europe Aviation Security Committee, and in his role he represents Scarabee on the ACI World Airport Security Standing Committee. He has been involved in several optimisation projects of security checkpoints at airports in Europe. He has a strong view on how to integrate the security process in the design of the passenger journey. He has experience in the field of cybersecurity strategies and cyber risk management. He is experienced in implementing and defining cybersecurity strategies throughout organisations, including airports. Before working at Scarabee, Bert executed several risk and threat analyses initiatives, with crisis management support for critical and sensitive infrastructure outside airports. During his career, he has dealt with in-depth risk analysis of internal and external processes within the supply chain of oil and gas and food and beverage companies.

MENNO CADEE
has been in the air transportation industry for over 15 years, working for Scarabee Aviation Group. He started his career in software engineering, broadening his knowledge through positions in technical integration of baggage handling systems. He is the senior technical project director responsible for Scarabee’s introduction of new technologies, such as artificial intelligence, in the field of airport operations, physical access, IT and cybersecurity. He gained experience as an IT security expert with penetration testing, vulnerability assessments, security audits, social engineering and advanced persistent threats. He has performed ethical hacking and penetration testing for numerous companies. During his career, he dealt with several technical challenges to improve mission critical processes and performance of airports.

Abstract
Airports are more and more dealing with considerable challenges towards effective airport security. The authors introduce a practice about creating a platform for sharing information and knowledge to defend airports against cyber and terror attacks. The threat is shifting from airside to landside, towards public areas. Security should be integrated into the design of the passenger journey, and the security boundary should be extended. This practice not only identifies zones with specific characteristics within the passenger journey but also connects vertical zones to infrastructure outside the airport perimeter. Access control, third-party supply chain and airports being part of a broader business network should not limit security to physical access but also include digital access, including insider threat. This initiative is translating general best practices into solutions against specific risks in determined areas. For cybersecurity as a start, it focuses on the baggage handling system (BHS) being industrial operating machines. Especially this baggage handling is a ‘forgotten’ area for (cyber)security. Airports tend to extend and build on existing equipment and therefore old programmable logic controllers (PLCs) and industrial (digital) equipment designed with an operational focus are still in use and often connected to newly installed machines. Since the main focus within airports is often on other areas, the implementation of European Civil Aviation Conference (ECAC) Std. 3 brings additional risks for BHSs to airports. Creating this (cyber)security information-sharing platform could build a road map for security to be shared with other airports. Implementation of location-based security, through monitoring of communication of surrounding control systems, will input identified specific BHS threats into the platform. After this first assessment of the BHS, the scope and the number of airports or external parties involved could be expanded.

Bert Willemsen, Scarabee Aviation Group, Hoeksteen 131, 2132 MX Hoofddorp (near Amsterdam), The Netherlands
Tel: +31-610969522
E-mail: Bert.Willemsen@live.com

Menno Cadee, Scarabee Aviation Group, Hoeksteen 131, 2132 MX Hoofddorp (near Amsterdam), The Netherlands
Tel: +31-622509089
E-mail: Menno.Cadee@scarabee.com
INTRODUCTION

We all know the horrible consequences of a terrorist attack at airports. Because of its high economic and social values, the aviation industry continues to be an iconic target. Improving physical security measures is a long-standing topic, but the cybersecurity measures seem to be lagging behind. Especially in the operational heart of the airport, the baggage handling system (BHS), cybersecurity is not seen as a priority. Both forms of attack are attractive to perpetrators because of the great damage they can cause.

At the same time, the aviation industry is growing rapidly; passenger traffic forecasts expect aviation travel to double in Europe alone. As many (major) airports, however, are not able to readily expand their real estate, capacity constraints must be resolved by improving the flow efficiency.

Besides that, passenger experience plays an important role too. Passengers tend to increase their retail spending when they are highly satisfied with the airport. For this reason, passengers become major stakeholders for airports and have the power to influence the airports’ profit. The growth of passengers and the need for a positive experience might interfere with the security checkpoints negatively.

To increase both the efficiency and passenger experience as well as maintain (or increase) high security standards, smart solutions and programmes are introduced. Innovative solutions to improve airports’ flow efficiencies feature more and more digital aspects. Biometrics, the use of (personal) data and smart systems are examples of those solutions. More and more devices and sensors that are connected to each other and share data are available on the market. This creates a vulnerable environment for cybercrime and thus poses a threat to business continuity. Figure 1 shows the context of challenges that airports are facing nowadays.

