STATE OF THE INDUSTRY

CYBERSECURITY

Operational Technology

OTA
OHIO TRUCKING ASSOCIATION

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

CYBERSECURITY

Operational Technology

The sophistication of cyber threat actors is perpetually on the rise, as evidenced by the ever-changing techniques and approaches they use to compromise systems. Their ultimate goal is usually profit—which they achieve using tactics that create both disruption and, specifically, the threat of lost revenue for the targets they pursue.

As with any normal business practice, threat actors encounter a cost to learning the tricks of the trade and developing the capabilities to execute their craft effectively. Understanding how this model works is an important step toward appreciating the level of commitment most organizations should undertake to thwart the cyber threats facing them.

Threat actors typically view organizations that have poor cyber protections in place as being easier targets with greater profit potential, but an important part of that equation is the impact (or potential threat of loss) that can be achieved through an attack.

The Transportation and Logistics (T&L) industry represents an attractive opportunity for threat actors due to the potential supply chain disruption resulting from a compromise in the systems responsible for schedules, payment cycles, shipments, etc.

To help better understand the cybersecurity challenges organizations like yours may face, our cybersecurity team shares some of the top cybersecurity concerns facing the T&L industry and the related best practices to mitigate these risks.

The Cyber Risk of Expanding Operational Technology

As modern organizations across all industries are becoming increasingly dependent on web application services and operational technology (OT), the sheer abundance of threat actors is but one of the many factors increasing the frequency and impact of cyber incidents. The exponential adoption of web services creates a shifting threat landscape for business leaders to navigate—often one with more cyber risk than commensurate budget levels needed to manage it.

Additionally, the level of security testing and protective capabilities of an individual OT or web application may not maintain pace with an industry that adopts it. Application security is a moving target and requires continuous research, testing and updates to maintain effective protective controls. Startups rushing to market, mid-market competitors minimizing costs or tech-giants slashing budgets can all impact the security of their applications and, consequently, the security of the organizations that depend on them.

Even mature organizations that aggressively fund security initiatives and only implement hardened industry-leading solutions are limited by the ability of their people, processes and technology to react to discovered vulnerabilities and exploitations. For those reasons and many more, it is difficult to find a cybersecurity professional who disagrees with the "not if, but when" reality organizations face as they seek to prioritize the cyber security controls most needed to plan and respond in the event of an incident.

Cybersecurity and the Transportation Industry

Cybersecurity broadly transcends industry, but there are noteworthy aspects of the T&L industry.

- **Historic Trends** – T&L has historically prioritized physical safety and security over cybersecurity, so they tend to have a larger gap to close across the board than do industries that prioritized cybersecurity sooner or that have yet to adopt OT as heavily.
- **Commonly Targeted Industry** – T&L cyber-attacks are attractive targets, as they historically pay higher dollar to avoid revenue and reputational loses. **Threat actors know they can add another zero to the ransom and still get paid when disruption to the global supply chain is at stake.** Below are a few examples of cyber incidents in the T&L industry for additional perspective on targets and potential damages:
  - » **2021: Metropolitan Transportation Authority** – The Metropolitan Transportation Authority (MTA) was breached by a hacking group that exposed severe vulnerabilities in the MTA's transportation network. The attackers, suspected to be the Chinese government, did not override any vehicle controls, but the fact they got into the system so fast caused great concern within the industry.
  - » **2021: ATC Transportation** – Threat actors used malware to launch a ransomware attack on ATC Transportation which resulted in a data breach exposing current and past employees' personal information. The data included social security numbers, drug test results and names.
  - » **2020: Matson** – Matson suffered a high-profile incident after being hit with a Windows REvil ransomware attack. The stolen data included employee data, as well as highly sensitive materials from their tax records, client databases and logistics group.
  - » **2017: Maersk** – The largest global shipping company Maersk was at the center of what industry experts believed to be the most devastating cyber-attack in history. In this scenario, Maersk was impacted due to a third-party that did not patch against the known Microsoft vulnerability Eternal Blue. The attack resulted in massive shipping delays after their systems were offline for three days. This impacted nearly 50,000 of their endpoints across over 600 cities in 130 countries… all because their vendor failed to apply a vulnerability patch.
- **Legislation and Regulation** – Since T&L is so vital to our health and economy, the industry is also subjected to influence from both the federal and state governments through legislation, regulations, spending and various funding. These additional requirements can have a significant impact on an organization's cybersecurity roadmap.

