UITP ADVANCING PUBLIC TRANSPORT

→ Position

Building Cyber-Resilient Public Transport Systems

An Executive Call to Action

© Zapp2Photo

In the past decade, the cybersecurity threat landscape has worsened significantly. Governments around the world are adopting stronger cybersecurity regulations to protect critical infrastructure and essential services – and this increasingly impacts public transport (PT). In this Position, explore how to build strong cybersecurity governance and shift from a cyber protection mindset to strengthening the cyber resilience of PT systems.

Key messages

In 2017, UITP's first publication on cybersecurity alerted executives to the dangers posed by cybersecurity and the potential risks of digitisation. Close to a decade later, the cybersecurity threat landscape has worsened significantly. Governments around the world are adopting stronger cybersecurity regulations across all sectors to protect critical infrastructure and essential services, increasingly impacting public transport. As 100% cybersecurity cannot be achieved, it is essential to protect PT systems from severe cyber events and minimise their impact.

UITP renews a call to action for PT executives to build strong cybersecurity governance and adopt a more comprehensive approach, going beyond a cyber protection mindset to strengthening the cyber resilience of PT systems. This Position puts a framework forward.

→ PT organisations must adopt a strategic framework to strengthen cybersecurity governance, from risk, threat, and incident management to much more.

→ Adopting cybersecurity by design – not just mere compliance – is essential for building resilient PT systems.

→ The global cybersecurity sector is short some 4 million workers, meaning tougher recruitment for PT organisations.

→ Increasing regulation can help the PT sector's cybersecurity maturity, while also imposing a steep learning curve.

→ For PT systems, IT-OT (operational technology) integration should be the focus of detailed planning, due to the increasing convergence of digital technologies with operational infrastructure.

→ There is no one-size-fits-all solution to cybersecurity; each organisation's approach must be tailored to its specific context, taking into account the regulatory frameworks and available resources.

TABLE OF CONTENTS

Cybersecurity – A core reponsibility for the public transport sector

As PT systems embrace their digital transformation, and with data increasingly becoming a high-value commodity, they face growing exposure to cyber threats that could disrupt operations, compromise passenger and staff safety, and erode public trust.

PT executives should no longer consider cybersecurity simply a technical issue; it is a core responsibility tied to service continuity, safety, and their companies' reputation.

A worsening cybersecurity landscape

The global cybersecurity threat landscape is worsening at an accelerated pace, enabled by emerging technologies and fuelled by increased geopolitical instability.

Cybersecurity is not an IT issue – it's a business issue.

Andy Lord, Commissioner, Transport for London

Europol's 2025 threat analysis points to a fundamental shift in serious and organised crime towards online activities[1]. Exploiting artificial intelligence (AI) and new technologies, cybercrime has become transnational, deeply integrated into digital platforms, and often aligned with political or ideological objectives, with cyber-attacks driven by both profit maximisation and destabilisation, as they are increasingly state-aligned and ideologically motivated. Criminal networks and hybrid threat actors are exploiting digital vulnerabilities to steal data, extort payments, and interfere with essential services. AI and new technologies lower the barrier to more sophisticated attacks, even by relatively unskilled actors. Both Europol and European Union Agency for Cybersecurity (ENISA) warn of a professionalisation of the cybercrime market, with hacker-for-hire, Malware-as-a-Service, and Distributed Denial of Service (DDoS)-for-Hire services available.

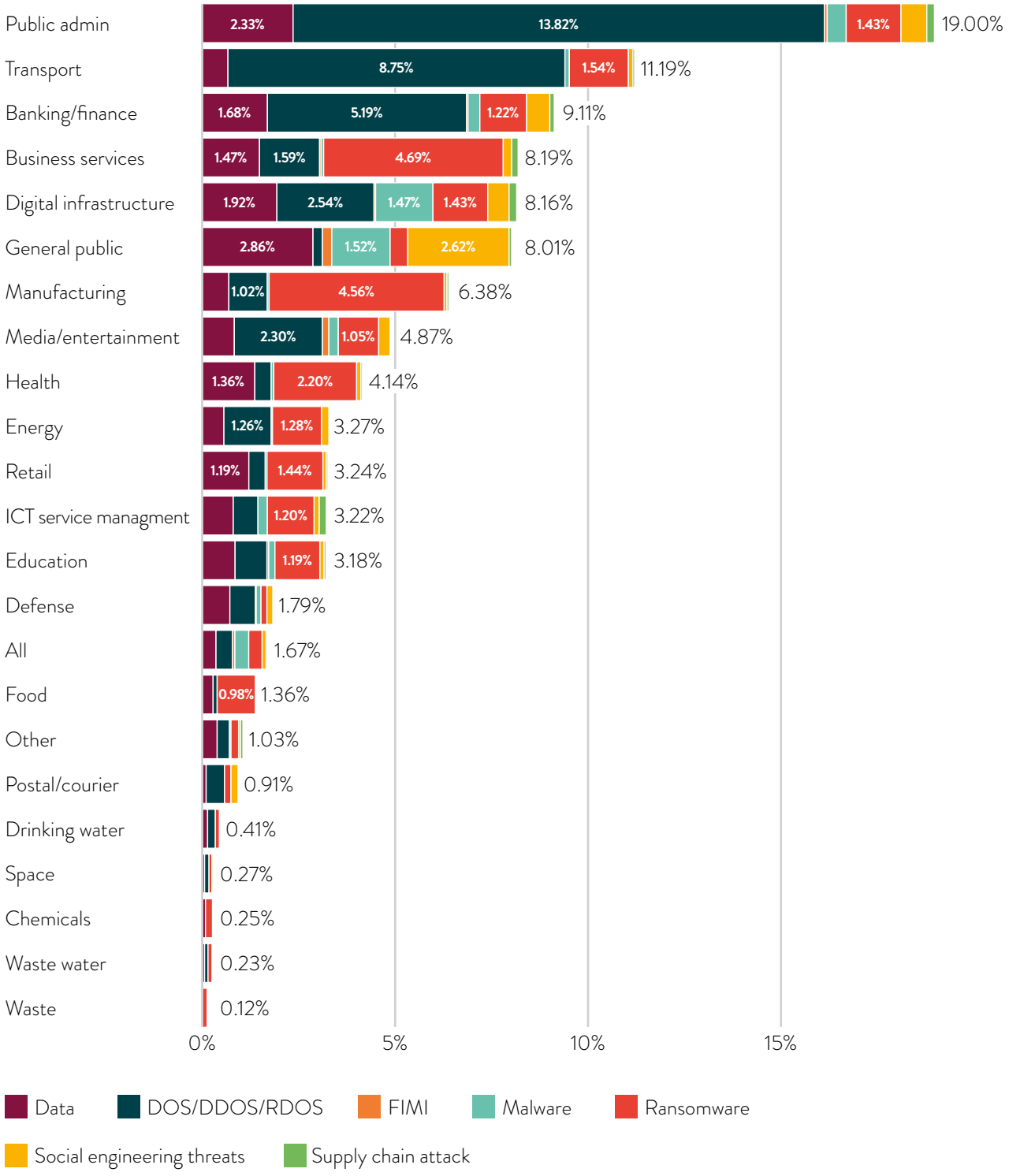
If data is the new currency of power; stolen, traded and exploited by criminal actors, then it is critical to proactively defend digital assets to safeguard businesses.

The changing DNA of serious and organised crime, Europol, 2025

ENISA reports in its 2024 Threat Landscape an escalation in attacks on critical infrastructure[2]. In 2023-24, transport (including all subsectors) was the second highest targeted sector, representing 11% of the reported cybersecurity incidents, following public administration (19%) but ahead of the finance sector (9%).