This paper provides a broader perspective on airport security, discusses the connection between physical and cybersecurity and recommends a collaborative approach.

Keywords

airport security strategy, passenger journey, connecting physical and cybersecurity, supply chain and third-party access control, baggage handling systems
approach related to the cybersecurity issues of BHSs. Efficiency (passenger flow) and passenger experience are the drivers in this context.

EXTENDING THE PHYSICAL SECURITY BOUNDARY

Change of nature and access control

Let’s start with looking at the airport itself. Over time, the character of airports has significantly changed. Where airports used to serve as just a short-stay pick-up point in the past, they are now changed into full ‘airport cities’. (Head) offices of large (inter)national companies are attracted to house around the airport, which gives the airport a high economic value. Apart from this value, airports also have huge human and symbolic values. From an ideological point of view, airports therefore have an increased threat level. Retail stores, offices, hotels, public transport, etc — anything belonging to airport cities — are attractive targets for malicious parties.

Due to the change of character, the complexity of access control is increased enormously. There are several categories of people who are using the airport facilities — for example, passengers, greeters, employees, visitors and users of the public transport. Lots of accesses are needed, and an open nature of space is necessary to serve all categories of people. Limiting accesses, as we have seen as a temporary measure after the attacks in Brussels (2016), causes other problems, such as major congestions and large groups of people in a small space, which bring new vulnerabilities.7

To enhance the landside security and get in control as well as possible, solutions are sought in the area of new and innovative technologies.

Passenger journey

As mentioned before, the aviation industry is growing rapidly. Therefore, the passenger flow has to improve and another factor that airports must contend with is that of improving their passenger travel experience. Digital solutions that make use of, for example, biometrics and the use of personal data seem to be useful. These security solutions could be integrated into the passenger journey, which starts at home.

Figure 2 shows an example of the passenger journey. The journey is divided into several zones, or stages, that a passenger goes through. In order to gain control as well as possible on the influx and the different categories of people, it is useful to identify the passenger before he arrives at the airport.

![Figure 2](image_url)  
An example of a passenger journey that starts at home
For example, in the course of 2018, airlines in the Netherlands have to provide passenger data to a so-called official Passenger Information Unit, whose task is to process and analyse them in order to prevent terrorism and crime. In this case, passengers are known when they arrive at the airport. Additional measures can be taken for passengers with a risk profile. On the other hand, ‘known’ and approved passengers can take part in airport programmes, such as undergoing a less-stringent security check. This benefits the passenger flow.

**Deviant behaviour**

Terrorist attacks are barely spontaneously committed; it takes terrorists weeks of preparation. The attacks at Atatürk Airport in Istanbul (June 2016) are an example of deviant behaviour. After research, it turned out that the attackers had visited the airport several times to observe the terminal security. They had executed multiple trials and spent hours and hours around the airport.

From a proactive point of view, law enforcements want to detect malicious people at the earliest possible stage. Looking at Figure 2, it is desirable to track down potential terrorists — for example, when they are preparing their attack at home, before they achieve their preselected target for the attack.

To make this feasible, deviant behaviour has to be looked at. This is called proactive profiling.

Every kind of situation, for example, situation in the different zones as showed in Figure 2, has defined its own behavioural standards. Everything that might be different should need attention, even when it is not initially suspicious. For example, wearing gloves might not be suspicious, but with 20 degrees Celsius outside, it definitely needs attention. Advanced technology is able to detect such deviant behaviour.

Another interesting aspect is the information exchange between organisations and governments within the different zones of the passenger journey. Communication is a very important key, especially in high-risk areas. Public transport, hotels or taxis can play an important role when talking about proactive profiling. For example, a person with a thick, long winter jacket is travelling by public transport to the airport during a shiny spring day. Not really suspicious, but the train conductor does not trust it and warns the law enforcement before he actually arrives at the airport.

Security is not just a matter of security guards and technologies; it is everybody’s responsibility. The more people are aware of deviant behaviour, the greater the change that malicious people will be noticed. It all starts with awareness.

**Screening systems**

During the travel journey of the passenger, the security checkpoint is an important stage — a security check both above and below the ground.

Innovative security solutions to improve airports’ flow efficiencies and security feature more and more digital aspects. Such novel technologies introduce new cyber risks to the airport flow infrastructure, but their novelty has often bestowed them with modern, reliable cybersecurity measures. More legacy airport technology, however, does not necessarily benefit from the same state-of-the-art cybersecurity. As cyberterrorism is becoming a growing risk to large infrastructure organisations such as airports, these assets may become more vulnerable than ever before. When
considering how these legacy assets, despite their age, still form critical elements for an airport’s flow efficiency, the risk that cyberterrorism poses to these assets has become unacceptably high.

