

The Transportation Lawyer

A Comprehensive Journal
of Developments in
Transportation Law

December 2018
Volume 20
Number 3



**Transportation Lawyers
Association**

translaw.org

A Joint Publication of the Transportation Lawyers Association
and the Canadian Transport Lawyers Association

CTLA  **ctla.ca**
Canadian Transport Lawyers Association

STATE DEPARTMENTS OF TRANSPORTATION AND CYBERSECURITY: *Fund Now or Risk Dire Consequences*



Dylan Smith*

The United States Department of Transportation asserts that State Departments of Transportation “are at the heart of planning, design, construction, and operations and maintenance projects across all travel modes.”¹ In centering on a specific state Department of Transportation, Texas’ Department of Transportation’s chief duties “are to delineate, build and maintain all state highway and public transportation systems; issue permits for the use of heavy trucks; and register motor vehicles.”² However, as public transportation systems have become increasingly complex with the proliferation of technology, more and more systems are being connected to Department of Transportation computer networks. As more systems are intertwined with Department of Transportation computer networks, state Departments of Transportation are burdened with maintaining much more complex public transportation systems. Without proper funding for state Departments of Transportation such as Texas to employ robust IT and cybersecurity committees (“Security Operations Centers”) to both combat and prevent access by cyber attackers, the departments are at risk, which could lead to the access of both

critical state and municipal infrastructures and valuable data about individuals/citizens.

Development of Departments of Transportation

As stated both broadly and specifically above, state Departments of Transportation have long been centered on building and maintaining projects across all travel modes, especially highways and public transportation systems. However, Departments of Transportation are now tasked with far more than maintaining asphalt and concrete. As we continue to evolve and advance into the Information Age and the Digital Revolution, there has been a rapid adoption of technology across all aspects of transportation, where Departments of Transportation are now digitally connected with many modes of transportation, including but not limited to, airports, ports, railways (including high speed rail), buses, toll roads and soon, self-driving automobiles. With this rapid adoption of technology comes significant risks for Departments of Transportation as they are increasingly becoming attractive targets for cyber attackers. However, despite Departments of Transportation wielding more and more control over large transportation hubs and cyber-attacks on state and municipal agencies on the rise, the departments themselves have been slow to create their own IT departments and Security Operations

Centers to properly protect themselves from cyber-attacks.

Recent Cyber-attacks Reveal State and Municipal Agencies are Prime Targets

Cyber-attacks have been increasing over the years, in both prevalence and disruptive potential, with the World Economic Forum now rating a large-scale breach of cybersecurity as one of the five most serious risks facing the world today.³ By 2021, the global cost of cybersecurity breaches is estimated to reach \$6 trillion, double the total for the year 2015.⁴ Cyber breaches recorded have almost doubled in five years and the costs of cyber-attacks are continuing to rise.⁵ While companies may have originally been the target for cyber attackers, it appears a shift towards state and municipal agencies, including Departments of Transportation, has been taking place in recent years due to their cybersecurity vulnerabilities. Just between February and March of this year, cyber-attacks were reported on: (1) Allentown, Pennsylvania’s municipal systems and Savannah, Georgia’s government servers; (2) twelve different state agencies of Connecticut in one attack; (3) Atlanta, Georgia’s infrastructure and computer systems; and (4) two separate attacks on Colorado Department of Transportation’s computer system. These attacks resulted in reactive responses due to lack of proper cybersecurity measures in place with millions being spent to regain control of government systems.

*Chamblee Ryan, P.C. (Dallas, Texas)

Allentown, Pennsylvania and Savannah, Georgia

The city of Allentown, Pennsylvania's computer systems were infected by a malware program, Emotet, causing the city to shut down their municipal systems to contain the virus.⁶ Consequently, among other things, Allentown's finance department could not complete any external banking transactions and the police department could not access databases controlled by the Pennsylvania State Police while the city assessed the damage caused by the cyber-attack.⁷ The virus was capable of infecting all city systems that ran Microsoft software if it continued to spread, including Allentown's surveillance camera network (the city has about 185 located throughout the municipality).⁸ It was estimated that it would cost Allentown around \$1 million to fix the problems caused by the cyber-attack, which did not include the lost productivity from the shutdown of its systems.