In the transport sector, DDoS and ransomware attacks top the list, followed by supply chain attacks. As per ENISA's analysis, financial gain remains the primary motivation, but disruption, espionage, and ideological factors are increasingly playing significant roles. Both organised crime and state-aligned actors are increasingly targeting transport systems, seeing them as potentially high-impact and high-return. Public transport-interconnected, publicly funded, and highly visible — is also a target.

Figure 1: Ranking targeted sectors & threats per sector
Source: ENISA Threat Landscape 2024



Recent cyber-attacks on public transport systems

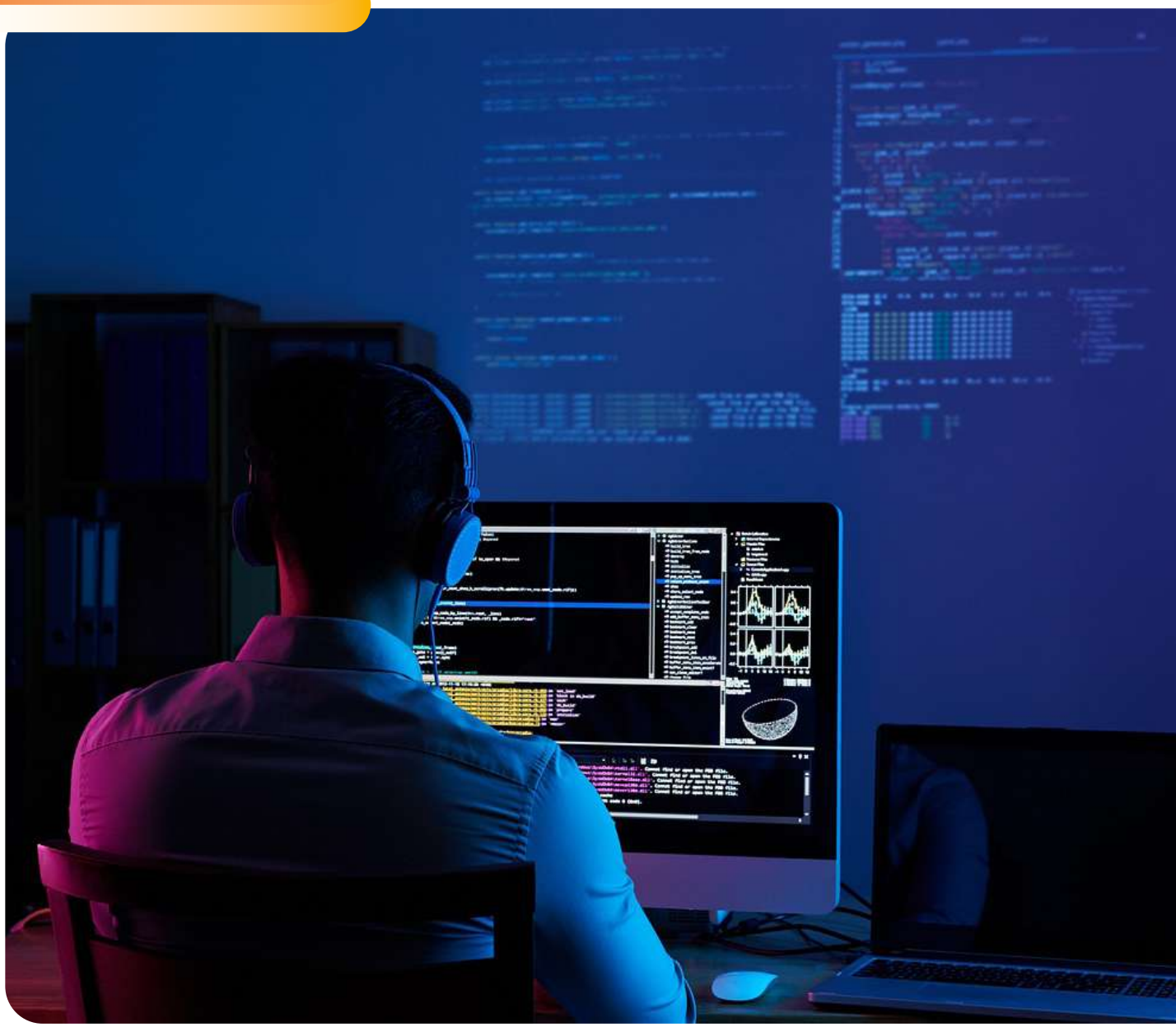
Over the past five years, **cyber incidents targeting PT systems have escalated in frequency, complexity, and reach.**

From ransomware attacks that have crippled ticketing systems to hacktivist campaigns disrupting digital services, these incidents underscore the **strategic importance of cyber resilience in urban mobility infrastructure.**

Impacts range from **temporary suspension of ticket sales and real-time passenger information to data theft, reputational damage, and multi-million-euro recovery costs.**

The table below provides an overview and illustrative cases of 2020–2025 cybersecurity incident trends impacting PT systems. The list of cases is non-exhaustive and based on open-source and publicly available information.

Trend	Description	Illustrative cases
Ransomware and data extortion surge	Transport operators have become targets for financially motivated ransomware groups. Attackers exploited remote-access systems, email servers, and third-party vendors to encrypt or steal data, demanding high-value ransoms.	STM, TransLink (Canada, 2020); ADIF (Spain, 2020); Stadler Rail (Switzerland, 2020–2021); Maryland Transit (USA, 2025).
Hacktivism and political cyber operations	Hacktivists increasingly use transport attacks to make political statements, disrupt logistics, or protest governments. These incidents often coincide with geopolitical tensions.	Belarusian Railway (2022); Italy-wide DDoS (2025); Tbilisi buses (Georgia, 2025).
DDoS disruptions and visibility attacks	DDoS attacks have become a low-cost, high-impact tactic to disable ticketing systems, apps, and public information displays, causing visible public disruption.	Czech Railways (2022); Auckland Transport (2023); ATAC Rome (2023); Italy-wide DDoS (2025).
Exploitation of vendor and supply chain weaknesses	Third-party service providers (ticketing, Wi-Fi, and data management) were exploited as entry points, leading to operational outages and data leaks.	Network Rail/C3UK Wi-Fi (UK, 2020 & 2024); DSB (Denmark, 2022); Elron/Rindago (Estonia, 2023)
Data breaches and privacy incidents	Public transport operators (PTOs) are custodians of sensitive passenger and employee data that hackers steal.	Indian Rail app (2020); Network Rail/C3UK (UK, 2020 & 2024); TfL (UK, 2024).
Insider and human factor risks	Misuse of administrator access and poor credential hygiene has contributed to internal compromise or unauthorised changes, highlighting the need for behavioural monitoring.	Network Rail (UK, 2024); various phishing-related ransomware incidents (2020–2025).
Operational technology (OT) exposure	The integration of Internet of Things (IoT) technology and the increasing digital coupling of information technology (IT) and OT have made transport infrastructure more exposed. While few incidents have reached OT, the risk is growing.	Olsztyn Smart City (Poland, 2023); Poland Railway "radio-stop" hack (2023).
Financial and reputational impact	Recent attacks caused millions in losses, required system-wide password resets, and delayed infrastructure projects, underlining cybersecurity as a strategic—not just technical—risk.	Auckland Transport (2023); TfL (UK, 2024); Maryland Transit (USA, 2025).



© Innova Labs

Increasing regulation

Faced with this worsening cybersecurity threat landscape, governments around the world are developing mandatory regulatory requirements to protect critical infrastructure and essential services. From Asia to North America to Europe, authorities are setting cybersecurity requirements that are increasingly impacting the PT sector.

While this regulatory wave can help enhance the PT sector's cybersecurity maturity, the implementation of these regulations represents a steep learning curve and can pose a significant challenge, particularly given the complexity of protecting long-life assets, often designed and commissioned decades ago with limited resources, both in terms of expertise and funding. Without accompanying supportive measures and an adapted implementation approach, PT organisations may struggle to meet regulatory requirements, ultimately leading to financial and legal implications and potential delays in PT project implementation.

