Moving with confidence in rail and transit

How to address the cybersecurity challenge

accenture

Securing the safety of rail and transit infrastructures has never been more challenging. Cyberespionage, cybercrime, hacktivism. All are exponentially on the rise. And all have the potential to paralyze transit networks increasingly reliant on technologies that enable data sharing across multi-partner mobility ecosystems.

The industry urgently requires better defense mechanisms. Operators must be ready to recognize cyber risk in all its forms. They need to be able to act swiftly to tackle cybersecurity challenges as and when they arise. They should also be confident enough to cope with sudden systemic shocks—from pandemics to terrorism—that threaten to complicate their responses.

Some operators are starting to develop these strengths and competencies. By adopting a multi-stranded cybersecurity program, based on a set of robust core capabilities, they are learning to leverage innovation in the security space while respecting data privacy and security. Applied with a determined focus on continuous improvement, such an approach can help boost the safety and resilience of the transit value chain, end-to-end.

New technologies, new partners—and new security challenges

New technologies and digital partnerships are dramatically improving both the operational efficiency of rail and transit enterprises and the quality of their customers' experiences.

Consider, for example, how traditional transportation services have been transformed into an integrated mobility offering by incorporating third-party add-ons such as parking, car-sharing and ride-hailing. Or how a combination of leading-edge technologies including Cloud, the Internet of Things (IoT), Industrial Internet of Things (IIoT), Artificial Intelligence (AI) and Robotic Process Automation (RPA) is helping to optimize business efficiencies.

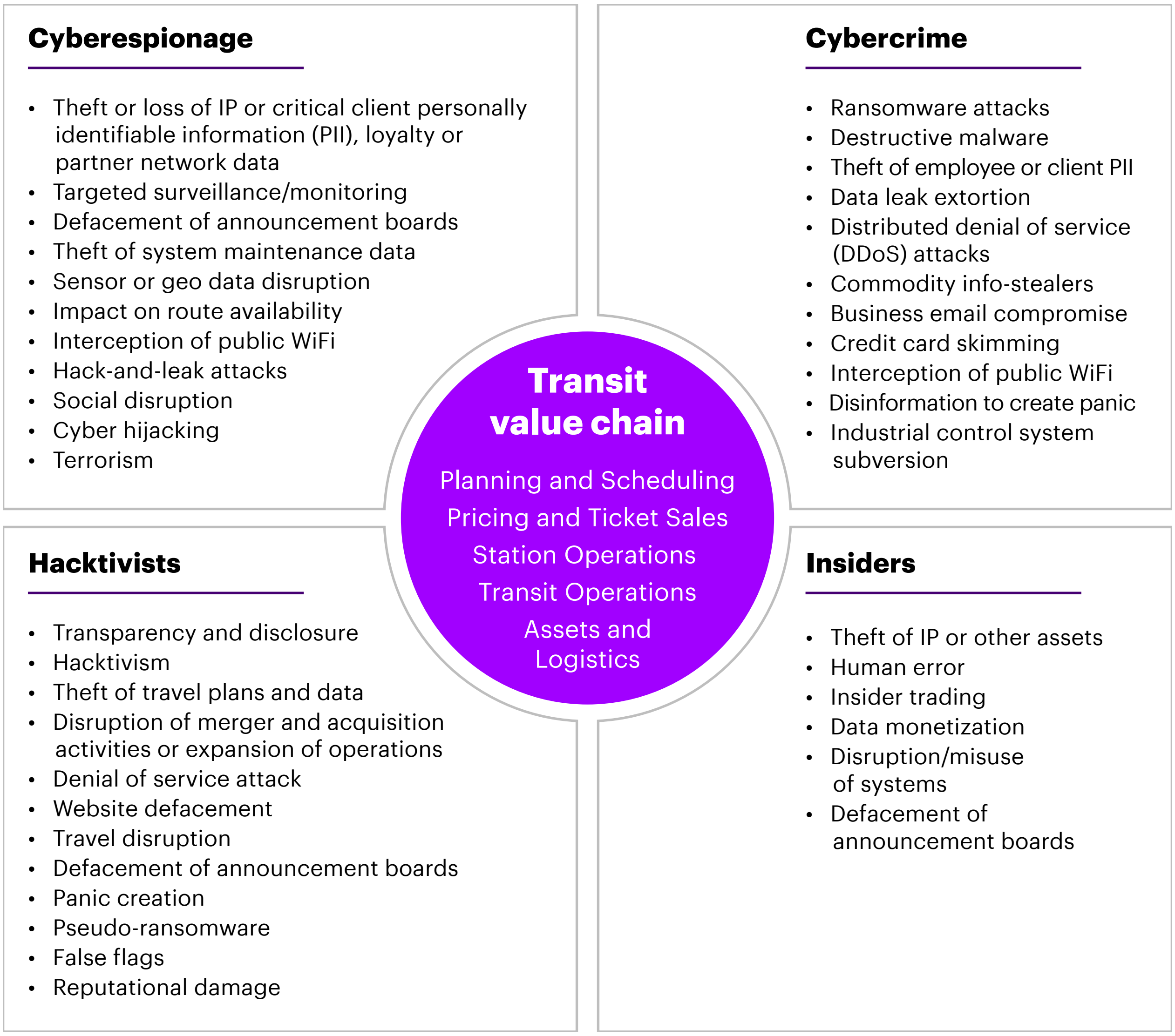
Yet these same digital initiatives and innovations are also compounding the cybersecurity challenge. The convergence of information technology (IT), operations technology (OT) and IoT/IIoT infrastructure and services—including assets leveraging third-party platforms—has greatly escalated security risk.

