MDOT Tech Talk

Presentation by:
Scott Belcher, Brandon Thomas

IS THE TRANSIT INDUSTRY PREPARED FOR THE CYBER REVOLUTION?

POLICY RECOMMENDATIONS TO ENHANCE SURFACE TRANSIT CYBER PREPAREDNESS

MTI MINETA TRANSPORTATION INSTITUTE

About MTI

To move is to live. At the Mineta Transportation Institute (MTI) at San Jose State University, our mission is to increase mobility for all by improving the safety, efficiency, accessibility, and convenience of our nation's transportation system. Through research, education, workforce development and technology transfer, we help create a connected world.

Cybersecurity: A Primer

What is Cybersecurity

Cybersecurity preparedness is more than just protecting your systems. It requires processes, planning, and people, in addition to technology.

The question is not if but when will an incident occur. You must identify, detect and protect, but also be ready to respond and recover.

NIST Framework

- **Identify**: develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities;
- **Protect**: develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services;
- **Detect**: develop and implement the appropriate activities to identify the occurrence of a cybersecurity event;
- **Respond**: develop and implement the appropriate activities to take action regarding a detected cybersecurity event;
- **Recover**: develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Study

- Literature Review
- 40+ Expert Interviews
- Digital Survey
  - Response Rate: 31% of APTA U.S. Public Transit Operators representing 1/3 of the U.S. Population
- Policy Recommendations

The Good News: Plenty of Guidance

- NIST Cybersecurity Framework
- Cybersecurity guidance specific for the transit industry
- Federal Support: Transportation Security Sector (TSS) – DHS (FEMA and Cybersecurity and Infrastructure Security Agency (CISA))
  - TSS Cybersecurity Framework Implementation Guidance
  - Cybersecurity Advisors Program (CSA)
  - U.S. DOT
- State support
- Industry association support

The Bad News: Resources are a Limiting Factor

- Many agencies do not have an accurate sense of the cybersecurity preparedness
- Most agencies do not have log maintenance schedules which satisfy a basic tenant of cybersecurity preparedness
- Most agencies do not have many of the basic policies and procedures in place to respond in the event of an incident
- Many agencies lack the staff and the necessary skills or training to address cybersecurity threats
- Agencies are engaging vendors for cybersecurity support, but they are not always protecting themselves or their customers with appropriate cybersecurity language

The Bottom Line: The Transit Industry is ill-prepared for Malicious Cyber Attacks and Other Cybersecurity Related Threats

Incident Awareness

Public Transit

22% Responded that they have suffered an incident

Vs.

Global Organizations

82% Responded that they have suffered a disruptive event

Source: Digital Survey

Source: Dell Technologies “Global Data Protection Index: Cloud Environments”, March 2020

Finding: Many agencies do not have an accurate sense of their cybersecurity preparedness

- 81% of agencies that responded believe they are prepared to manage and defend against cybersecurity threats, and;
- 73% feel they have access to information that helps them implement their cybersecurity preparedness program.

Yet…

- Only 60% actually have a cybersecurity preparedness program;
- 43% do not believe they have the resources necessary for cybersecurity preparedness; and
- Only 47% audit their cybersecurity program at least once per year.

Finding: Most agencies do not have log maintenance schedules which satisfy a basic tenet of cybersecurity preparedness

- 51% of agencies that responded do not retain their log data for a year or more—one of the most basic requirements for cybersecurity preparedness

- 12% of agencies surveyed do not retain their logs at all

Finding: Most agencies do not have many of the basic policies and procedures in place to respond in the event of an incident

- 42% don't have an incident response plan; of those that have one, over half have not had a drill in over a year
- 36% do not have a disaster recovery plan
- 53% do not have a continuity in operations plan
- 58% do not have a business continuity plan
- 67% do not have a crisis communications plan

Finding: Many agencies lack the staff and the necessary skills or training to address cybersecurity threats

- Only 41% of agencies provide at least annual cybersecurity training for staff
- Cybersecurity staffing levels are low, even among large agencies or agencies that have suffered an incident, relative to other industries

% of Agencies	Certification
23%	Certified Information Security Professional (CISSP)
9%	Certified Ethical Hacker (CEH)
7%	Certified Information Systems Auditor CISA

Finding: Agencies are engaging vendors for cybersecurity support, but they are not always protecting themselves or their customers with appropriate cybersecurity language

- 84% have engaged at least one vendor to provide cybersecurity software, tools, and support
- Only 38% include standard clauses in their contracts to impose cybersecurity requirements on all their vendors

Policy Recommendations:

Executive Branch

- Promulgate a set of minimum cybersecurity standards and cybersecurity assessment tools and determine how they should best be developed, managed, and implemented
- Provide technical guidance to transit agencies on the collection, retention, and assessment of system logs
- FTA should require that transit CEOs attest that their organization has met the minimum cybersecurity standards established above prior to receiving federal funds
- Require that transit agencies either outsource management of payment data to PCI-compliant vendors, or require that their CEO attest that they are PCI-compliant prior to receiving federal funds

Policy Recommendations:

Legislature

- Increase funding to DHS and U.S. DOT to develop and promulgate a set of minimal cybersecurity standards and tools and for their promotion
- Congress should increase formula grant funding to transit agencies to ensure that they have sufficient resources to meet the minimal cybersecurity standards established above
- Congress should ensure through its oversight powers that U.S. DOT and DHS work together to improve cybersecurity preparedness within the TSS

Policy Recommendations:

Associations

- Develop a clearinghouse for cybersecurity best practices, in particular for small and medium transit operations.
- Create minimum guidelines for cybersecurity audits
- Develop model cybersecurity contract language for agencies to integrate into their vendor contracts.
- Develop a model Incident Response Plan, Business Continuity Plan, Continuity of Operations Plan, Crisis Communications Plan, and Disaster Recovery Plan that can be tailored to meet the needs of public transit organizations of varying sizes and needs.
- Develop cybersecurity training modules and certificates. In doing so it should take advantage of the guidance developed by TSS, CSAs and others.

Policy Recommendations:

Operators

- Develop an individualized cybersecurity plan.
- Conduct a periodic cybersecurity audit and address the shortcomings identified in that audit in a timely manner.
- Outsource the handling of PCII to the extent possible and ensure that it has current, robust, cybersecurity contract language protecting it. Conduct an audit of all external contracts and ensure that it has current, robust, cybersecurity contract language protecting it.
- Transit Operators should have the necessary response plans in place, and review them periodically. In doing so, Transit Operators should avail themselves of the most currently guidance available from APTA, the TSS, and other agencies. Transit Operators should regularly conduct drills to ensure that they are prepared for inevitable intrusion
- Provide the appropriate level of cybersecurity training at least annually.