Facing the Threat of Cybersecurity Workshop

CTAA SUN Conference 2022
Brooke Ramsey – HIRTA
Mark Talbot – CYBRBASE
Agenda

- Introductions
- Security in the Transit Sector
- Industry Research
- Federal Mandates and Directives
- HIRTA’s Story
- Where to start?
- Q&A
Security in the Transit Sector

• In August of 2021, Rhode Island Public Transit Authority (RIPTA) experienced a ransomware attack.

• It was forced to pay a $170k ransom, and over the following year it was discovered that the hackers stole information, including social security numbers, from 17,000 state employees during the breach. This opened RIPTA up to an investigation by the state’s attorney general.

• Recently, Valley Regional Transit, a small agency with approximately 1.2 million yearly riders in Boise, Idaho, experienced an attack that compromised hundreds of personal records.
Security in the Transit Sector

Transit Agencies are High Value Targets

Increased Risk to Daily Operations
Interruption of Bus/Rail schedules

Rider Safety and Security
Not just exposing Personally Identifiable Information (PII) but physical safety

Ability to Secure Affordable Cyber Insurance
Most Insurance Companies now require that a CyberSecurity program is in place
Industry Research – MTI Publications

- Personal Data Protection as a Driver for Improved Cybersecurity Practices in U.S. Public Transit
- Will the Biden Administration’s ‘Made in America’ Executive Order Present Significant New Cybersecurity Obligations for Transit Operators?
- Implications of the Sunburst Cybersecurity Attack on the Transit Industry
- Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendation for Identifying and Addressing Cybersecurity Challenges
Key Findings
Incident Awareness

Public Transit
22% Responded that they have suffered an incident

Global Organizations
82% Responded that they have suffered a disruptive event

Source: MTI Digital Survey
Source: Dell Technologies “Global Data Protection Index: Cloud Environments”, March 2020
Cyber Security Preparedness

40%  Do not have a cybersecurity program in place

43%  Do not believe they have enough resources necessary for cybersecurity preparedness

50%  Conduct annual security audits

60%  Either do not have/do not know if they have cybersecurity clauses in their vendor contracts

60%  Do not provide annual cybersecurity training
Federal Guidelines and Mandates

Executive Order – 14028
• Updated federal contract language with more stringent incident reporting rules

Cybersecurity Maturity Model Certification (CMMC)
• Updated to a new version in November 2021, this certification applies to DOD contractors.

Infrastructure Investment and Jobs Act (IIJA)
• Requires the Federal Highway Administration to develop a cybersecurity tool for transportation agencies based on the NIST framework.

National Defense Authorization Act (NDAA)
• Directs the TSA to update cybersecurity guidance on handling Sensitive Security Information.

Omnibus Appropriations Act of 2022
• Requires incidents affecting “critical infrastructure” to be reported within 72 hours of detection and ransoms to be reported within 24 hours of payment.

TSA Security Directive for Public Transit and Rail (1582-21-01)
TSA Security Directive for Public Transit and Rail

1. Designate a cybersecurity coordinator
2. Report cybersecurity incidents to CISA
3. Develop a cybersecurity incident response plan
4. Conduct a cybersecurity vulnerability assessment
About HIRTA
Heart of Iowa Regional Transit Agency

- Founded in 1981
- Serve 7 Counties in Central Iowa
- 57 Employees
- 177,686 yearly unlinked passenger trips
- 61 Revenue vehicles
- 845,159 vehicle miles
About HIRTA
Heart of Iowa Regional Transit Agency

- One employee acts as IT liaison
- 3rd party / outside IT vendor
- First security breach in 2012
- Employee impersonation 2 weeks ago
Where to Start
General Outlook

▪ Our general working theory is that cyber attacks are no longer “threats” but are “risks” that need to be effectively managed; and

▪ Effective cybersecurity resilience programs are complicated but essential to manage and mitigate an agency’s risk.