Furthermore, as rail and transit's highly dispersed traditional operations combine with an emerging mobility ecosystem sustained by these convergent technologies, the risk to operational security and passenger safety is becoming increasingly cross-industry and even trans-national in nature.

An expanding “attack surface”

New technologies and the way they converge pose a challenge to the security of the entire transit value chain. Planning and scheduling, pricing and ticket sales, station and transit operations, assets and logistics—no area is immune from attack (see Figure 1).

FIGURE 1. Examples of cyber threats to the transit value chain



Cyberespionage

- Theft or loss of IP or critical client personally identifiable information (PII), loyalty or partner network data
- Targeted surveillance/monitoring
- Defacement of announcement boards
- Theft of system maintenance data
- Sensor or geo data disruption
- Impact on route availability
- Interception of public WiFi
- Hack-and-leak attacks
- Social disruption
- Cyber hijacking
- Terrorism

Cybercrime

- Ransomware attacks
- Destructive malware
- Theft of employee or client PII
- Data leak extortion
- Distributed denial of service (DDoS) attacks
- Commodity info-stealers
- Business email compromise
- Credit card skimming
- Interception of public WiFi
- Disinformation to create panic
- Industrial control system subversion

Transit value chain

Planning and Scheduling
Pricing and Ticket Sales
Station Operations
Transit Operations
Assets and Logistics

Hacktivists

- Transparency and disclosure
- Hacktivism
- Theft of travel plans and data
- Disruption of merger and acquisition activities or expansion of operations
- Denial of service attack
- Website defacement
- Travel disruption
- Defacement of announcement boards
- Panic creation
- Pseudo-ransomware
- False flags
- Reputational damage

Insiders

- Theft of IP or other assets
- Human error
- Insider trading
- Data monetization
- Disruption/misuse of systems
- Defacement of announcement boards

Source: Accenture

Until recently, cyber risk was largely the responsibility of IT; a relatively simple matter of securing sensitive operator and customer data. Now, however, as technologies converge, more such risks are associated with OT, IoT and IIoT, whose security poses different challenges.

Securing OT is particularly testing, largely because OT devices and systems, which control the safe operation of rail and transit networks, must cope with ageing legacy technologies, siloed operations, and difficulties in tracking how data moves between OT and IT systems.

Similarly, the exploding use of networked IoT devices to support operational infrastructure—including track load-bearing monitors, heating ventilation and air conditioning (HVAC) sensors, wheel and brake monitors and traffic automation monitors—generates massive amounts of data that need to be reviewed for anomalies and potential indicators of cyber incidents. What's more, because many such devices lack inherent security, they create significant vulnerabilities for their wider networks.

