CYBER RISKS IN TRANSIT

The exposure of transit agencies to cyber risks is growing significantly as the industry moves towards interactive technologies to address many of its impending issues of operation. New vehicle and movement control systems that provide integration between the transit operator and the systems of other governing bodies from throughout the service region in "smart cities," as well as through the internet, offer new methods to access the programs that control transit operations and finances to an extent previously unconsidered.

As a target for security threats, the public sector is unique, experiencing more cyber incidents than any other industry. US federal, state and local government agencies need to improve key aspects of their digital defenses against this threat landscape.[1]

As agencies move towards "smart-city" technology with more digital capabilities, they become much more vulnerable to remote tampering by persons with nefarious intent. Operationally, transit operators are exposed to improper access to critical safety systems related to vehicle movement controls, patron station movement, utility support systems or data communications. While such access can certainly target such essential operating systems, creating risks to employees and patrons through improper transactions, an equally accessible and troublesome path can be found through the many new revenue management systems that have been established in transit sites around the world. By their very nature, new revenue systems allow access to openings from a huge volume of access points. All users of smartphone access, smart card access or cellular access into transit revenue protocols are permitted access into agency systems through their phones, web sites or Bluetooth devices. If intra-system access controls are inadequate, disaster could strike.

In recent years, with the advent of connected devices and the expanding width and scope of patron cyber interaction with agency systems, the risks of cyber casualty have grown tremendously. Due to the increased volume and complexity of direct linkages with external parties through cell phone, web and other new tools, systems that have historically caused little concern for cyber-security are now ripe with opportunity for hackers.

Greater interaction between financial and operational systems, as well as the greater power of operating systems to access or control vehicle movement or control systems produces huge exposures. Sharing data across channels into other city agencies and operating units in "smart-city" environments expands the number of interfaces that require control. Agencies must protect themselves from such breadth and scope of accesses in the core development of all systems.

[1] "Rebooting" Public Sector Cybersecurity, 2017, Accenture, https://www.accenture.com/us-en/insight-rebooting-public-sector-cybersecurity

Examples of Transit Breeches
Experiences in the United States and European transit arena have pointed to these exposures.

Recently, hackers attacked the Sacramento Regional Transit's computer network, erasing data and threatening to do worse harm if the agency failed to cough up a bitcoin ransom.

San Francisco's MTA experienced a similar breach several years ago.[2] A ransomware attack took ticket machines for San Francisco's light rail transit system offline all-day during one of the busiest shopping weekends of the year, but rather than shutting down, the agency decided instead to let users ride for free. By Sunday the system was once again running normally.[3]

In Kiev, the capital of the Ukraine, the government reported disruptions including in the country's power grid and computers in many government offices. Ukraine's largest airport, in Boryspil, also reported an attack, delaying some flights. Ukraine's central bank said several banks had been hit, as well as the metro transit system's payment network in Kiev.[4] The malware used for the cyberattack in Kiev was Diskcoder.D — a new variant of ransomware known also as Petya. The malware often enters the system through phishing efforts.[5]

In addition, last year, the director general of the Swedish Transport Agency, was fired for negligent handling of classified data. The agency entered into an outsourcing agreement with IBM Sweden in April 2015, worth nearly $100 million, to manage vehicle registration and driver's license databases. But adequate safeguards were not adopted, and as a result, unauthorized personnel at IBM subsidiaries in Eastern Europe had access to vast troves of sensitive information, including details about bridges, roads, ports, the subway system in Stockholm and other infrastructure. In addition, the identities of people working undercover for the Swedish police may have been revealed. Unlike other cases involving breaches of government data, the case in Sweden does not appear to involve hacking or other malice. Instead, the focus has been on an apparent absence of proper safeguards and oversight or authorized third party entries.[6]

[2] Yes, Transit Users, You Could Get Hacked, Too LAURA BLISS NOV 22, 2017Citylab.com © 2018 The Atlantic Monthly Group; https://www.citylab.com/transportation/2017/11/yes-transit-users-you-could-get-hacked-too/546635/