Legacy airport infrastructure may not be readily refitted with new digital architecture but may need a hybrid security solution enabling both cyber and physical security elements. A prime exemplar legacy system to investigate is the BHS.

Airport screening equipment, such as the one used for baggage screening, was designed for local screening operation and to be reliable and safe rather than secure. There is an increase of connectivity and integration of screening equipment with wider airport security systems. Once-isolated equipment is now being connected to larger airport networks. Screening systems more and more use standard IT technologies such as operating systems. This exposes them to external threats, such as malware and hackers, which they were never expected to encounter. For that reason, the digital security boundary has to extend.

EXTENDING THE DIGITAL SECURITY BOUNDARY

The threat of cybercrime is ever rising. The one who thinks that airports are not affected by this is wrong: In 2013, the passport control system at a Turkish airport was under cyberattack, which caused chaos and crowds among the passengers and hours of delay. Under such circumstances, business continuity is threatened and may cause enormous damage.

In January 2017, thousands of travellers were stranded for hours and hours at the airports of Miami, New York, Houston and Atlanta because of a massive computer malfunction at customs. Passport control stations shut down and caused huge damage. This might have been a computer crash instead of a hack, but it shows the chaos that can arise when computers stop working.

At the airport, various technological devices are present and vulnerable for cyberattacks. These devices that may be affected are not limited to network devices that compose the typical information technology (IT) infrastructure. Access control devices, BHSs, flight information (display) systems and a broad range of other critical systems, such as airfield light controls, rely on digital technology that may be vulnerable to attack. Cybersecurity protective measures are often not applied as these systems are often not regarded as computing devices.

Airports often use integrated systems and local engineers to install, monitor or service these industrial systems, such as BHSs and many others. These systems are not always owned by the airport itself, but third parties, like airlines and suppliers, are responsible for those. Those organisations might have different interests, especially when it comes to cybersecurity.

Airports are also increasingly relying on cloud-based computing services, delivered via the internet. When using this off-premise computing solution, airports no longer have the same level of physical control over the security of their data and systems, so additional measures should be taken to secure unauthorized access and integrity.

In addition to this potential risk, through their supply chains, organisations such as airports are getting more and more exposed to third-party risk from small and medium-sized entities (SMEs). Business partners and other third parties could be SMEs, and for those parties, cybersecurity might be less interesting. And it happens that they are largely failing to adequately protect themselves
against cyber risks, because costs are too high and they face a lack of resources and knowledge.

In view of the rapid development of digitalisation and the associated risks, the cyber risks should also be mitigated through close cooperation and monitoring of the third parties in the supply chain, especially SMEs.

Figure 3 shows an example of an airport and the connection between the airport operations and the third parties. The risk of all different kinds of crime in the operations should be part of a wider security risk management programme that effectively identifies cyber and physical security risks.

Close collaboration between various departments and stakeholders, such as IT security teams, engineering operations and physical security operations managers, is needed. For cybersecurity, the same applies as physical security: it all starts with awareness. Awareness of the risks and the potential impact.

Public areas
To make security everybody’s business and responsibility, it is important to train airport staff, tenants and service providers to help protect the airport. But the largest groups of individuals visiting the airport are the passengers, greeters and visitors and they should be considered as well when assessing (cyber)security vulnerabilities. Direct access to and interaction with the airport and airport systems should be limited.

Public areas are often equipped with devices such as heating, ventilation and air conditioning controls, access control devices, CCTV cameras and passenger screening equipment. Publicly available Wi-Fi networks grant people access to the internet, and although these public networks are often separated from the airport’s internal network, it may be possible to gain access that affects passengers or airport operations.

Figure 4 shows that passengers can have direct access to kiosks, vending

---

**Figure 3** Airport access control monitoring third parties in the supply chain
Source: Picture based on map of Luxembourg Airport.
machines and other devices. It would be relatively easy to gain physical access to systems and devices in a manner that could increase the likelihood of a more serious attack.

The proactive security approach, as discussed before, could also be applied within cybersecurity. The usage of advanced technology could identify deviation of normal behaviour in a specific area, if persons try to gain physical access to digital systems. Measures should be taken to protect airport data and systems against cyberattacks from malicious people in public areas. This can be realised by connecting cybersecurity to physical airport security and the execution of a practical approach.