Thanks to the ongoing integration of services, those networks are constantly expanding. The development of Mobility as a Service (MaaS), which allows high volumes of user data to be exchanged via multi-operator technology platforms, is already challenging data protection protocols. As more third-party relationships emerge—such as, when rail and transit operators allow other service providers to use their infrastructure more directly, or when ride-sharing companies bring autonomous vehicles into the rail and transit environment—the potential attack surface increases significantly.

As technologies converge, more such risks are associated with OT, IoT and IIoT, whose security poses different challenges.

A multi-stranded approach can build resilience

The vulnerabilities and risks that result from all this require an approach that takes account of multiple components, from the individual to the integrated. By establishing a strong yet agile security program, organization-wide, incorporating all partners and stakeholders and targeting all areas of the transit value chain with continuous improvements as new technologies materialize, operators can minimize disruptions and mitigate security concerns (See Figure 2).

FIGURE 2. Core capabilities

Rail and Transit Security Program Management

Assess **security policy and standards**

Design and launch security **Governance Commitee Structure**

Develop **security dashboard**

Security Requirement Assurance

Assess **Product Lifecycle Management (PLM)/Application Lifecycle Management (ALM) capability** from security perspective

Design **traceability assurance**

Enhance PLM/ALM to **manage rail and transit security** requirements, vulnerability and testing results

Security by Design

Apply security policy and standards to **systems design**

Analyze security **risks** and define requirements

Review systems design and configuration from a security perspective

Operations Technology Security

Assess and improve **OT security governance and strategy**

Design and develop **OT security controls**

Deploy **managed OT security operation service**

Transit Security Incident Response Team Operation

Design **IoT platform** to monitor and detect security incidents

Integrate PLM/ALM information into TSIRT operation

Design and develop **TSIRT operation dashboard**

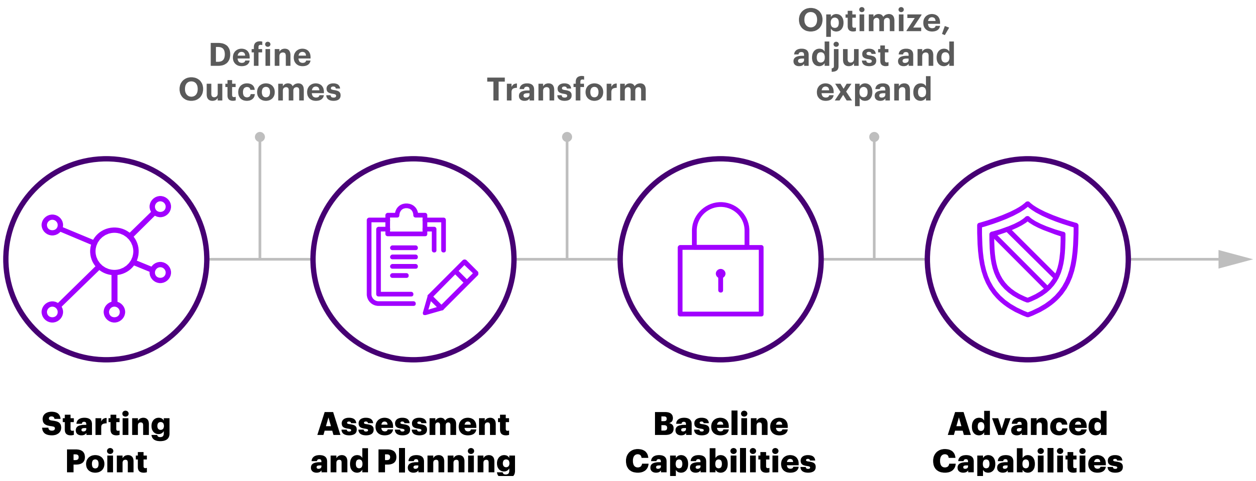
End-to-end Security Testing

Conduct **penetration testing** for IoT platform, network, IT/OT/IIoT and third-party ecosystems platforms

Plan and deliver **team training**

A resilient response to the mounting cybersecurity challenge in rail and transit should also mature over time—hence the need for a mindset of continous improvement. By applying a lifecycle approach, operators can leverage new security innovations to meet emerging operating and customer experience demands as they arise (See Figure 3).