Table 1: Sample cybersecurity regulations impacting PT around the world, compiled by UITP

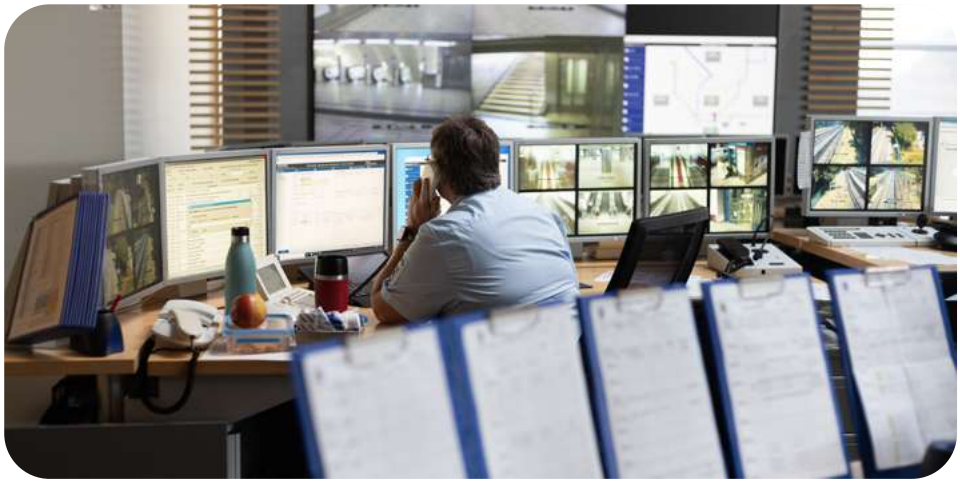
Country	Legislation	Impact/provisions
Singapore	Cybersecurity Act (2024 Amendment)	PTOs can be considered operators of critical information infrastructure (CII). CII denotes computer systems that are necessary for the continuous delivery of an essential service in Singapore; the loss or compromise of such systems would have a debilitating effect on the relevant essential service's availability. Broadens the scope of the 2018 Cybersecurity Act to include virtual systems, overseas CII, and new categories. Provides the Cyber Security Agency of Singapore greater oversight and the authority to issue penalties of up to 10% of the annual turnover of the entity in Singapore. Expands reporting obligations for cybersecurity incidents.
	Cybersecurity Code of Practice for Critical Information Infrastructure (CCoP 2.0)	Applies to designated CII in the transport sector (among others). Specifies minimum cybersecurity requirements for CII owners, covering access control, data security, cryptographic key management, duty segregation, and regular security audits. The code establishes the ongoing monitoring, assessment, and adaptation of security measures to address emerging threats and vulnerabilities.
USA	Transportation Security Administration (TSA) Directives (2023 update)	First introduced in 2021, TSA Security Directives aim to enhance cybersecurity for critical infrastructure, including rail and public transport. These directives mandate specific actions to protect against and respond to cyber threats, focusing on incident reporting, cybersecurity coordinators, and vulnerability assessments. The 2023 updates SD 1580/1582-2022-01A, SD 1580-21-01B, and SD 1582-21-01B extended and strengthened previous measures, including: → Operators must test at least two objectives from their Cybersecurity Incident Response Plans each year. → Operators must submit an updated Cybersecurity Assessment Plan every year and audit specific cybersecurity controls on a rotating schedule (all controls must be assessed within three years).

Country	Legislation	Impact/provisions
EU	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)	NIS2 Directive expands the scope and obligations of the 2016 NIS Directive. It imposes obligations for critical and important entities, including: → Implementation of risk-based cybersecurity measures → Mandatory reporting of cybersecurity incidents within a defined timeframe → Implementation of risk-based cybersecurity measures → Accountability for top management. Non-compliance can lead to fines of up to 2% of company turnover or a minimum of EUR 10 million or the temporary prohibition of the company chief executive officer (CEO) from exercising managerial functions. Public transport is not identified as a sector of high criticality under NIS2 Directive; however, local PTOs and PT authorities (PTAs) in the European Union (EU) may be brought into the scope by member states through the transposition into national law or the transposition of the Critical Entities Resilience (CER) Directive.
	Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act (CRA))	CRA aims at strengthening cybersecurity for products with digital elements (PDEs)—including software, hardware, and connected devices—placed on the EU market. Products are divided into different criticality classes based on risk level, with higher-risk items subject to stricter conformity assessments. It entered into force in June 2024, allowing for a transition period of up to 36 months. CRA requires that manufacturers, importers, and distributors ensure cybersecurity throughout the entire product lifecycle. Key obligations include: → Conducting risk assessments → Implementing secure-by-design principles → Addressing vulnerabilities via updates → Reporting actively exploited vulnerabilities and incidents Non-compliance can lead to fines of up to 15 million euros or 2.5% of global turnover. CRA applies to the PT supply industry (as all modern PT assets and systems integrate digital elements), with the exception of road vehicles, already covered under Regulation (EU) 2018/858 or UN Regulation No. 155 on cybersecurity and cyber management systems (mandatory for all new vehicle types in the EU from July 2022 onwards).

Critical skills and resource gap

As of 2024, there is a global cybersecurity sector shortage of nearly 4 million workers, and the gap could reach 85 million by 2030[3]. In such a competitive job market, PT organisations are struggling to hire and retain cybersecurity talent, especially OT experts.

Limited funding plays a role in this situation, as PT entities often face significant challenges in allocating sufficient resources to cybersecurity. Cybersecurity investments, e.g., for hiring experts at competitive salaries or implementing threat detection systems, must be balanced against a range of competing priorities. Cybersecurity may consequently be deprioritised, at the risk (particularly for smaller entities) of falling behind, in what the World Economic Forum defines as a widening cyber inequity gap: small(er) organisations are reaching a critical tipping point where they can no longer adequately secure themselves against the growing complexity of cyber risks[4].



→ HOCHBAHN's metro control centre, Hamburg, Germany © UITP

Addressing the cybersecurity OT skills gap

As IT and OT systems become increasingly interconnected, the demand for cybersecurity professionals with expertise in OT systems is growing, but such expertise is quite rare.

This gap can be dealt with by **enhancing existing OT experts' cybersecurity knowledge.** Upskilling OT experts in cybersecurity has proven more effective than attempting to hire and train cybersecurity professionals to become OT specialists.

To support this effort, in 2021, the Cyber Security Agency of Singapore developed an **Operational Technology Cybersecurity Competency Framework (OTCCF),** providing a structured pathway for OT professionals to develop cybersecurity expertise. PT companies can use the framework to identify key roles, expert profiles, and advantageous entry points into cybersecurity and establish career paths, necessary skills, and training requirements to develop OT cybersecurity capabilities within their workforce[5].

Upscaling cybersecurity: A case study

In 2023, KONE R&D and KONE IT launched a Cybersecurity Champions Programme, aimed at embedding cybersecurity expertise in operational teams. The Cybersecurity Champions are not new hires, but rather motivated existing team members who receive advanced, role-based training. They serve as the first line of security support within their teams, acting as local advocates and guides for secure development practices.

Key programme elements:

- → Targeted selection: The first batch of nominees was selected by research and development (R&D) and IT managers, focusing on experienced, high-performing staff with software development expertise and strong communication and organisational skills. The nomination process aimed for even coverage across different departments, and candidates had to be willing to learn and engage with security topics.
- → Immersive training: In the programme's kick-off phase, participants attended two intensive, offsite training weeks without laptops, ensuring full engagement. The content was tailored to different roles through breakout sessions, interactive workshops, and group exercises.
- → Certified external learning: Each participant complemented internal training with a certified external course relevant to their role. Passing an external certification exam both validated the training and provided more diverse security skills than could be developed in-house.
- → Graduation, certification, and empowerment: Graduates received a certificate and digital badge and took on responsibilities as trusted first-line cybersecurity advocates. The certificate conferred authority for security checks within process gates, enabling teams with a Certified Security Champion to operate in a more agile way, with less reliance on the central cybersecurity team.
- → The Certified Security Champion responsibilities include:
  - → Providing the first level of security support for their teams.
  - → Advising on required security measures in development projects and secure operation of applications.
  - → Hosting regular security "clinics" for peers.
  - → Supporting security audits—preparing and recording evidence of compliance.
  - → Ensuring that defined security practices are followed and identifying security gaps in implementation.