[3] Ransomware attack hit San Francisco train system Elizabeth Weise, USA TODAY Published 12:42 p.m. ET Nov. 28, 2016 USA Today https://www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/

[4] O'Brien, Chris & Ayres, Sabra, Cyberattack using data-scrambling software causes disruptions in Europe, JUN 27, 2017, http://www.latimes.com/world/europe/la-fg europe-cyberattack-20170627-story.html

[5] Kiev metro hit with a new variant of the infamous Kiev metro hit with a new variant of the infamous Diskcoder ransomware, We Live Security ESET, https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/

[6] Anderson, C; Swedish Government Scrambles to Contain Damage From Data Breach, New York Times, 7/25/17, https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html

While these events reflect exposures to an agency unrelated to safety, the same technology could be employed to create much graver impacts. Through gaining access to vehicle movement control systems, patron movement systems such as escalators or other safety sensitive IT platforms, direct impacts on patron or equipment safety could be achieved.

Risks to Patrons and Employees

Employees and patrons are certainly at risk from misdirection of vehicles, finances or data. Not only could horrific results occur due to an improper instruction to a vehicle movement, but improper payments of patrol or payables transactions can occur if these systems are not protected.

A case of improper access to vehicle control systems occurred in Lodz, Poland, where a 14-year-old modified a TV remote control so that it could be used to change track points. The teenager broke into a number of tram depots to gather the information needed to build the device, which turned the tram system in Lodz into his own personal train set. As a result, four vehicles were derailed injuring twelve people.[7]

Risks to Finances

Improper access to financial systems can result in improper reporting of revenue, expenses, assets or liabilities or closure of revenue collection, as in the San Francisco example. The costs of such breeches can be monumental if left undetected or uncontrolled.

Exposure of credit / debit card and personally identifiable information (PII) is another area in which transit agencies are exposed, although newer systems offer more protection due to new banking-industry security standards related to protection of PII. The breech of systems at Target in 2013, which allowed improper access to 40 million debit/credit card accounts, presents a sample of the types of exposure that are often unaddressed in review of security system security.

In that instance, the Target systems were accessed through an authorized third-party contractor which had been granted access to Target systems for monitoring of HVAC operations. This contractor was hacked through a phishing operation which provided the ability to insert malware that ultimately spread into the POS devices and patron cards. Due to inadequate protections against malware, especially those instances inserted through an internal source, the Target systems were compromised.[8]

The company was exposed through a relatively weak part of their overall cyber protection – proper authorizations of external access into systems, without pertinent coverages. Inadequate protections against phishing also caused the issues.

---

[7] Marsh Insights: Cyber Risk in the Transportation Industry, Marsh & McLennan Companies, http://www.oliverwyman.com/content/dam/marsh/Documents/PDF/UK/en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf

8 Aidan Carrol, A & Rigden T, Target Security Breach, Carleton College, https://people.carleton.edu/~carrolla/index.html

If third parties are allowed access into any agency systems, pertinent monitoring must be imposed to prevent disruptions similar to the Target and Swedish Transport intrusions. Agencies need to become aware of such weaknesses in system protocols and employ measures to protect against exposures through the "weak-link" into their systems. "Weak-links" can be caused by improper password protections, inadequate protection against phishing attempts and other ancillary tentacles of the core systems.

Solutions to Transit Exposures

For several years, the American Public Transit Association (APTA) through the efforts of its Enterprise Cyber Security Working Group, has embarked on a long-term effort to educate the transit operators and business members of the associations in the risks and solutions related to cyber-security. Ongoing educational efforts before the association membership have been proceeding with numerous sessions on cyber awareness being offered at association conferences. Members are encouraged to work with the Working Group in defining their risks and explore potential cost-effective solutions to the issue.

