Cybersecurity Practices in Industry

BRIAN FAZ | ASSISTANT VICE PRESIDENT, TECHNOLOGY
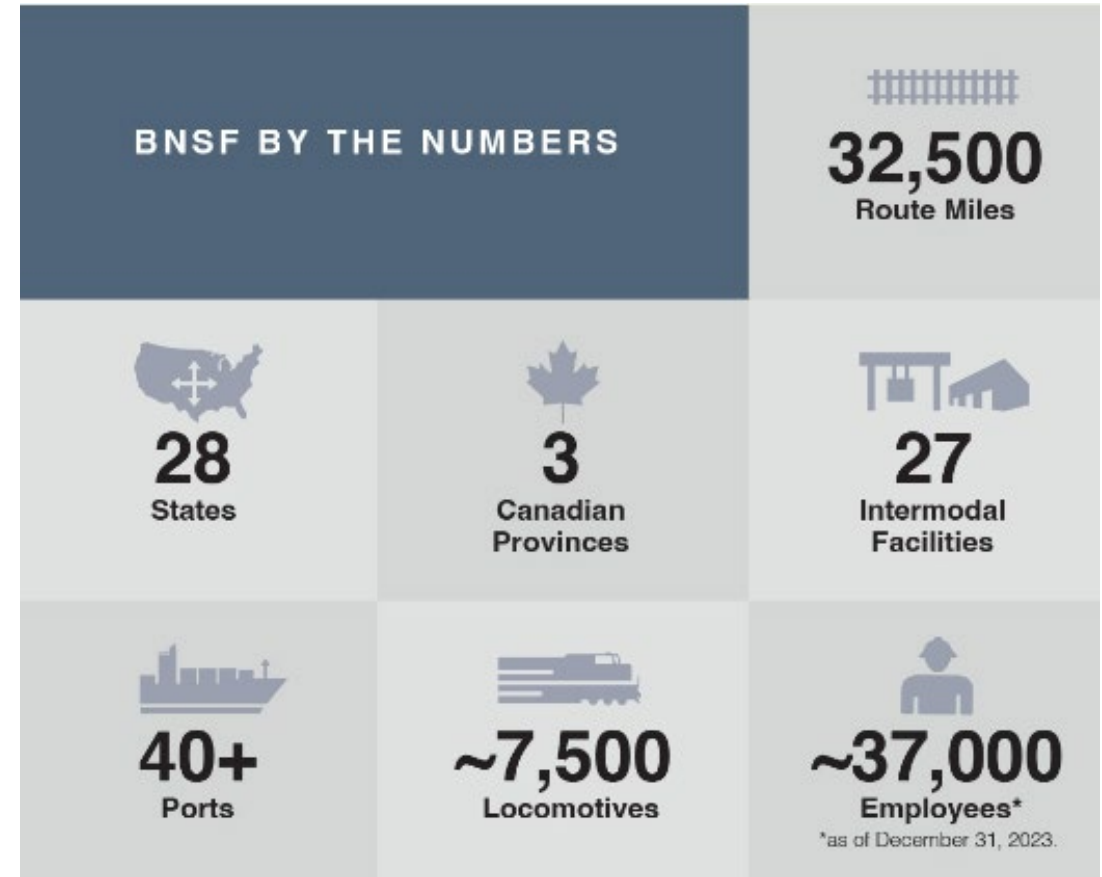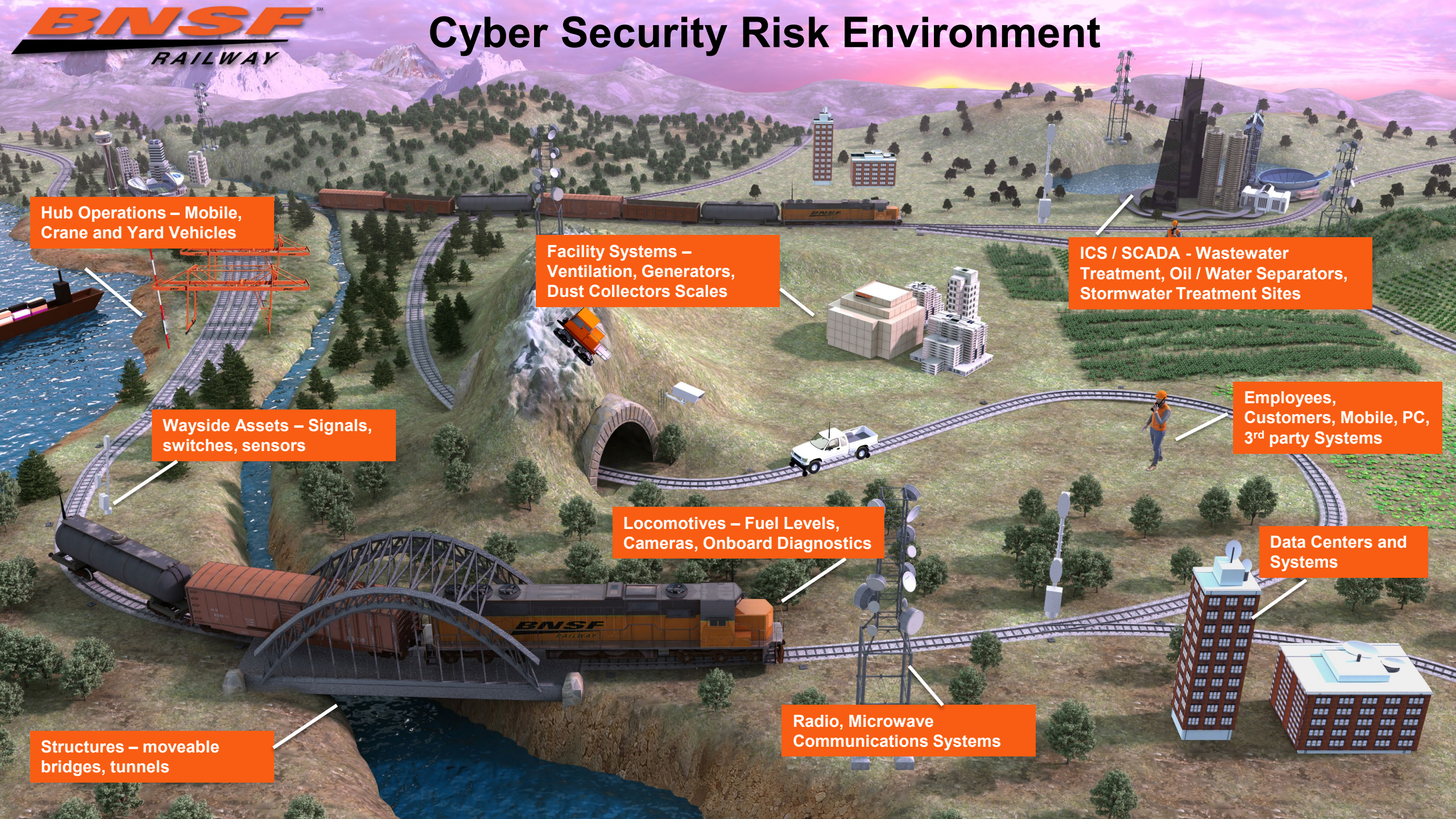
MAY 2024