While batch-oriented classroom training was effective for the programme launch, KONE is transitioning to a continuous intake model for its maintenance phase. The new approach will be based on remote and recorded training sessions, with local workshops supplementing the lectures as needed. This offers greater flexibility, as it does not require assembling large groups, enabling participation without the constraints of group capacity or travel budgets.

Through the Champions Programme, KONE expanded its embedded cybersecurity capacity, strengthened the security culture to foster accountability, and created a sustainable model for scaling cybersecurity knowledge across the organisation.

Leveraging technology to bridge the cybersecurity skills gap

Investing in PT-specific cybersecurity solutions can help address the skills gap by providing operational teams with purpose-built visibility, automated threat detection, and intuitive response playbooks. These tools reduce reliance on deep OT cybersecurity expertise while enabling staff to identify and respond to threats in real time.

For instance, implementing a rail-specific security operations centre (SOC) can significantly streamline cybersecurity processes. The SOC is designed to contextualise alerts within the rail network's unique operational environment, reducing the need for cybersecurity analysts to possess extensive rail technology knowledge when performing triage, investigation, and incident response. However, the system should be supported by a small team of rail technology specialists with some foundational cybersecurity knowledge. These experts assist analysts where in-depth rail system understanding is required and coordinate with other departments (such as engineering, maintenance, operations control, and system manufacturers) during incident investigations and responses. In some organisations, operational control centre (OCC) personnel themselves may take on this specialist role, working closely with the SOC team to ensure rapid and informed responses whenever rail technologies are affected.

By supporting human expertise with purpose-built cybersecurity technology, PTOs can bridge the skills gap and develop a more resilient and self-reliant approach to cyber threat management.

→ Lima, Peru
© Fernando Narvaez

Protecting OT assets with long life cycles

PT systems rely on the complex integration of OT systems often designed decades ago, not for today's interconnected digital landscape.

Transport assets' long operational lifespan leads to embedded hardware and software becoming outdated or unsupported over time, requiring proactive obsolescence management. Obsolete equipment is more vulnerable to cyber-attacks, as it may not receive or support security updates, and integrating modern cybersecurity measures into legacy systems can be technically challenging and costly, often requiring customised solutions that balance security needs with operational continuity[6].

Even in the case of new systems, major project implementation or new asset commissioning often spans decades. By the time the new system or the first units of a train fleet are delivered, operators may already be facing the obsolescence of some of its equipment and components and a cybersecurity design no longer aligned with applicable regulations.

Project development or modernisation also brings its own risks; with the increasing integration of cloud services, IoT devices, and third-party applications, the cybersecurity perimeter becomes both broader and harder to control. Guidance and best practices on how to manage risk during a technology upgrade can be found in the Cybersecurity Committee's 2023 report on tendering[7].

Public transport is a cyber-physical system: Safety is at stake

Cyber-attacks on cyber-physical systems, which integrate computing, networking, and physical processes, pose significant safety risks. A breach in these systems can lead to direct physical consequences, such as disrupted operations, damaged infrastructure, or harm to human life.

Because OT systems control real-world equipment, cyber incidents can escalate beyond data loss and trigger critical safety failures.

With the growing frequency of attacks targeting critical OT infrastructure, a joint approach to safety and security is becoming indispensable. Security considerations must inform safety assessments; assumptions that bespoke systems or air-gapped architectures are immune to threats are no longer sufficient, and standards and regulations are evolving accordingly, as emphasised, e.g., by the upcoming IEC 63452 rail cybersecurity standard.

At the same time, the interaction between safety and cybersecurity poses significant challenges. Safety engineering addresses risks that stem from predictable failures (wear, design flaws, or human error) and can be quantified using historical failure rate data.

As a result, safety measures are stable, well-documented, and long-lasting, with controls designed around statistically established probabilities. In contrast, cybersecurity operates in a dynamic threat landscape, where risks evolve rapidly due to constantly emerging vulnerabilities, attacker ingenuity, and shifting threat actors. Cybersecurity risk requires continuous monitoring, adaptive defences, and timely updates to stay ahead of new and unforeseen attack techniques. This inherent difference means that it would not be possible, or even desirable, to have a system's safety case updated whenever the cybersecurity case needs to evolve.

It is increasingly important for safety and cybersecurity experts to build a mutual understanding of how cybersecurity can impact safety, even when systems are theoretically designed to fail safely, and ensure that a system's safety case is underpinned by a cybersecurity case.

To support the sector in addressing this challenge, the UITP Cybersecurity Committee is developing a set of guidelines on the cybersecurity of safety critical systems[8].

Strategic framework to strengthen cybersecurity governance in public transport organisations

UITP calls on PT executives to adopt a proactive, strategic approach to addressing cybersecurity challenges as they develop their business and digital strategies.

→ Bahia, Brazil
© CCR Image Library

Cybersecurity must be embedded in capital planning, procurement policies, and operations. As the PT sector increasingly seeks to modernise its legacy systems and deliver services through and with the support of digital channels, it is imperative to strengthen our cybersecurity approach by implementing a comprehensive cybersecurity governance framework.

The UITP Cybersecurity Committee recommends a model based on the United States (US) National Institute of Standards and Technology (NIST) Framework[9], as adapted by MTR Hong Kong. We propose this methodology as best practice for the sector in 2025, as it provides a holistic and dynamic approach to cybersecurity management that PT organisations can adapt to their own operational contexts.

Cybersecurity efforts need to evolve from merely implementing technical security controls — i.e., cyber protection — to a broader strategy focused on safeguarding core business objectives—cyber resilience. As defined in the World Economic Forum Cyber Resilience Compass, the goal of cyber resilience is not just to prevent cyber incidents, but to minimise their impact on an organisation's primary goals and objectives, such as maintaining critical services, safeguarding stakeholder confidence, protecting strategic value, and promoting long-term growth[10].

The proposed Cybersecurity Governance Framework is developed around seven core principles, as illustrated in Figure 2, based on a corporate cybersecurity governance model. This is supported in the outer layers of the graphic with recommended organisational and technical approaches. Together, they provide a comprehensive ecosystem for cybersecurity risk and management in a digitally enabled PT system.

Figure 2: Corporate Cybersecurity Governance Model for public transport companies, adapted from NIST by MTR Hong Kong

The following section describes the seven core segments in more detail and presents an overview of the key elements to consider in the framework's implementation, pointing to further resources and recommendations when available.

1. Organisation

PT entities must create comprehensive cybersecurity policies outlining their security approach. This starts from the top: the executive level needs to be aware of the organisation's cyber risk landscape and how it impacts business. It is also their responsibility to develop a comprehensive cybersecurity framework to ensure that adequate resources (financial, technological, and human) are allocated to cybersecurity initiatives and support investments in cybersecurity tools, training, and infrastructure. Policies should include guidelines for data protection, incident response, and employee responsibilities.

Specific areas of attention & recommendations for implementation:

1A. Cybersecurity roles and responsibilities

- → Establish defined roles, assign responsibilities, and clarify reporting lines[11].
- → Ensure that users, senior executives, and cybersecurity personnel understand their roles and responsibilities.
- → Inform and train users about the organisation's cybersecurity architecture, policies, procedures, and implementation.

