UITP ADVANCING PUBLIC TRANSPORT

ACTION POINTS

CYBER SECURITY IN PUBLIC TRANSPORT

INTRODUCTION

Cyber security is a current and growing challenge that public transport organisations from large to small must recognise and take appropriate action to mitigate. With the unprecedented pace and complexity of cyber attacks, and the increasing digitalisation of the sector, a public transport organisation must be proactive and adopt a holistic approach at the strategic level to protect its critical information and systems and to fulfil its obligation to its customers.

A PROACTIVE AND HOLISTIC APPROACH

Information is critical for any business today, as are the ICT systems (Information and communication technology) systems used to store and process it. In order to be more efficient and customer friendly, public transport organisations are striving to use ICT to support business processes: ticketing and payments become cashless, planning and maintenance are supported by electronic tools, passenger information is provided online, ready to be accessed wherever and whenever.

Information is the lifeblood of public transport organisations and obviously needs to be protected. Information systems are increasingly automated and interconnected, a compromise in one area can impact the entire transport operation and its passengers. Therefore, it is crucial to identify and protect all relevant assets.

WHAT IS CYBER SECURITY?

Cyber security, information security, computer security, IT security, digital security: these and other terms refer to the protection of IT systems, in terms of damage to the hardware, software, or information found on the systems, as well as disruption or misdirection of the services they provide. In this document, the term cyber security will be employed.

THE RISK

WHAT IS AT STAKE?

An attack on information systems may have many faces: information and/or services may be stolen, blocked, destroyed or compromised, therefore it is important to protect the confidentiality, availability and integrity of information and services. Failing to do so bears the risk to lose money, operational capacity, image and trust – ultimately money again.

As described in full details below, the ICT infrastructure of a public transport organisation consists of operational systems, enterprise information systems and customer facing systems, each of which could be the target of a cyber attack. The vulnerability of public transport operators is increasing due to the interconnectivity of different operational as well as data collection systems and reporting tools.

For example, data that is generated in the operational systems of a public transport operator, like real-time departure information, can be used for mobile applications or internet based information systems. For an analysis concerning cyber threats the processes of system communications are extremely important to recognise, because these data transfer processes can be the potential 'transport lines' of cyber software threats and activities.

TYPICAL ICT INFRASTRUCTURE

Operational systems

Core IT systems or operational control systems, especially for rail, are usually referred to as SCADA (Supervisory Control and Data Acquisition) systems. These systems are critical as they are usually responsible for control of the operations and equipment. Examples are:

- Signal control systems
- Vehicle-system communication systems, including predictive maintenance
- Power supply and energy distribution systems

In the history of SCADA systems the system architecture was usually designed to be separate from the outside world with no interfaces or air-gaps. However, more and more information from these systems are used for other means, for example real time customer information.

It is a common misconception, therefore, that SCADA systems are "closed" and are not vulnerable to cyber attack.

Enterprise Information systems

As digitalisation creeps into every aspect of public transport, IT systems are relied on heavily, especially relating to information and business systems. Characteristics of these systems are that they are used by a huge number of persons in a company, which makes them potentially vulnerable to cyber threats. These systems very often also process data coming from the operational control systems and interact via interfaces with other, often external, systems. In an analysis and description of the IT landscape, these connection and exchange paths need to be considered.

These systems are used by most of the IT users in a company. **Threats including contaminated email attachments that can cause infection or USB-sticks infected with malware are two of the most common threats facing companies.**

Access rights to information for different staff groups is another element of the IT landscape which is important to consider when assessing risk, vulnerabilities as well as designing security measures, especially considering access to classified, critical or personal data.

Customer facing and external systems

External systems include ICT systems outside the company's IT infrastructure, such as website, mobile phone applications, cloud storage systems, points of sale. Social media and mobile applications are today using enterprise data, very often in real time, such as status of operation and departure times. Ticket shops via mobile or internal applications and customer interfaces operate with personal data like credit card details in their databases.

One significant characteristic of these elements is that they are very often subscribed to external companies. Software tools and services provided by external parties are not fully under the control of the company; hence it is crucial to ensure that the same cyber security level for internal systems is built into and maintained for subscribed systems.

In an IT landscape it should be considered how these applications are operated and by whom, as well as where possible critical and/or personal data is stored, who has access and who is responsible. It is recommended in a tendering process to define cyber security features of subscribed systems.