Working closely with the U.S. Department of Homeland Security Transportation Security Administration's Office of Cybersecurity and Communication, the large variety of resources available from the U.S. federal government are directed towards specific transit exposures, with guidance and direct assistance provided by the cyber analysts of the TSA. Efforts to fully advise transit operators on the importance of the NIST Cybersecurity Framework - Identify, Protect, Detect, Respond and Recover - and the ways to ensure full sensitivity to these components of protection throughout all transit system developments are key goals of APTA's efforts.

Agencies are getting more sensitive to cyber security. A well-publicized report by the inspector general of the Washington Metropolitan Transit Authority (WMATA) revealed the need for significant improvements to cyber security practices at the agency.[9] A recent scam had allowed Metro users to charge their SmarTrip cards but still walk away with their cash. This condition caused the transit agency to upgrade the software on all the system's farecard machines.[10] Increased sensitivity to cyber exposures can mitigate the adverse impact of negative public relations on the subject, while ensuring that adequate resources are applied towards preventive actions prior to serious problems.

Discrete Vendor Solution

Throughout its history of developing and installing innovative, state-of-the-art technologies for use in all modes of transport, Conduent, Inc. has ensured strict adherence to basic cyber-safety protocols related to the protection of data and systems from intrusion by external parties. The company has begun a program of careful examination of all of its legacy products in the transit arena to ensure continued strength in the protection of relevant data and systems through cybersecurity within the changing cyber environment.

---

[9] Powers, M, Metro cybersecurity audit highlights growing concerns at agencies across the country - The Washington Post, 7/9/2018, https://www.washingtonpost.com/local/trafficandcommuting/metro-cybersecurity-audit-highlights=-growing-concerns-at-agencies-across-the-country/2018/07/07/3020

[10] Martin Austermuhle, M, Software On Metro Farecard Machines Upgraded After SmarTrip Scam Uncovered https://wamu.org/story/14/11/14/metro_farecard_machines_upgraded_after_scam_uncovered/

The firm is expending resources towards a careful review of all telecommunication access points into our systems, as well as controls on data outflows from our systems. Through use of identity protections, we are ensuring that all access events are instituted through pre-defined and pre-approved flows.

Conduent has recognized that since its CAD/AVL tools can now be directly linked into driver control systems and fareboxes, this instrument now offers direct links into vehicle operations and finance systems that had historically been completely divorced from the CAD/AVL activity. The CAD/AVL units are linked to overall revenue reporting and payroll systems to an extent never anticipated, as the units become connected to front-of-bus fare control systems and driver scheduling systems. Such new connectivity has caused the firm to carefully assess all methods of accessing our systems, as well as controls governing outflows from the units. This OEM is proactively enhancing legacy designs to provide identity protections.

These enhanced security capabilities will ensure that all device interactions are trusted. Untrusted interactions are blocked and alerted. System operations on continuously monitored to ensure that devices only do what they are supposed to. Non-approved operations are blocked and alerted. Finally, all communications are encrypted. The new protocols eliminate backdoor vulnerabilities.

It is a software solution for strong public key infrastructure (PKI) credential management, enforced both at the server/cloud and at the device. The system will optimize device protection via declarative enforcement at all levels: Network, File, Process, OS. It blocks unauthorized accesses/uses and reports on anomalies and defends against both traditional IT malware as well as control messages that misuse Internet of Things (IoT) devices.[11]

Coincidently, some of Conduent's ticketing systems now allow access for transactions through cell phone communication from the patron. Similar protocols for testing and protecting systems through enhanced access controls are also being crafted for their Atlas ticketing systems, Seamless Transportation Solution and the Mobility Analytics Program (MAP) and Mobility Companion platforms.

As their efforts produce definitive results, Conduent will be positioned to share these control capabilities with clients across all modes of transport, such as tolls and parking, each of which contain similar new exposures to cyber-crime.

[11] Zuul IoT, Inc. https://zuuliot.com/, July 24, 2018