→ Hangzhou, China

1B. Policy, standards, and procedures

Creating a successful cybersecurity plan involves a comprehensive approach to policies, standards, and processes. Here are the key steps an organisation should consider:

→ 1B.1. Establish clear policies

- → **Define cybersecurity objectives:** Outline the cybersecurity plan's key goals, such as protecting sensitive data, ensuring business continuity, and complying with regulations.
- → **Access control:** Implement policies that define who has access to what information and under what circumstances.
- → **Incident response:** Develop a clear cybersecurity incident response policy, including reporting procedures and recovery plans.

→ 1B.2. Adopt recognised standards

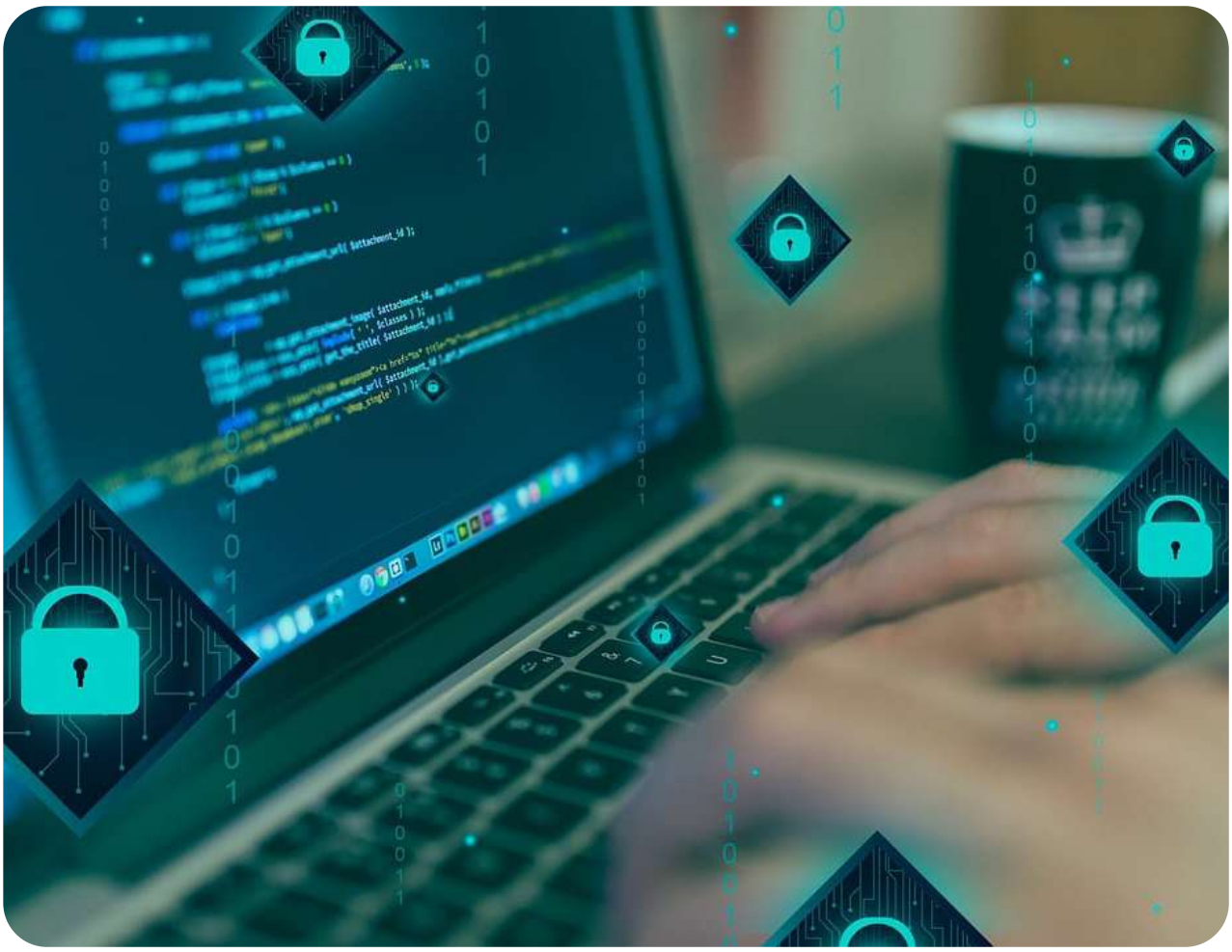
Adopting cybersecurity standards is a crucial step for organisations to ensure robust protection against cyber threats. Determine which cybersecurity standards are applicable to your profile and your regulatory environment. Conduct a gap analysis to compare your current cybersecurity practices with the standards. Identify areas where your organisation needs to improve. Common standards include:

- → The **NIST Cybersecurity Framework,** which provides guidelines on cybersecurity risk management and reduction.
- → **ISO/IEC 27001,** which specifies requirements for establishing, implementing, maintaining, and continually improving information security management systems[12].

→ 1B.3. Implement robust processes

Create a detailed plan to address the identified gaps, including timelines, responsible teams, and specific actions to achieve compliance with the standards. Educate employees about the new standards and their roles in maintaining compliance. Regular training sessions and awareness programmes are essential. Implement monitoring tools and processes to ensure ongoing compliance. Regularly review and update your cybersecurity practices to address new threats and changes in standards. Consider undergoing external audits to verify compliance. Certification can enhance your organisation's credibility and demonstrate your commitment to cybersecurity.

- → **Risk assessment:** Regularly conduct risk assessments to identify vulnerabilities and threats to your organisation's information systems.
- → **Continuous monitoring:** Implement continuous monitoring processes to detect and respond to security incidents in real time.
- → **Training and awareness:** Ensure all employees are trained on cybersecurity best practices and aware of the latest threats and how to mitigate them.



→ 1B.4. Regularly review and update cybersecurity policies

Regular cybersecurity reviews and updates are essential for maintaining a strong security posture. Organisations should conduct regular assessments to identify vulnerabilities and risks. Consider the use of tools like penetration testing and vulnerability scanning to evaluate your systems. Review and update cybersecurity policies to reflect new threats and regulatory changes. Ensure policies are communicated effectively to all employees.

- → **Audits and compliance:** Regularly audit your cybersecurity policies and processes to ensure compliance with relevant laws and standards.
- → **Update policies:** Continuously update your policies and procedures to adapt to new threats and technological advancements.

→ 1B.5. Collaborate and share information

- → **Industry collaboration:** Engage with industry groups and cybersecurity communities to share information about threats and best practices.
- → **Government resources:** Use resources provided by government agencies like Cybersecurity and Infrastructure Agency (CISA), which offer guidelines and support for enhancing cybersecurity.

→ Munich, Germany
© Alex Fu

2. Risk management

Cybersecurity risk management is a continuous process of identifying, analysing, evaluating, and addressing your organisation's cybersecurity threats to avoid safety, regulatory, financial, and reputational harms related to cyber incidents while simultaneously ensuring operational continuity. Employees and business unit leaders often view risk management from the perspective of their business function, but in the case of cybersecurity risk management, everyone in the organisation has a role to play.

Cybersecurity risk management best practices involve a comprehensive, proactive approach. We call on PT executives to promote a holistic approach and address risk in a comprehensive, consistent manner: PT organisations must regularly conduct risk assessments to identify potential threats and vulnerabilities and prioritise risks based on their potential impact and likelihood.

Specific areas of attention & recommendations for implementation[13]:

2A. Internal and external risk management

→ Establish and manage cybersecurity risk management processes.

→ Define and document your organisation's cybersecurity risk tolerance.

→ Set up specific authorisation, approval, and log-in processes for remote maintenance.

→ Set up third-party personnel and systems screening & authorisation prior to connection to networks and systems; control and monitor third-party access to systems.

2B. Cybersecurity risk evaluation

→ Identify cyber threats and their potential impact on your organisation.

→ Determine cybersecurity risks on the basis of threats, vulnerabilities, likelihood, and impact.

→ Perform cybersecurity risk assessments regularly.