WHO IS THE ENEMY?

There are many types of people and organisations who may pose a risk to a company's information.

- Cyber criminals, interested to make money from fraud, selling valuable information or ransomware
- Competitors attempting to get access to business intelligence
- Hackers, who enjoy interfering with computer systems
- Hacktivists, trying to attack companies and societies for political or religious motivation- or simply to show they can do it
- Disgruntled employees and persons with legitimate access and opportunity for deliberate misuse

Beyond such active motivation, **human error must be taken into account** as well as social engineering: manipulating a person to click on a malicious link, open restricted areas of a network or reset passwords. **The first line of defence is always well informed and trained staff with an understanding of why it is important to follow digital security procedures, for example password policy.**

HACKER DERAILS TRAMS IN LODZ, POLAND

In 2008 in the city of Lodz, Poland, a teenager modified a television remote control to hack the tram system, taking control of a tram vehicle and the points systems. During the incident, 4 trams were derailed and several others had to make emergency stops, leading to twelve people injured. To conduct the stunt, the teenager used open source information and trespassed into tram depots to gather the necessary information and equipment.

SAN FRANCISCO'S MUNI HIT BY RANSOMWARE ATTACK

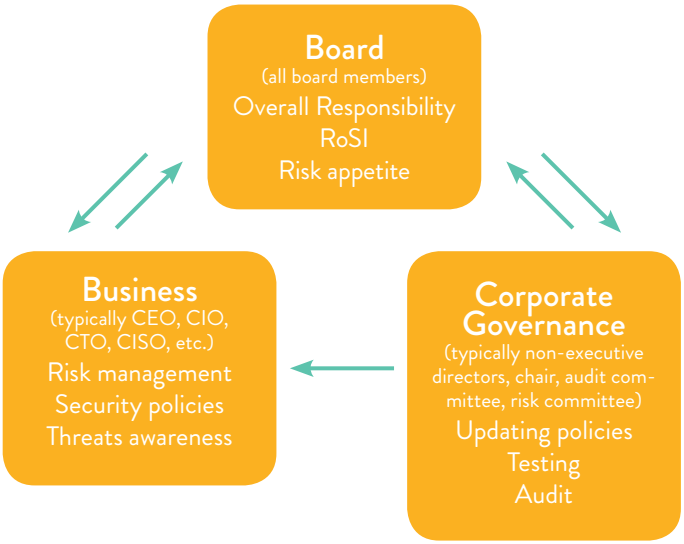
The San Francisco Municipal Transportation Agency (Muni), suffered an attack to its fare machines in November 2016. There was no disruption to operations, but passengers were unable to purchase tickets over Thanksgiving weekend. It is reported that the perpetrators responsible demanded a ransom of 100 bitcoins, the equivalent of approximately $73.000. During the incident, kiosk screens displayed the phrase "You hacked, ALL Data Encrypted". The system was restored, however, without any ransom being paid. The hacker gained access with malicious software sent by email which affected a number of other systems, including email and pay-roll.

CYBER SECURITY – A BOARD LEVEL TASK

GOVERNANCE

Cyber security is not simply a technical issue to be solved by the IT department alone. Like other corporate risks, cyber risks need to be managed proactively by the Board, led by senior management and assured by corporate governance. A model for managing cyber risks is suggested below. Implementation will clearly need to reflect the nature of your business and your appetite for risk.

Cyber risks need to be managed proactively by the Board, led by senior management and assured by corporate governance.



Roles and responsibilities of departments for cyber security have to be established by the Board, for example using the RACI principle (Responsible, Accountable, Consulted, Informed).

- Security policies have to be clearly defined by responsible business units and endorsed by the Board
- Responsible business units should also see to establish close contact with relevant authorities, law enforcement, etc.
- The Board should actively communicate the information protection policy to embed cyber security awareness and culture throughout the organisation

RETURN ON SECURITY INVESTMENT

Security investment, like any other corporate investment, has to be quantified and aligned with corporate goals and security strategies. As a result, executive decision makers need a reliable method; RoSI, the Return on Security Investments, which assess the cost-effective security investments, can definitely support them.