**PRACTICAL APPROACH TO COUNTER OPERATIONAL AND BUSINESS RISKS**

Cybercrime is becoming a worldwide threat against all nations, their governments, their high-risk infrastructures, and their large-, medium- and small businesses. Losses of privacy and confidential data, losses of direct income, operational standstills and terrorist activities are lurking around in the high density of digital systems and equipment at airports.

Once impacted, or if a digitally connected supplier is targeted, the affected airport will become a breaking news item by daily media distributors, with a secondary negative impact on passenger experiences and desired travel routes. Many examples can be given of hacked companies that lost lots of credit card data of their customers; the case of retail giant Target might be one of the biggest disasters. More than 41 million of the company’s customer payment-cards accounts were affected.12

Airports are using all types of industrial control system (ICS) devices. These systems are used to monitor and control various systems, such as baggage handling; heating, ventilation and air conditioning (HVAC) and airfield lighting. Baggage control systems (BCS), process control, supervisory control and data acquisition (SCADA) and industrial automation are all different categories of ICS.

These types of devices are also becoming increasingly interconnected and interdependent with other airport information systems, which may introduce
additional risks. Because of this interconnectivity, these devices are exposed to similar vulnerabilities as computers and network devices.

ICS devices can be vulnerable even if they are not connected to the internet. Control devices or sensors could also be compromised by access through an unprotected physical access point, by usage of a removable storage (such as USBs) to update the firmware or applications on an ICS.

Programmable logic controllers (PLCs) control machinery for integrated BHSs. This PLC is a digital computer used for automation of a typically industrial electromechanical process. Such a unit can be programmed to perform a variety of functions. PLCs often lack the security features of authentication and physical protection that traditional IT computers include.

And like almost all systems, they have grown in complexity and functionality, and their vulnerabilities have increased as a result. Many PLCs now include programming ports, external network or wireless access for upgrade, monitoring or configuration.

Some have at least a decade as a lifetime, before they will be replaced by newer equipment. Therefore these systems are not designed to face cyber risks nowadays.

Business partners

Airports use third parties, often SMEs, to provide systems for information and control systems. Therefore airports should ensure that their (cyber)security requirements are met before these systems are installed and used.

During the procurement process, the specific requirements should be identified so that qualified computing service providers are fully aware of the requirements they must meet, confirmed in purchasing agreements.

To effectively integrate cybersecurity requirements into the procurement process, IT and airport (security) managers should work with purchasing managers to ensure that their functional, technical and security-related requirements are all incorporated into system-and-data-procurement requests and the related supplier contracts.

Audits: Be prepared

Regular IT assessments and vulnerability scans throughout the supply chain are helpful to keep the airport’s extended IT infrastructure up-to-date, but actual penetration testing with advanced techniques will provide the airport organisation the needed insight on whether it is actually in control of its IT security (including third parties) or have been shutting their eyes to the real (ever changing) dangers out there while adding ticks to checklists.

Ensure that the people, involved in penetration testing, executing the IT security assessments, are able to actually execute very advanced attacks. Real IT specialists (ie hackers) not only know how to use available tools but are also able to think outside of the box and develop additional and advanced attacks when needed.

When an airport organisation experiences a serious security incident (and it will), it’s all about preparedness based on the understanding of such an event that will guide a successful recovery. It does not matter if the target is the security of the airport perimeter or the IT security of the airport hold baggage; this fact will always remain true.

If an airport organisation is not only looking for a positive score on the ‘in
control’ checklist but really wants to know if it is capable of withstanding the kind of very advanced attacks that currently take place on a global scale, the airport should exchange specific airport-related information with other airports. IT security advances. It always has been, and will probably always be, a precarious balance between attacks and defences. The available tools will be enhanced and become more powerful, and more advanced tools will become available.

Baggage handling systems

Multiple governmental departments are developing general ‘best practice’ documents, looking at the airport from a holistic point of view, with different departments as expressed in Figure 5. But where to start?

As the main focus on defeating cyber risks is mostly oriented on office networks, websites, parking, etc, the operational heart of the airport is the BHS.

The hold baggage is a ‘forgotten’ area for cybersecurity. Airports tend to extend and build on existing equipment and therefore old PLCs and industrial (digital) equipment designed with an operational focus are still in use and often connected to newly installed machines.