3. Situational awareness

In cybersecurity, **situational awareness** means having a clear and current understanding of your organisation's digital environment. It involves regularly assessing and monitoring network activity, user behaviour, and system vulnerabilities to identify risks and emerging threats.

Originally a military concept, situational awareness is now vital for protecting complex systems such as metros and light rail networks. It enables leaders to anticipate cyber risks, make informed decisions, and respond quickly to incidents.

By embedding situational awareness in daily operations, PT organisations can shift from reacting to attacks to proactively strengthening resilience. A continuous, organisation-wide understanding of the digital environment is key to maintaining safe, reliable, and trusted services.

Specific areas of attention & recommendations for implementation:

3A. Information management

→ Identify your organisation's critical services and the corresponding dependencies.

→ Ensure that system diagrams and data flows are kept up-to-date.

→ Establish & manage a baseline of normal user, system, and network behaviour.

3B. Intelligence collection and analysis

→ Collect threat intelligence from internal and external sources.

→ Analyse threat intelligence to understand attack targets, attack methods, and potential impact on systems in the organisation.

4. Threat management

Cybersecurity threat management is the proactive process of identifying, assessing, and mitigating potential cyber risks to protect an organisation's digital assets, operations, and stakeholders. It ensures that threats are detected early, prioritised according to their potential impact, and addressed through appropriate security measures and response plans.

Cybersecurity threat management is critical for PT organisations to safeguard operations, assets, and passengers. Integrating a structured approach to threat management into daily operations can enable PT executives to prioritise risks, implement effective security controls, and ensure rapid response to incidents.

Best practices involve continuously monitoring networks and systems to detect and identify potential threats. Organisations typically use monitoring tools like security information and event management (SIEM) and intrusion detection systems (IDS), which detect system anomalies.

Organisations need to evaluate threats' likelihood and potential impact and prioritise risks based on their severity and impact. To prevent threats, they should implement security controls such as firewalls, encryption, and access controls and regularly update and patch systems to address vulnerabilities.

Furthermore, organisations need to develop and maintain an incident response plan to address security breaches and conduct regular drills and simulations to ensure preparedness, as detailed in section 5. They should regularly review and update threat management practices to tackle new and evolving threats, incorporating feedback and lessons learned from past incidents.

Specific areas of attention & recommendations for implementation:

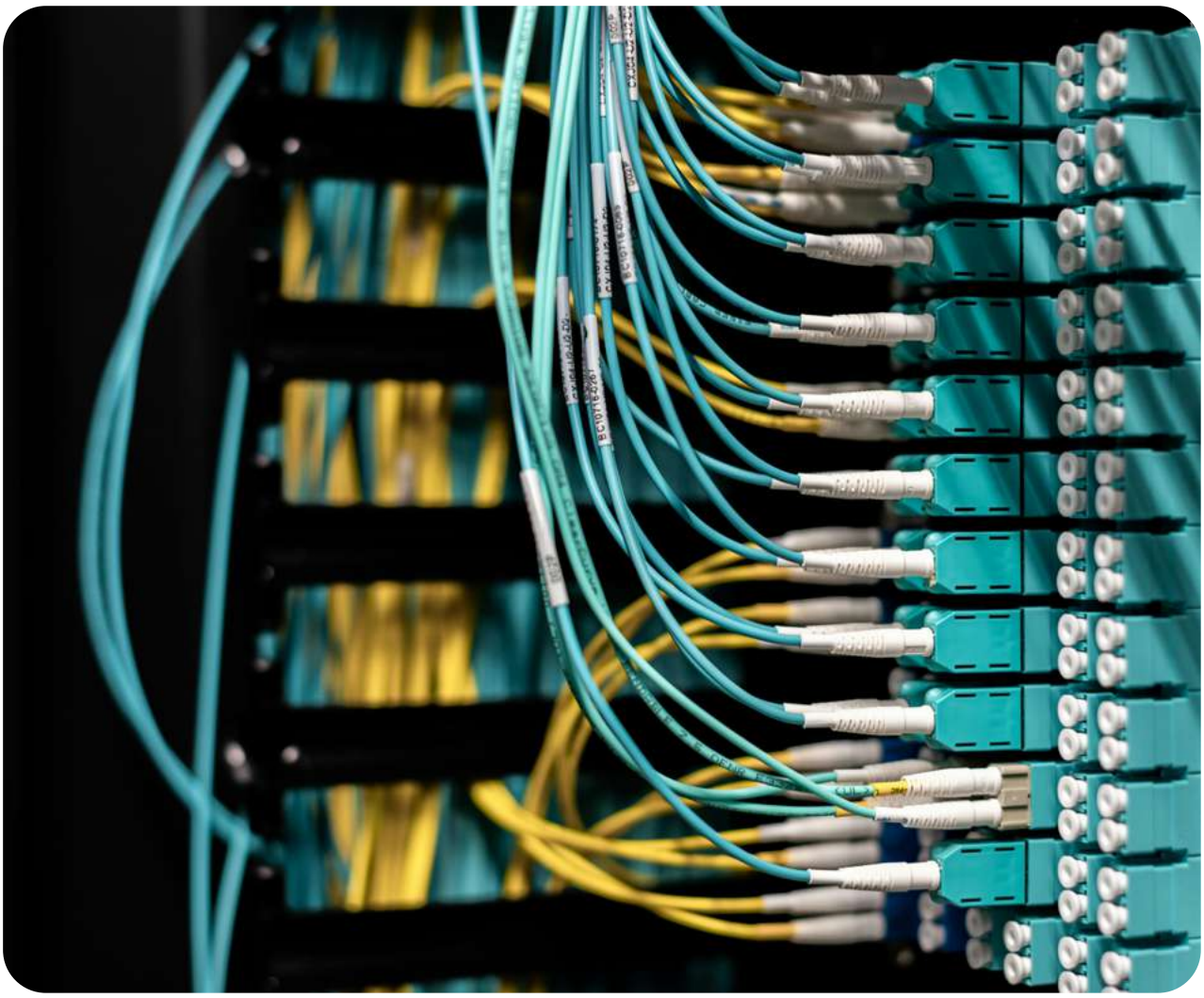
→ Bahia, Brazil

© Erik Mclean

4A. Vulnerability management:

Develop and implement a vulnerability management plan covering the following elements:

- → Make vulnerability disclosure a contractual obligation for suppliers.
- → Vulnerabilities should be mitigated or documented as accepted risks.
- → Establish robust patch management procedures. Whenever this is not possible, evaluate and document risk when not patching.
- → Establish key performance indicators (KPIs) for vulnerability management.
  Suggested indicators:
  - → Time required to address critical vulnerabilities.
  - → Average demand closure time.
- → Minimise and monitor external connections.
- → Manage remote access with appropriate security mechanisms.
- → Credentials should be properly managed.
- → Implement network segregation, considering the 'zero trust network approach' for critical systems: micro-segmentation enables authentication and access control at the level of devices, applications, and users, even within the same network segment, thereby reinforcing the security posture.
- → Encrypt sensitive data.
- → Ensure adequate system capacity to guarantee availability.
- → Implement protective measures against data leaks.
- → Check data and system integrity.
- → Scanning production systems is costly and can introduce risk: an alternative is to use test platforms that mirror production systems.



© Brett Sayles

4B. Configuration management

→ Define a baseline system configuration with minimum cybersecurity requirements; measure and control deviations.

→ Set up configuration change control processes; ensure that changes are logged.

→ Set up identity and credential management.

→ Continuous testing and validation.

4C. Detection and protection

→ Protect and monitor control networks and systems to detect potential cybersecurity events.

→ Set up malicious code detection.

→ Restrict the use of removable media in accordance to the defined cybersecurity policies.

→ Communicate and investigate detection information.

→ Set up regular testing and capability feedback loops.