▪ Interviewed more than 50 leaders in transit as CYBRBASE on top of the 100s interviewed as part the MTI research

▪ Presented at over 10 industry events this year alone to elevate the conversation about cyber readiness and resilience
Cyber Breaches Have Real Costs

Cyber Risk is Real

Cyber Readiness Guidelines from Federal Gov.

What Can You Do?

Three Things We Know
Our tool provides:

- A simple, intuitive, online NIST-based assessment
- Secure cloud storage of all assessments
- Dashboard reporting to monitor progress
- Quantitative assessment maturity level reporting; baseline, q/q, y/y
- Qualitative analysis with baseline recommendations focus areas based upon current risk exposure and
- CYBRBASE RideAlong © - Guided assessment with cybersecurity experts
Vulnerability Management

The purpose of Vulnerability Management is to identify, analyze, and manage vulnerabilities in a critical service's operating environment.

Goal 1:
Preparation for vulnerability analysis and resolution activities is conducted.

01. Has a vulnerability analysis and resolution strategy been developed?

People
- No
- Incomplete
- Yes

Information
- No
- Incomplete
- Yes

Technology
- 
- 
- 

Last Updated by:
Jun 15, 2022 1:14 PM
James Gilmour
01 Asset Management

The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.

INITIATE ASSESSMENT

Goal 1:
Services are identified as prioritized.

01. Are services identified?

Yes

NIST CSF Reference: ID.BE
CERT-RMM Reference: SC:SG2.SP1
Good Job!

You have successfully completed Goal 1

Let's go ahead and complete Goal 2

THAT'S IT FOR TODAY

PROCEED
Dashboard

Progress Graph

Maturity Level Indicator

Asset Management | Controls Management | Configuration and Change Management | Vulnerability Management | Incident Management | Service Continuity Management | Risk Management | External Dependencies Management | Training and Awareness | Situational Awareness

Jamie Test 1: Jamie Test 2: Test 3
SAMPLE DOCUMENTS – INCIDENT MANAGEMENT PLAN

HIRTA Public Transit Incident Management Plan

Date: ____________________________
Name of person completing this form: ____________________________

Executive Support
List the executives who had input to this document and endorse its development and applicability:

<table>
<thead>
<tr>
<th>Name of executive</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sponsor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Process Description
Explain the incident management process in a manner that provides a high-level understanding to personnel who must implement this plan.

Critical Services
Indicate the priority of critical services.

<table>
<thead>
<tr>
<th>Priority level</th>
<th>Service restoration time objective</th>
</tr>
</thead>
</table>

Plan Activation Criteria
Describe conditions that must be met before the incident management plan can be executed.

HIRTA Public Transit Incident Reporting Template

Date: ____________________________
Name of individual completing this form: ____________________________

Tracking number: ____________________________

Incident Priority

- [ ] HIGH
- [ ] MEDIUM
- [ ] LOW
- [ ] OTHER

Additional notes: ____________________________

Incident Type
Check all that apply:

- [ ] Compromised System
- [ ] Compromised User Credentials (e.g., lost password)
- [ ] Network Attack (e.g., DoS)
- [ ] Malware (e.g., virus, worm, Trojan)
- [ ] Reconnaissance (e.g., scanning, sniffing)

Incident description notes: ____________________________

Incident Timeline
Please provide as much detail as possible.

A. Date and time when the incident was discovered
B. Date and time when the incident was reported
C. Date and time when the incident occurred

Additional timeline details: ____________________________
RECOMMENDATIONS

1. Identify persons responsible within the agency for cyber risk management
2. Conduct a cyber assessment at least annually using a NIST based tool
3. Based on results of the assessment, develop and implement cyber readiness and response plan
4. Incorporate cyber monitoring into overall integrated risk management plan
5. Engage in public and private information sharing programs
MARK J TALBOTT

MARK.TALBOTT@CYBRBASE.COM