RoSI in practice

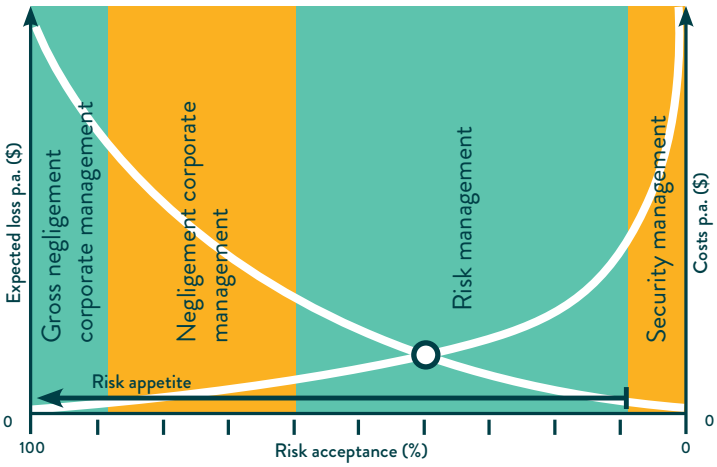
In general RoSI is calculated as follow:

$$RoSI = \frac{Monetary\ Loss\ Reduction - Cost\ of\ solution}{Cost\ of\ the\ solution}$$

The monetary loss reduction can be defined as the evaluation of the potential loss savings by security investment. Quantifying loss reduction for each component in a complex business environment, such as public transport is a difficult task in many ways. On the one hand, historical data indicating real monetary loss of an incident often do not exist, in particular for rare security incidents, and on the other hand evaluating the effect of security measures can be subject to misevaluations.

Of course risk managers can make use of risk assessment frameworks, for example based upon ISO 31000. These frameworks provide methods and recommendations for tools to model even complex business models and evaluate their risk in a standardised way. By means of standardised surveys and methods each component within a business model or business scenario is assessed and so the monetary value of a loss as well as the monetary impact of security investments can be approximated.

But to be more accurate and cost effective, RoSI calculation inputs should come from risk assessment and process modelling tools, that make use of content libraries (IT, Scada, RT, ITS, AFC....), which are adapted to the public transport operator and public transport authority business environment.



Economic equilibrium of security investments and expected monetary loss

RoSI is not rocket science, but a practical quantitative model, which provides quantitative answers to decision makers and helps to evaluate proper cost effective security investments.

RISK MANAGEMENT

A risk management process helps to understand and analyse the threats, risks and impact of risks on a company. Risk management is used in a number of disciplines, for example safety, security, financial and so on. The same risk management approach can also be employed for cyber risks. Risk management is a key aspect of effective governance and the only way to have a systematic, cost-efficient and proportionate approach to risk.

To conduct a risk assessment for cyber risks, a mapping of existing relevant assets, devices, networks, systems and so on is the first step, in other words describing the IT landscape. Then, possible threats, existing safeguards and possible vulnerabilities are defined.

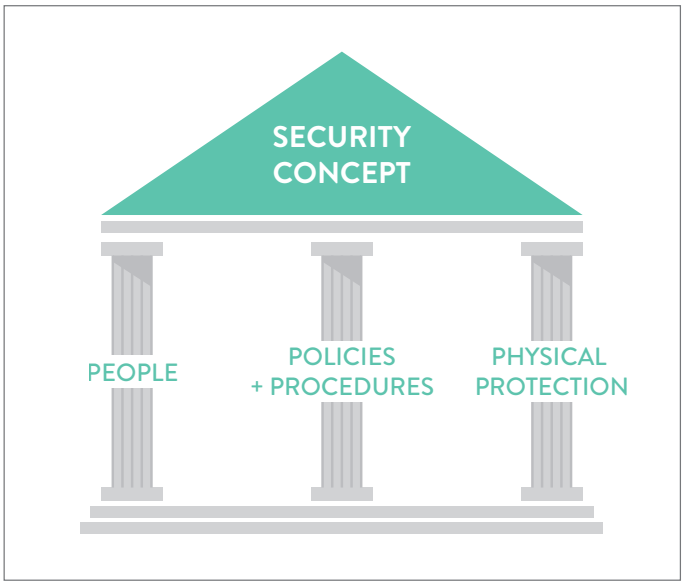
In order to have a complete assessment, it is necessary for a number of staff groups to be involved: IT experts, security, operations, HR, engineering, maintenance and so on. Indeed, for the cyber risk assessment to be part of the holistic risk management approach of an organisation, it is useful for the whole organisation to have an overview of all risks from all disciplines. Furthermore, cyber risks are not simply an IT issue, with all staff members having a role to play. Involving other departments in the risk assessment process, therefore, helps to raise awareness.