All European airports face the impact of the integration of the new security screening machines, ECAC Std.3 for hold baggage, where the layout, controls and IT infrastructures of the airport are affected. The implementation of these machines during the coming years will bring additional risks for BHSs to airports.

Looking at the introduction of ECAC Std. 3 at airports, many changes will be
made to the airport operations, and again both IT security and access control are major issues in these critical business processes of airports.

Weak protection can result in both data leakage and disruption of operations:

Data/privacy driven — security — General Data Protection Regulation (GDPR) compliancy.

- Baggage source message (BSM) — passenger details exchange connected to baggage items.
- Article 30: Maintain a process/data mapping register.
- Article 33: Breach notification.
- Perform data and privacy impact assessments.
- Perform risk assessments against business processes and assets.

Operations driven — security — ECAC Std. 3.

- Integrated systems.
- Perform risk assessments against business processes and assets.
- Responsibility for change management and third-party controls — supply chain.

**RECOMMENDATIONS**

An airport-specific platform could be built that will be looking at specific (cyber) risks for airports and even more specific ones with focus on a specific airport organisation and a specific department, such as the BHS, being the industrial operating machines.

To achieve this, an audit checklist for a specific category will be drafted from the best practices of a limited group of airports. These airports will benefit from each other by sharing this cyber risk information. For equal equipment, such as screening machines, SCADA systems and control suppliers, these best practices will help them to secure their assets efficiently.

After this initial phase, the platform (see Figure 6) is available for practical usage to share information on specific cyber risks by specific category. It will continuously grow not only by connecting more airports but also by integrating more categories in addition to the BHS.

The platform itself could also be used as a template to help airports act on a quicker and structured basis by the implementation of new cyber and privacy-oriented regulations, such as GDPR. It also helps airports prepare themselves for data and privacy audits and makes sure they are prepared and secured against digital inconveniences.

Airports decide which critical assets are of interest and which may overlap with one of the other participating airports. The idea is to set up the platform in such a way that all parties will benefit from each other’s findings, checklists and best practices from the same owned assets by different owners. This will make the template effective.

The suggested practical approach will result in a quick and clear understanding of applying practical checklists, based on
best practices and regulations, to achieve a cyber-secure environment for the airport within acceptable time frames. It is based on an approach used in other industries, such as energy and telecom, where it has become a standard to share information about cyber-related topics even between competitors so they can protect themselves against global, collateral or industry-specific targeting by unwelcome guests via the digital channels around their infrastructures.

**CONCLUSION**

What is the connection between physical and cybersecurity? First of all, an understanding of the physical security and the passenger journey is needed. Due to the rapidly growing amount of passengers, solutions to increase the passenger flow are needed. These solutions are often digital technology driven, and that is what brings new (cyber) threats. Besides the new technological solutions, airports are using legacy systems as well, which are quite often not fully protected. Especially when talking about the BHSs.

To manage and secure existing operational processes without modification or migration of existing hardware or software, airports should consider the protection of each individual location without the risk of system or operational impact. Physical access control at a specific location, on the control cabinet itself, will prevent unauthorized access to the control system and will facilitate change management on both the hardware and the software.

Installation of a security-monitoring solution for industrial control is highly recommended, which concentrates on three core IT principles: infrastructure and network structure, software integrity and physical security. This prevents any unauthorized modifications to existing integrated infrastructure and mitigates cyber risks.

Implement this industrial solution for the security of existing hardware and/or software in the BHS without modification or migration at each individual location. This could be possible without system, functionality or operational impact.

The monitoring is based on artificial intelligent systems and installed at each individual location; a ‘self-learning’ system will be installed, monitoring the communication on ‘normal’ behaviour. Any deviation of this behaviour will be alarmed on a stand-alone dashboard or can be directed into a SCADA or security incident and event management (SIEM) solution.

An integrated monitoring solution will reach a high level of communication security for the control software. The system will be able to monitor the data communication between the control system and the surrounding systems. Both deviations of behaviour and content in this communication will be alarmed as potential threat. Each reported event would be separately identified.

Newly identified threats could be reported into the joint cyber airport information platform and become available to other airports to join forces to focus on specific risks by category to the BHS.

The door of the control cabinet itself is equipped with an opening alarm for the physical security of the location. Usage of cameras enables access control monitoring for identification of authorised engineers with a working permit. This access control can be integrated into any dashboard or event management solution, executing the connection between physical and digital security.
References


(5) Ibid.

(6) IATA, ref. 1 above.


(9) ACI, ref. 7 above.

