Cybersecurity Practices in Industry

BRIAN FAZ | ASSISTANT VICE PRESIDENT, TECHNOLOGY

MAY 2024
Who We Are

At BNSF Railway every day our team moves the freight that moves the nation, playing a vital role in the success of our customers and the strength of the American economy.

We strive to operate free of accidents and injuries, with sustainability at the top of our minds, to serve our customers and our team members with respect, and to demonstrate the resilience and commitment to our customers that will empower us to keep our nation moving forward for decades to come.
Cyber Security Risk Environment

- Locomotives – Fuel Levels, Cameras, Onboard Diagnostics
- Data Centers and Systems
- ICS / SCADA - Wastewater Treatment, Oil / Water Separators, Stormwater Treatment Sites
- Employees, Customers, Mobile, PC, 3rd party Systems
- Wayside Assets – Signals, switches, sensors
- Hub Operations – Mobile, Crane and Yard Vehicles
- Facility Systems – Ventilation, Generators, Dust Collectors Scales
- Employees, Customers, Mobile, PC, 3rd party Systems
- Radio, Microwave Communications Systems
- Structures – moveable bridges, tunnels
- Hub Operations – Mobile, Crane and Yard Vehicles
- Facility Systems – Ventilation, Generators, Dust Collectors Scales
- ICS / SCADA - Wastewater Treatment, Oil / Water Separators, Stormwater Treatment Sites
Digital Progression in Rail

Operational data increasing at an exponential rate

Deployment of digital assets in the workforce for real time data and work capture

Extensive physical world mapping and asset tracking

Leveraging real time information for inspect and management of freight movement

Investment in new capabilities with AI, ML and algorithmic operational models
Cyber Security Challenges in the Railroad Industry

Who Might Attack?
- Cyber Criminals
- Hacktivists
- Nation States
- Insiders / Competitors
- Individual Hackers

What are the key business risks for industry to mitigate?
- Degradation of Critical Infrastructure
- Business Disruption
- Reputation Damage
- Financial Fraud
- Theft (Physical and Sensitive Data)

Critical Infrastructure Attacks
- Utilities
- Pipelines
- Trucking
- Public Transit

Railroad Industry Agency Collaboration
- Association of America Railroads (AAR)
- Federal Railroad Administration (FRA)
- Surface Transportation Board (STB)
- Transportation Security Administration (TSA)
Overall, 3000 threats per minute blocked at the perimeter

- 6M Firewall events / day
- 10M IPS events / week
- 45M+ messages / month
Security First Mindset

It takes a community to effectively protect BNSF with each of us taking responsibility to think about security in every aspect of our jobs

Shared Accountability

- Education and Responsible Use
- Vigilance and Awareness
- Comprehensive Cyber Security Operations Program
## Cybersecurity Strategic Pillars

<table>
<thead>
<tr>
<th>Identity and Access Management and Control</th>
<th>Know who is on the network at all times and control what they can do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive Monitoring and Response; Vulnerability Management</td>
<td>24x7 Security Operations Center (SOC) and related processes. Frequently assess all systems and code and apply rigorous patch discipline</td>
</tr>
<tr>
<td>Training and Culture</td>
<td>Ensure all employees understand threats and practice how to detect and defeat them</td>
</tr>
</tbody>
</table>

### Identity and Access Management
- Centralized ID Mgmt
- Multi Factor Authentication (MFA)
- Role-based Access Control (RBAC)
- Perimeter Security - IPS, Firewall, VPN
- Network Segmentation
- Encryption (in-flight / at rest)

### Proactive Monitoring & Response; Vulnerability Management
- Security Information & Event Mgmt
- Security Operations Center
- Metrics, Reporting & Event Management
- Server and Code Scanning
- Patching and Environment Refresh
- Endpoint and Mobile Protection
- E-mail Scanning/Filtering
- Automation and Access Control

### Training & Culture
- Cybersecurity Awareness
- Secure Coding Practices
- Threat Reviews
- Tabletop Exercises
- IT Controls & 3rd Party Governance
- Risk Analysis & Pen Testing
- Communication

---

**One Layer Down**