Cyber threats in public transport are often comparable to other sectors and industries. This is not often the case for other disciplines, such as safety or security. Therefore, on top of internal expertise, input from external experts may be valuable. Additionally, many countries have national cyber security strategies, thus input from authorities may also be relevant and helpful.

HOW TO PROTECT DIGITAL SYSTEMS?

PILLARS OF SECURITY

As for security in general, a successful information security management system needs to rest on three pillars- **people, policies and procedures** and **physical protection.**



People*

Regardless of the level or amount of technology deployed as part of any security system, it is the human element that will remain the weakest link in any security system. It is difficult to predict the intent of the human mind or determine one's motives. However, transit agencies can build a culture of awareness within the organization, creating like-minded individuals to further support and be supported by other pillars. Building a culture of awareness and further enhancing cybersecurity capabilities will consist of three primary areas:

- **Education** integrates all the security skills and competences of various functional specialities into a common body of knowledge and adds a multidisciplinary study of concepts, issues and principles. Information security education strives to produce information security specialists and professionals who are capable of vision and proactive responses.
- **Training** aims to produce relevant and needed security knowledge and skills within the workforce. Training supports professional development and assists personnel in performing their security roles, as outlined by their duties and responsibilities. The most important difference between training and awareness is that training seeks to teach skills that allow an individual to perform a specific function at a certain level of competency, while awareness seeks to focus an individual's attention on an issue or a set of issues. Awareness and training normally involve all the staff of a given organization.
- **Awareness** is a blended solution of activities that promote security, establish accountability, and inform the workforce. An awareness program includes a variety of tools of communication, outreach and metrics development. Awareness programs continually push and reinforce security themes to users in a variety of formats and provide them security information. The first part of addressing awareness is to introduce concepts of responsibility, expectations, and accountability as a platform on which to develop the necessary skills.

Awareness and training programs must be designed to incorporate the mission, goals and objectives outlined in the information security strategic plan, if one exists.

Policies and Procedures

Clear policies and procedures are key to the implementation of an effective cyber security strategy. An information security plan should outline all relevant measures for routine and emergency activities and, for instance, cover procedures for:

- **Certification/accreditation** – ensuring to give staff access to information only according to need and to have an exit procedure to shut down access when staff leave the company;
- **Access control** – providing clear rules for access protection and regular update of passwords;
- **Incident response** – outlining clear steps to be taken in case of a successful cyber attack, aiming to minimize the impact and restore normal operations/business as quickly as possible.

Standard ICT operating procedures have to clearly explain the dos and don'ts for employees, which should be subject to regular training and be acknowledged in writing by every employee.

Procedures need to be updated regularly in order to be inline with technology state of the art and the general cyber threat picture.

Physical Protection

The IT infrastructure has to be considered a backbone of business and operations. In order to protect it, several segments have to be considered:

Hardware – all physical IT infrastructure, from USB sticks to surveillance cameras. It is important to consider that any device can be connected to the ICT network. In order to prevent manipulation, vandalism or using these devices to gain unauthorized access, IT hardware needs to be physically protected and out of reach, accessible only for authorized users.

Software – necessary as an interface with the user, software also offers the possibility to access and manipulate information and IT

*Source: *Cybersecurity Considerations for Public Transit*, APTA. Full version found available on www.apta.com/resources/standards

hardware. While application and website hygiene as well as firmware and software updates, including patching, are crucial, they are not enough. Software also needs to be deployed as part of an active cyber security concept with logging systems, malware protection and so on.

Configuration – governs the relation between hardware and software. Proper access control management and firewall configuration may help create system redundancies, facilitate intrusion detection and data recovery, thus helping to harden any IT system.

INFORMATION SECURITY MANAGEMENT

In general, cyber security strategies, as currently defined by most governments, should have a twofold objective: improving resilience and reducing the threat.

- Improving resilience – digital infrastructure should be hardened to be resistant against penetration and disruption. Organisations need to improve their ability to defend against sophisticated and agile cyber threats and recover quickly from incidents, whether caused by malicious activity, error or natural disaster.
- Reducing the cyber threat – through working with allies on technical standards and international norms of acceptable behaviour in cyber space, strengthening law enforcement capabilities against cyber crime and deterring potential adversaries from taking advantage from remaining vulnerabilities.

