AON

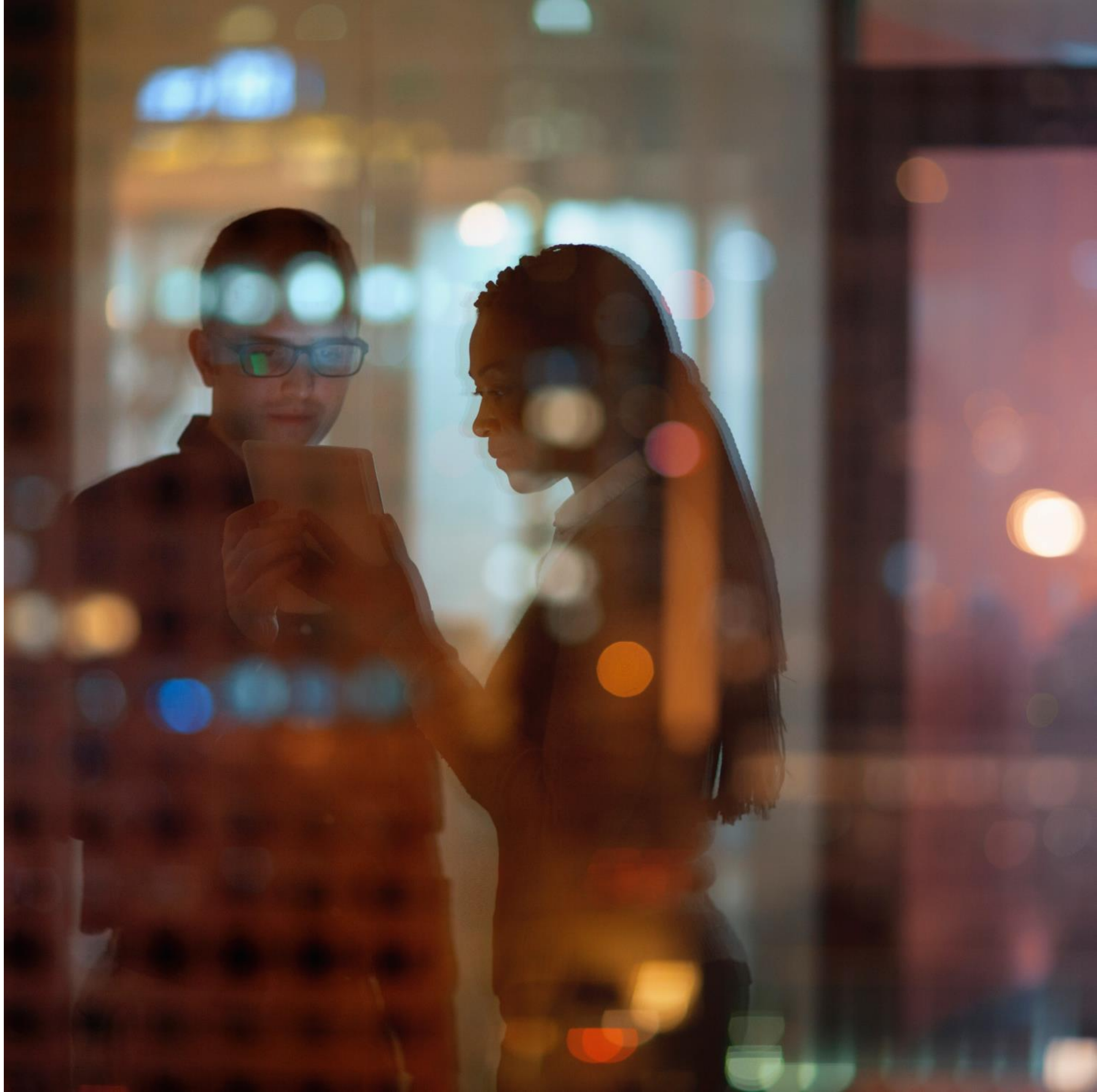
Cybersecurity Threats to the Transportation & Logistic Industries

Heather Hughes, J.D.

Vice President, Cyber Solutions

Heather.L.Hughes@aon.com

832-480-3266



Full Spectrum of Threats

HACKTIVISM

Motivation:
Hacktivists use computer network exploitation to advance their political or social causes.

TERRORISM

Motivation:
Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.