Understanding Cyber Insurance

Insurance carriers continue to increase requirements for targeted industries such as T&L. Below are a few examples of cybersecurity insurance policy requirements:

- **Multi-factor authentication** – When it comes to any remote access or accounts with administrative privileges, it is critical that businesses require users to identify themselves with something more than just a username and password. The second form of identification needs to be something you are or something you possess.
- **Endpoint Detection and Response (EDR)** – Businesses need to make sure that their employees' devices are protected by second generation anti-virus and anti-malware software. The solutions that only look for a virus' "fingerprint" are no longer considered acceptable.
- **Secured, Encrypted and Tested Backups** – To protect their data, businesses need to ensure that their backups are both encrypted and stored in a secure location. Many of the underwriters are defining "secure" as: the backups are either offline or immutable.
- **Privileged Access Management** – Businesses should make sure that access to highly privileged accounts (including system accounts) are protected and managed using an encrypted password vault.
- **E-mail Filtering and Web Security** – The easiest way to access one's system is to take advantage of human curiosity. Automatically interrogating emails for suspicious content (attachments and links) before the designated recipient has a chance to open them can help reduce their risk of falling for a phishing attack.

Strategic Takeaways

Fortunately, the average modern threat actor prioritizes higher-revenue and lower-effort targets to maximize profits. **This is why the goal for most organizations is not to become un-hackable, but rather to raise the bar high enough that they don't offer low-hanging fruit to exploit.** As an organization grows, so does its cyber risk—and its cybersecurity posture should respond in kind.

Below are some best practices and strategic takeaways for consideration:

- **Assessment Services** – Get a baseline of your posture through a combination of network penetration testing, cyber maturity framework assessments and tabletop exercises.
- **Back up Files** – Routinely back up files on secure servers.
- **Cyber Liability Insurance** – Explore options and know the policy limitations.
- **Enforce Password Defenses** – Require strong passwords, policies and multi-factor authentication.
- **Incident Response** – Have an incident response plan ready and a team on 24/7 retainer.
- **Industry-Leading Solutions** – Invest in effective products and tools, but vet your vendors: ask them for proof and results of third-party security testing.
- **Leverage Trusted Advisors** – Why reinvent the wheel? Talk to peers and experts.
- **Security Awareness Training** – Educate users about strong passwords, phishing, etc.
- **Update Software** – Keep all software up to date to ensure vulnerabilities are patched.

About Schneider Downs Cybersecurity

The Schneider Downs cybersecurity practice consists of expert practitioners offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team. In addition, our Digital Forensics and Incident Response teams are available 24x7x365 at 1-800-993-8937 if you suspect or are experiencing a network incident of any kind.

To learn more, visit our dedicated Cybersecurity page or contact the team at cybersecurity@schneiderdowns.com.

Want to be in the know? Subscribe to our bi-weekly newsletter, Focus on Cybersecurity.

OTA
OHIO TRUCKING
ASSOCIATION

Ohio Trucking Association

The Ohio Trucking Association is a 100-year-old full-service trade association operating in Columbus, Ohio. With over 815 total members in the trucking, logistics, warehousing and moving industries, our promise to our members is simple: the Ohio Trucking Association will work to improve operational efficiency, profitability and relevancy for all of Ohio's transportation industry. Advocacy, professional development, networking and cost savings initiatives are the keys to carrying out this promise to our members. No matter what the cause, our industry is stronger when operating as one. We encourage you to explore more about becoming involved with the Ohio Trucking Association at **www.joinota.com**.

Thomas A. Balzer, CAE
President & CEO
(614) 653-0290
tom@ohiotrucking.org

Bradie Berry
Vice President
(614) 519-6462
bradie@ohiotrucking.org

Michelle Finney
Marketing & Events Coordinator
(216) 632-9029
michelle@ohiotrucking.org

Della Hole
Office Manager
(614) 753-5125
della@ohiotrucking.org

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Schneider Downs Transportation and Logistics Industry Group

Established in 1956, Schneider Downs has grown to be one of the largest independent public accounting and advisory firms in Columbus, Ohio; Western Pennsylvania and Washington D.C., with nearly 500 personnel in total, including 52 shareholders and partners.

More than 25 years ago, we established the Schneider Downs Transportation and Logistics Industry Group. The group includes assurance, tax, technology and management consulting professionals who combine their individual expertise to serve our wide range of transportation and logistics clients—from local carriers to national enterprises, including: trucking, general freight, flatbed and box, TL, LTL, tank waste brokerage, bulk commodity dump, 3PL, heavy hauling/permitted loads, moving and warehousing. The Transportation and Logistics Industry Group meets on a regular basis to review and analyze issues central to this industry. As a result, our transportation and logistics professionals possess the most current knowledge of transportation issues, regulations and trends. We work with you to seek innovative ways to reach your strategic goals.

Carl D. Scharf, CPA
Shareholder, Tax Services
(614) 586-7139
cscharf@schneiderdowns.com

Michael A. Renzelman, CPA
Shareholder, Audit and Assurance Services
(614) 586-7203
mrenzelman@schneiderdowns.com

For more information about this report, please visit
https://www.schneiderdowns.com/transportation-logistics-resources

OTA
OHIO TRUCKING ASSOCIATION

655 Cooper Road
Westerville, OH 43081

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

65 East State Street
Suite 2000
Columbus, OH 43215