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.

BNSF BY THE NUMBERS

32,500 Route Miles

28 States

3 Canadian Provinces

27 Intermodal Facilities

40+ Ports

~7,500 Locomotives

~37,000 Employees*
*as of December 31, 2023.

Source: www.bnsf.com, 2023 Impact Report

Cyber Security Risk Environment

Hub Operations – Mobile, Crane and Yard Vehicles

Facility Systems – Ventilation, Generators, Dust Collectors Scales

ICS / SCADA - Wastewater Treatment, Oil / Water Separators, Stormwater Treatment Sites

Wayside Assets – Signals, switches, sensors

Employees, Customers, Mobile, PC, 3rd party Systems

Locomotives – Fuel Levels, Cameras, Onboard Diagnostics

Data Centers and Systems

Structures – moveable bridges, tunnels

Radio, Microwave Communications Systems
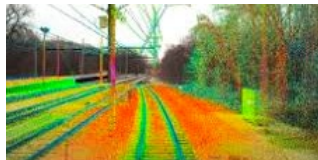
Digital Progression in Rail

Data

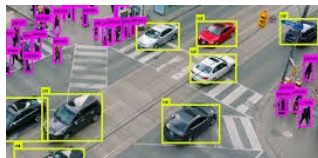Operational data increasing at an exponential rate

Mobility

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

LiDAR / GIS

Extensive physical world mapping and asset tracking

Image/Video Analytics

Leveraging real time information for inspect and management of freight movement

AI / ML

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)
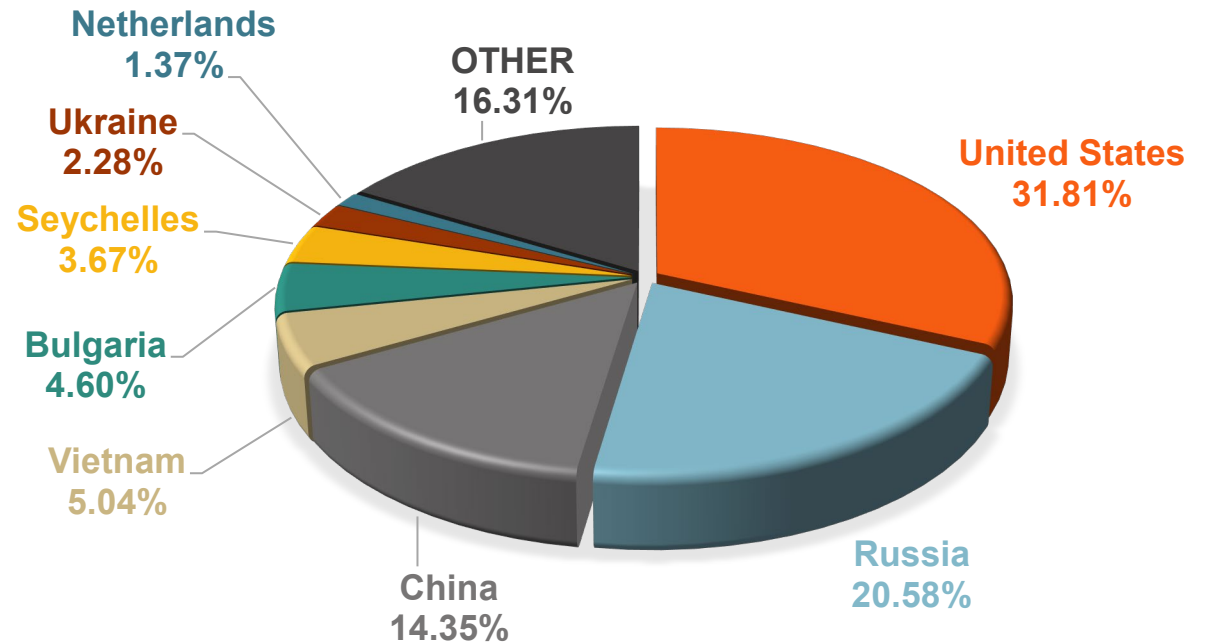- Transportation Security Administration (TSA)

Railroad Network Defense

Overall, 3000 threats per minute blocked at the perimeter

- 6M Firewall events / day

- 10M IPS events / week

- 45M+ messages / month

THREATS BY COUNTRY

- Netherlands 1.37%
- Ukraine 2.28%
- Seychelles 3.67%
- Bulgaria 4.60%
- Vietnam 5.04%
- China 14.35%
- OTHER 16.31%
- United States 31.81%
- Russia 20.58%

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

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

One Layer Down

Identity and Access Management	**Proactive Monitoring & Response; Vulnerability Management**	**Training & Culture**
• Centralized ID Mgmt • Multi Factor Authentication (MFA) • Role-based Access Control (RBAC) • Perimeter Security - IPS, Firewall, VPN • Network Segmentation • Encryption (in-flight / at rest)	• 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	• Cybersecurity Awareness • Secure Coding Practices • Threat Reviews • Tabletop Exercises • IT Controls & 3rd Party Governance • Risk Analysis & Pen Testing • Communication

BNSF ®
RAILWAY

- Brian Faz | Assistant Vice President, BNSF Railway