Against this background, public transport organisations should focus on the following four priorities:

Standards, policies and procedures

Public transport organisations should develop, formalise and document thorough standards, policies and procedures in protecting against cyber threats and improving resilience to such incidents.

Information system technology and infrastructure

Public transport organisations should ensure the capability, maintenance, serviceability and interoperability of their ICT infrastructure. They should implement a thorough system development life cycle process that integrates risk management into the process.

Awareness, training and education

Public transport organisations should focus on developing a general culture of cyber security awareness. They should identify specific individuals necessary to receive further training and education as part of their professional development and career, in order to enhance the organisation's internal capabilities against cyber threats.

Information security risk management

Public transport organisations should integrate information security into their risk management strategy from the very top to align with the organisations vision, mission and goals. Integrating information security into the risk management process will ensure adequate identification and allocation of resources in enhancing the ability to mitigate and increase resilience against cyber attacks.

RECOMMENDATIONS

› Governance

Make digital security a corporate priority with responsibility at Board level.

› Risk and vulnerability assessment

Assess the risks to your ICT systems just as you assess operational, financial or physical risks.

› Secure configuration

Remove or disable unnecessary functionalities from your ICT system and keep them patched against known vulnerabilities.

› User education and awareness

Develop user security policies that are coherent and understandable, staff and contractors should formally acknowledge them. All users should receive regular training about cyber risks and their role and responsibility.

Network security

Connecting to untrusted networks, such as the Internet, can expose an organisation to cyber attacks. Follow recognised design principles when configuring your system, filter traffic at the system perimeter to ensure only relevant data and information is allowed and monitor traffic for unusual or malicious activity, which could indicate an attack or attempted attack.

Managing user privileges

Users should only be granted access rights and privileges that are necessary to do their job. Limit the number of critical accounts, such as administrators. Monitor user activity, especially access to sensitive information, or unexplained access from abroad. Ensure that the closing of ICT accounts is part of any staff termination procedure.

Removable media

Produce removable media policies that govern the use of removable media for import and export of information. Scan all media for malware using a stand-alone scanner before any information is imported into the system.

Malware prevention

Produce policies that directly address business processes, such as emailing, web-browsing and the use of removable media and personal devices. Protect machines with anti-virus solutions that actively scan for malware. All incoming messages and files should be scanned for malicious content.

Incident management

Develop incident response and disaster recovery plans that address the full scope of possible incidents. All plans should be regularly tested and updated.

Monitoring

Establish a monitoring strategy taking into account known previous incidents and attacks. Continuously monitor incoming and outgoing data traffic to identify unusual activity that may indicate attacks or compromised information.

Home and mobile working

Assess the risk of mobile working including access to remote systems, for instance built into rolling stock. Train users on the secure usage of mobile devices. Protect mobile devices though encryption, if possible, and protect data transfer with securely configured virtual private network (VPN).

Tendering processes and contracts

For tendering IT services, providing applications in the Internet or hosting databases it is extremely important to develop a framework to secure the integrity, confidentiality and availability of IT data when systems are subscribed. In these cases the so called SANS 20 Critical security controls can be useful. Experience shows that it makes sense to develop check lists in the company to be used by departments responsible for tendering and tendered projects. This will also depend on the tendering history of the company, existing contracts and the general approach to subscribed services.

This is an official **Action Points** of UITP, the International Association of Public Transport. UITP has over 1,400 member companies in 96 countries throughout the world and represents the interests of key players in this sector. Its membership includes transport authorities, operators, both private and public, in all modes of collective passenger transport, and the industry. UITP addresses the economic, technical, organisation and management aspects of passenger transport, as well as the development of policy for mobility and public transport worldwide.

This Action Points document was prepared by the Working Group on Cyber Security, a joint initiative of the Security Commission and IT & Services Industry Committee.

A digital version is available on Mobi+

FEBRUARY | 2017

UITP ADVANCING PUBLIC TRANSPORT

Rue Sainte-Marie 6, B-1080 Brussels | Belgium | **Tel** +32 (0)2 673 61 00 | **Fax** +32 (0)2 660 10 72 | info@uitp.org | **www.uitp.org**