5. Incident management

A cybersecurity incident management framework is a strategic approach designed to detect, manage, and minimise the impact of cyber-attacks. It provides a structured process for businesses to respond effectively to security incidents, ensuring minimal damage and rapid recovery. The key to effective cybersecurity incident management is preparation and organisation. Understanding the importance of a solid incident management framework is the first step towards a resilient cybersecurity response.

Specific areas of attention & recommendations for implementation:

5A. Incident response

→ Set up and test a cybersecurity incident response plan, including clearly defined roles, responsibilities, and immediate and subsequent actions.

→ Report cybersecurity events in a timely manner to the authorities and relevant stakeholders.

→ Classify cybersecurity incidents according to impact and severity.

→ Communicate and train your staff: they should know their roles and responsibilities in the case of cybersecurity incidents.

5B. Recovery and business continuity

→ Set up a cybersecurity recovery plan and business continuity plan.

Preparing for communications disruptions is crucial to ensuring business continuity: an alternative communication system should be established for key individuals within the organisation in the case of public networks (4G/5G) being unavailable or saturated or when internet connectivity is disrupted. This will accelerate recovery and ensure continuity of critical operations.

San Francisco, USA ←
© Ted Eytan

Figure 3: Business continuity plan
Source: US Department of Homeland Security

The Achilles heel: Dependencies & secondary impacts

When developing a business continuity or disaster recovery plan, it is crucial to account for **internal dependencies and cyber-attacks' potential secondary impacts.** Cyber incidents often cause collateral damage that extends beyond the initially targeted system, triggering cascading effects across the organisation, similar to a supply chain attack, but occurring within internal networks. For instance, a breach of enterprise IT systems such as email, identity management systems, or network infrastructure can disrupt OT systems, even if the OT systems remain technically uncompromised. These internal interdependencies, if overlooked, can undermine continuity efforts and delay recovery. Effective planning must go beyond siloed recovery strategies and instead ensure a holistic understanding of how IT and OT systems interact, identifying critical touchpoints and shared services. This integrated approach will help organisations recover more quickly and effectively, while minimising unexpected disruptions during a cyber crisis.

Secondary impacts can include the following:

→ **Data corruption and loss:** Cyber-attacks can inadvertently corrupt or delete data, impacting businesses and individuals who were not the primary targets; loss of passwords, access to email, customer contacts, facility management capabilities, and diary systems can be highly disruptive.

→ **Service disruptions:** Attacks like DDoS can cause widespread service outages, affecting users and organisations that rely on the targeted services, such as web services for passenger information, bookings, ticketing, and top-ups.

→ **Economic impact:** Cyber-attacks can lead to significant financial losses for businesses due to downtime, recovery costs, and loss of customer trust, e.g., when the attacks target ordering and invoicing, staff payment, and human resources (HR) systems..

→ **Privacy violations:** Sensitive information may be exposed, leading to privacy breaches for individuals whose data was not the intended target. For example, when customer loyalty programmes are hacked, passwords, personal data, and banking details are exposed.

→ **Physical damage:** In some cases, cyber-attacks have caused physical damage to infrastructure, such as power grids or industrial systems; this causes loss of power to critical systems and communication networks.

→ **Passenger trust:** In an increasingly digitalised environment (apps, IoT, and connected services), digital trust is a key driver of PT adoption, and cybersecurity plays an essential role in a positive passenger experience. Service disruptions (e.g., ticketing, traffic information, and mobile apps) impact passenger comfort and trust, and data breaches can damage the passenger relationship and the operator's reputation.

© Anzhelika Costin

6. Governance

The Cybersecurity Governance Framework outlines the principles, responsibilities, and protocols to protect the organisation's digital assets, ensure operational resilience, and comply with legal and regulatory requirements. It is designed to safeguard the PT company's information systems, infrastructure, and customer data while supporting its mission to deliver safe, reliable, and efficient services.

Specific areas of attention & recommendations for implementation:

6A. Organisation effectiveness

→ Define accountability, identifying roles and responsibilities.

→ Define and prioritise risk responses.

→ Define risk tolerance, based on an organisation-specific risk analysis.

6B. Programme management

→ Establish risk management processes.

6C. Compliance

→ Ensure compliance with cybersecurity regulations, policies, and reporting requirements.

7. Additional requirements

NIST has several publications detailing additional security and privacy requirements:

- NIST Special Publication (SP) 800-53 Rev. 5: This document includes security and privacy controls for information systems and organisations. The latest update (Release 5.1.1) introduces new controls and enhancements related to identity providers, authorisation servers, cryptographic key protection, and token management.
- NIST Special Publication (SP) 800-172: This supplement to SP 800-171 provides enhanced security requirements for protecting controlled unclassified information (CUI) in non-federal systems and organisations. It focuses on advanced persistent threats and includes additional controls for high-value assets.
- NIST Special Publication (SP) 800-63: These Digital Identity Guidelines provide detailed requirements for identity proofing, authentication, and life cycle management of digital identities.

Based on MTR's experience, additional elements to address in PT companies include:

7A. Anomalies, events and detection

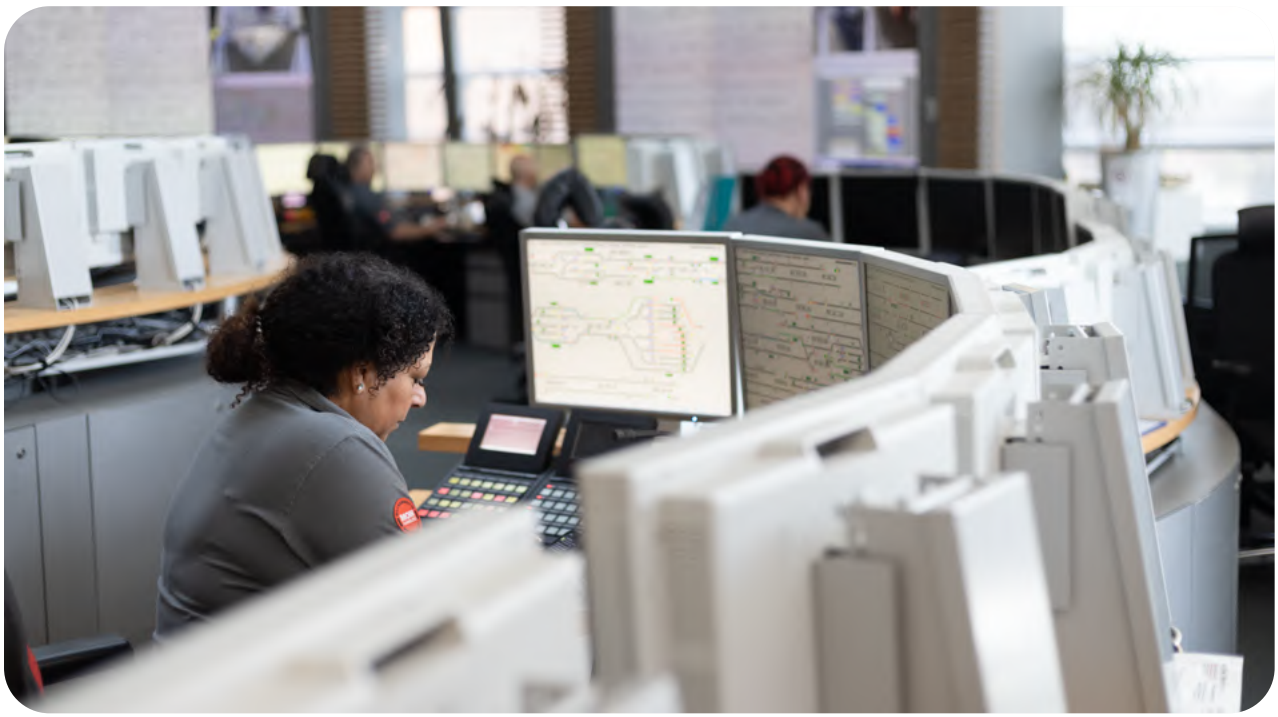
- Cyber event data should be aggregated and correlated.