CRIME

Motivation:
Individuals sophisticated criminal enterprises steal personal information and extort victims for financial gain

WARFARE

Motivation:
Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

INSIDER

Motivation:
Trusted insiders steal proprietary information for personal, financial, and ideological reasons.

ESPIONAGE

Motivation:
Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

Cyber Threat Landscape: Transportation & Logistics Sector

Critical Infrastructure as prime target for cybercriminals – lucrative and opportunity to disrupt supply chain

Increased connectivity and dependency on technology = larger attack surface and fresh entry points for hackers

Outdated systems and lack of investment in cybersecurity

Regulatory requirements (e.g., new SEC cybersecurity rules for publicly-traded companies)

Threats to this sector include ransomware; leaked data; DDoS attacks; social engineering (phishing/spear phishing); supply chain attacks

Third Party Risks

Supply chain attacks are designed to circumvent controls and take advantage of the inherent trust in third-party relationships—software vendors, customers, etc.

Without the proper controls, your vendors and contractors can become the **weakest link** to your organizations and customers' privacy.

BEST PRACTICES

- Process for **evaluating** new vendors as they are onboarded—
- Understand your most **critical assets** and their locations.
- Monitor who has **access** to the identified critical data.
- Include **cybersecurity requirements** in vendor contracts that include;
  - ✓ Documented evidence showing that security testing is done at least annually
  - ✓ Incident Response Plans
  - ✓ Employee Training
  - ✓ Access Management
  - ✓ Cyber Insurance

The Epidemic of Ransomware

Demands for payments by threat actors are in the millions.

Damages to businesses and organizations and costs associated with ransomware extend to **business interruption** and loss of **customer trust.**

Prior to encryption, threat actors are exfiltrating data, which they use to coerce payment.

Threat Actors are now contacting **employees, patients** and even the **SEC** (AlphV) to coerce payment.

Insurers have introduced new ransomware-specific applications.

These efforts are focused on enhancing insured risk controls, and risk selection for insurers.

Deep Fakes and Artificial Intelligence (“AI”)

Threat Actors are posing as executives with spoofed phone numbers and AI Deep Fakes using speeches and talks found online.

Identifying deepfake audio can be challenging, especially over the phone. But if you suspect the person you’re talking to may not be who they say they are, the best thing to do is ask questions that an imposter will not be able to answer correctly.

- ✓ Establishing a set of security questions or codewords in advance can help safeguard your business against scammers who use deepfake technology to commit theft and fraud.
- ✓ Confirm identity using a known callback number. Never offer sensitive financial or personal identifiable information (PII) over the phone.
- ✓ Make sure your company’s financial dual controls are well-established so that employees don't make significant fund transfers without verification.
- ✓ Verify with the bank to confirm both the account number and the name on the account before sending a wire.

Proactive Cybersecurity Tips

Regular and robust phishing **training** for all employees

Multi-factor authentication for access into any system

Ensure systems have off-line/cloud **backups**--if on-site backups are encrypted, you still have backups to use

Install network monitoring and response tool: **Endpoint Detection and Response ("EDR")**

Implement and practice your **Incident Response Plan**

Have trusted partners chosen and on stand-by; legal, forensics, insurance broker

If hit with ransomware: disconnect all machines from the network but not power off

Cyber Key Controls

Marketplace Minimum Expectations

- Multi-Factor Authentication (MFA)
- Endpoint Detection and Response (EDR)
- Phishing Exercise/ Cyber Awareness Training
- Vulnerability Scanning & Patch Management
- Secure RDP/VPN
- Incident Response Plan/ Ransomware Exercise
- Access Control/ Service Accounts
- Disaster Recovery/Backups
- Email Filtering & Security (DMARC / DKIM)
- Zero Day Vulnerabilities and Supply Chain Risks
- Network Segmentation/ Network Monitoring
- M&A DD and Integration

Thank You

Heather Hughes
Vice President, Cyber Solutions
Stroz Friedberg, an Aon Company
832-480-3266
Heather.L.Hughes@aon.com

About Aon Cyber Solutions:
Our Cybersecurity experts help clients solve complex challenges prevalent in today’s digital, connected and regulated world.
Our focus is on cybersecurity, with leading experts in digital forensics, incident response and security science; investigations; and due diligence.

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.