FIGURE 3. A lifecycle of continuous improvement



STEP 1: Define the desired security outcomes, including assessment and planning outcomes

- Create a Transit Security Program Charter
- Identify the transit industry and extended ecosystem processes
- Develop an inventory of people, assets and data

STEP 2: Establish baseline capabilities

- Develop policies and standards
- Implement a vulnerability and patch management capability
- Infrastructure transformation where needed to support the policies, standards, and baseline capabilities

STEP 3: Establish advanced capabilities

- Implement a Transit Systems security monitoring and an Open Source Intelligence (OSINT) program to widen the threat intelligence spectrum around operations and customer experiences
- Perform consistent penetration testing on applications and infrastructure including advanced simulation exercises
- Establish an insider threat management capability

Some rail and transport players are already reaping the rewards of such a multi-stranded approach. Case in point: a North American public transport operator that has significantly boosted its cybersecurity capability by mobilizing a security operations center to ensure continuous monitoring.

Mobilizing a Security Operations Center

After building foundational elements to improve the security maturity of the organization, an automated fare collection system for public transport in North America looked to operationalize key components of its security program by ensuring continuous monitoring of the new system for potential cyber threats. The organization partnered with Accenture to mobilize and operate its Security Operations Center (SOC).

Within three months, a team had been mobilized, necessary processes had been tested and documented and appropriate tools were employed to:

- Enhance security monitoring with new procedures for threat detection, analysis and complex incident management
- Incorporate new and fine-tuned use cases for security event detection, and implement approved system integrations and onboarding security information sources
- Perform scans and report on vulnerabilities and severity to stakeholders
- Identify specific and industry-relevant threat intelligence feeds to be integrated into the platform.

The organization's overall security maturity improved significantly with 24/7 threat monitoring and investigation, faster vulnerability identification using infrastructure scans, and more timely and accurate stakeholder communications of potential threats.

Constant vigilance and the human dimension

In a fast-changing world "cybersecurity" is a relative concept. New risks will arise continuously. Hence the need for constant vigilance—and a clear and consistent focus on the human dimension.

Data privacy issues will not only persist but are likely to intensify as transit operators introduce new technologies and partners and expand their ecosystems' service offerings. Additional user experiences to help customers self-manage such transit experiences as trip planning and the scheduling of third party services, or measures to optimize the availability of parking spots and ride shares will require a better understanding of customer behaviors.

But this in turn involves collecting more and more customer data and sharing it with an expanding universe of ecosystem partners—opening the door to yet more opportunities for potential cyber sabotage. COVID-19-related contact-tracing measures have complicated the picture. As new, post-pandemic data security regulations are implemented, organizations would have to decide how best to ensure the security of passengers, employees and their own systems without compromising privacy.

In short, transit organizations are under persistent pressure to enhance the effectiveness of their security programs, look for ways to innovate securely, and provide transparency to the customer with respect to their data and how it is used.

A multi-stranded approach to cybersecurity, as described, can help build the resilience organizations need. It takes full account of the convergent technologies and expanding ecosystems that are driving the spread of cybersecurity risks. It provides a framework of core capabilities robust enough to tackle them.

And by affirming the critical importance of continuous improvement it helps ensure that organizations' resilience matures over time, facilitating them to respond in a timely and appropriate fashion to their own and their customers' emerging needs. Armed with such an approach to the challenges of cybersecurity, rail and transit operators can move forward with confidence.

Key contacts/Authors

PIERRE-OLIVIER DESMURS
Managing Director — Rail and Transit, Global Lead
p-olivier.desmurs@accenture.com

MICHAEL ENGLISH
Managing Director — Rail and Transit, North America Lead
michael.english@accenture.com

TYLOR TRUONG
Managing Director — Accenture Security, Canada
tylor.truong@accenture.com

KEVIN O’BRIEN
Senior Principal — Accenture Security, Canada
kevin.obrien@accenture.com

For more information visit:
https://www.accenture.com/us-en/services/industrial/rail-transit

About Accenture

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.