7B. Asset management

- Set up asset inventories to facilitate monitoring and patch management.
- Information backups should be conducted, maintained, and tested periodically.
- It may be necessary to define the cybersecurity system's initial scope and then establish a progressive approach that continues to incrementally identify both processes and relevant systems to provide a pathway for growth and adaptation over time.

7C. Additional protection

- All critical systems should be designed with redundancy for resilience.



→ Hamburg, Germany
© UITP

Further considerations for implementing an effective cybersecurity framework

When developing a cybersecurity governance framework, PTOs and PTAs need to keep in mind the importance of **prioritising cyber resilience over mere compliance.** While regulatory compliance is important, treating cybersecurity as a checklist exercise can lead to a false sense of security, overlooking real operational risks and emerging threats. A governance framework that focuses solely on satisfying external requirements may miss critical vulnerabilities or fail to adapt to evolving attack landscapes. In contrast, emphasising cyber resilience ensures that the organisation is not only meeting baseline standards but also building the capacity to anticipate, withstand, recover from, and adapt to cyber incidents. The ultimate goal of any cybersecurity framework should be to protect the integrity, availability, and continuity of essential systems and services, especially in high-dependency sectors like public transport, treating security as a core, dynamic element of operations, not just a compliance obligation.

Adopting **cybersecurity by design** is essential for building resilient PT systems. Rather than relying solely on procedural controls or retrofitting protections after deployment, cybersecurity must be integrated from the earliest stages of system design and development. Incorporating security principles such as least privilege, secure architecture, threat modelling, and encryption into the foundational design ensures that systems are inherently more resistant to compromise. Procedures, policies, and checklists are important, but they are not sufficient if the underlying infrastructure is fundamentally insecure. By adopting a cybersecurity-by-design approach, organisations proactively reduce vulnerabilities, minimise attack surfaces, and create systems that are both functional and secure by default, laying a strong foundation for sustainable, long-term cyber resilience.

For PT systems, **IT-OT integration** should be the focus of detailed planning, due to the increasing convergence of digital technologies with operational infrastructure. As fare collection, vehicle diagnostics, traffic control, and signalling systems become more connected to enterprise IT networks, the interfaces between these domains represent critical points of vulnerability. OT systems are often not designed with cybersecurity in mind, and introducing connectivity without proper safeguards can expose them to threats. It is therefore vital to embed IT security principles in OT environments, ensuring secure data flows, access controls, and monitoring mechanisms across both domains. Strengthening these integration points will enhance the PT system's overall resilience in the face of evolving cyber risks.

Physical security remains the last line of defence in PT cybersecurity, as critical systems are widely distributed and often accessible in public spaces. While technical controls, such as firewalls, encryption, and monitoring, are essential, they can be rendered ineffective if unauthorised individuals gain physical access to servers, control panels, network switches, or onboard vehicle systems. A physical breach can allow direct manipulation or sabotage of operational technology, bypassing digital protections entirely and causing severe disruptions to service, safety, and infrastructure. Effective cybersecurity governance must therefore treat physical security as an integral component, incorporating measures such as access controls, surveillance, tamper detection, and secure housing of critical assets to prevent physical intrusion and ensure operational continuity and integrity.

→ Ostrava, Czechia
© Ivan Delichristov/
DPO

Conclusion

There is no one-size-fits-all solution to cybersecurity; each organisation's approach must be tailored to its specific context, taking into consideration the applicable regulatory framework and available resources.

At the same time, cybersecurity is no longer optional; in an increasingly digital and interconnected PT sector, it has become a fundamental requirement. Nevertheless, with a worsening cybersecurity threat landscape, preventing all cyber incidents is impossible. PT entities should therefore embrace a cyber resilience mindset, aiming at minimising incidents' potential impact on critical infrastructure and systems to ensure passenger and personnel safety, operational continuity, and public and stakeholder confidence.

Ultimately, public confidence in PT systems depends on safety, reliability, and trust, and these are increasingly underpinned by and dependent on digital infrastructure. In a sector built on public service, cybersecurity is not just about preventing attacks; it is about protecting the essential mobility lifelines that keep cities and communities running.

→ Manila, Philippines
© Charles Edward Cansino

Key cybersecurity questions that PT executives should be able to answer (or need to ask)

→ **Governance and strategy**

Who is accountable for cybersecurity at the executive level?
Do we have an up-to-date cybersecurity strategy aligned with operational priorities?

→ **Risk management and audits**

What are our most critical assets and services from a cyber risk perspective?
Are we proactively managing the cybersecurity risks that arise from IT-OT integration?
When did we last conduct a cybersecurity audit? What were the recommendations?
Who is responsible for implementing them and by when?

→ **Third parties and legacy systems**

Do we have processes in place to ensure that third-party vendors, contractors, and suppliers meet our cybersecurity requirements?
Do we have a plan in place to manage cybersecurity risk in our legacy systems?

→ **Staff training & culture**

Do we have a staff cybersecurity training plan in place?
Are staff and operators aware of cyber risks relevant to their role?
Do we have the skills we need to effectively manage cyber incidents? Do we need to recruit new staff?

→ **Incident preparedness & business continuity**

Do we have a tested cyber incident response and recovery plan that includes business continuity for both IT and OT environments?
Who is responsible for it, when was it last exercised, what were the recommendations, and when will they be implemented?

→ **Cybersecurity maturity matrix**

Do we have a cybersecurity maturity matrix in place?
How are we doing, and what do we need to achieve in the next 12/24 months?
Are we continuously improving based on lessons learned and new threats?

© Tima Miroshnichenko

References

[1] Europol (2025), 'European Union Serious and Organised Crime Threat Assessment – The Changing DNA of Serious and Organised Crime', Publications Office of the European Union, Luxembourg, accessed May 2025.

[2] ENISA (2024), 'ENISA Threat Landscape 2024', accessed May 2025.

[3] World Economic Forum, 'Strategic Cybersecurity Talent Framework' White Paper, April 2024.

[4] World Economic Forum, 'Global Cybersecurity Outlook 2025', January 2025.

[5] 'Operational Technology (OT) Cybersecurity Competency Framework', October 2021, CSA Singapore.

[6] For recommendations on how to address this challenge, see the UITP Cybersecurity Committee Report 'Obsolescence on Operational Environment and Cybersecurity', 2022, available to UITP members through MyLibrary.

[7] 'Practical Guidance on Cybersecurity Requirements in Tendering', 2023.

[8] 'UITP Design Guidelines on Security of (Rail) Safety Critical Systems', expected for publication in 2026.

[9] National Institute of Standards and Technology, 'NIST Cybersecurity Framework 2.0', 2024.

[10] World Economic Forum, 'Cyber Resilience Compass', April 2025.

[11] For guidance on cybersecurity roles, consult ENISA's Report 'Cybersecurity Skills and Roles for NIS2 Essential and Important Entities', June 2025.

[12] For a more comprehensive list of cybersecurity standards and technical specifications, consult sections 2.2.3 and 2.2.4 in the UITP Europe Report 'Technical Specifications on Safety, Security and Cybersecurity Applicable for Non-SERA Urban Rail Systems in the European Union', January 2025, available to UITP members in MyLibrary.

[13] For a more detailed set of recommendations on cybersecurity risk management, refer to the dedicated UITP Report 'Cybersecurity Risk Assessment for Public Transport Operators'.

This is an official publication of UITP, the International Association of Public Transport. UITP has more than 2,000 member companies in 100 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.

UITP ADVANCING PUBLIC TRANSPORT

Legal deposit: D/2026/0105/08 - Rue Sainte-Marie 6, B-1080 Brussels, Belgium | Tel +32 (0)2 673 61 00 | info@uitp.org | **www.uitp.org**