Likewise, a malware virus attack occurred on the city of Savannah, Georgia, resulting in the infection of government servers and computers.¹⁰ The City Hall of Savannah thankfully took swift action to halt communications between city servers, limiting the spread of the virus. As a result, the attack interrupted several city services and every individual city computer needed to be examined to eliminate the virus.¹¹

Atlanta, Georgia

As evidenced by the large scale cyber-attack on Atlanta, Georgia, not even capital cities/metropolises are necessarily safe from cybercriminals depending on their cybersecurity measures. Atlanta was victim to a ransomware attack that crippled its computer systems and targeted the city's infrastructure.¹² After the cyber attackers gained control, in order for the city to regain access to its computer systems, a ransom of \$51,000 in bitcoin was demanded.¹³ The city ended up entering into emergency

contracts totaling \$2.7 million to help restore the city's computer network, which does not even account for the cost of the coordination of the city's recovery efforts or the lost productivity encountered by city employees (could not access their computers for days after the hack).¹⁴

Connecticut State Agencies

After the state of Connecticut's security monitoring system detected a suspicious event, it was discovered that 160 computers across twelve (12) different agencies in the state were infected with a ransomware virus.¹⁵ Like the virus in Allentown, Pennsylvania, it was capable of infecting all city systems that ran Microsoft software.¹⁶ However, the discovery of the cyber-attack resulted in the mobilization of Connecticut's agency IT workforce, which worked to and did effectively contain the spread of the ransomware virus after the fact, still costing the state considerable time and resources to recover.¹⁷

Colorado Department of Transportation

Finally, in perhaps an omen to come to Departments of Transportation across the nation unless preventative measures are taken, the Colorado Department of Transportation was the subject of two ransomware attacks within a couple weeks of each other that forced the department to shut down more than 2,000 computers in the immediate aftermath.¹⁸ Like the cyber-attack on Atlanta, the cyber attackers demanded payment in bitcoin in order for the state to recover encrypted computer files.¹⁹ Those who were brought in to help the Colorado Department of Transportation investigate, contain and recover files while not succumbing to the cyber attackers' demands included: (1) IT employees; (2) the FBI; (3) the Colorado National Guard; (4) state emergency operations; and (5) private companies.²⁰ While the state of Colorado's backup system prevented data loss,

personal data on employee's computers may not be recovered.²¹ In total, the Colorado's Office of Information Technology estimated that the costs associated with the cyber-attack would total between \$1 and \$1.5 million, which only includes overtime pay and other unexpected costs.²²

However, given the interconnectivity of Departments of Transportation today which could allow cyber attackers access to anything connected to the department's network, \$1-\$1.5 million in remedial damages and the potential loss of personal data on employee's computers is a relatively advantageous outcome considering what could have happened. For example, in 2008, a fourteen year old boy hacked the tram system in Poland, giving him the control to change the tram's track points.²³ Consequently, the teenager caused the derailment of four trams and injured at least a dozen people.²⁴ More recent and applicable examples include both the San Francisco's light rail system²⁵ and the Sacramento regional transit agency²⁶ being the targets of cyber attackers who subsequently demanded a ransom for the cities to regain control of their mass transportation systems. Departments of Transportation desperately need to increase their funding towards cybersecurity to ensure cyber attackers in the future cannot obtain such control over all of the modes of transportation that are and will be digitally connected to the departments, especially if the cyber attackers are looking for leverage in regards to their demands for ransom.

Cybersecurity Funding and Knowledge Across Organizations

The lack of funding and dedicated IT departments and Security Operations Centers is not just a problem unique to Departments of Transportation and other state and municipality agencies. Each year, Ernst & Young conducts and produces a Global Information Security Survey

TLA Feature Articles and Case Notes

exploring the most important cybersecurity issues facing organizations.²⁷ This past year, Ernst & Young gathered information from nearly 1,200 organization's CIOs, CISOs and other executives and compiled it into their Global Information Security Survey for 2017–2018. While these findings deal with organizations across the board and not just Departments of Transportation, they highlight needs for all organizations in regard to cybersecurity:

- 87% of respondents said they need up to 50% more for their cybersecurity budget;
- Only 12% of respondents felt it was very likely they would detect a sophisticated cyber-attack;
- 48% of respondents do not have a Security Operation Center, even though they are becoming increasingly common;
- 57% of respondents do not have, or only have an informal, threat intelligence program;
- Only 36% of Boards believe they have sufficient cybersecurity knowledge for effective oversight of cyber risks;
- 89% of respondents say their cybersecurity function does not fully meet their organization's needs;
- Only 4% of organizations are confident that they have fully considered the information security implications of their current strategy, and that their risk landscape incorporates and monitors relevant cyber threats, vulnerabilities and risks.²⁸

State Departments of Transportation's Needs Moving Forward

Increase in Funding

As the numbers above show, organizations across the board do not have enough funding going into their cybersecurity budget. In order for state Departments of Transportation to adequately protect their vast

infrastructure and compiled personal data from cyber attackers, more resources must be allocated to the funding of state IT departments and cybersecurity. Without an increase in funding to bolster state Departments of Transportation's defenses, state Departments of Transportation will continue to be vulnerable and only capable of reactive responses to cyber attackers, causing millions of dollars of damages and placing the welfare of the public they serve into the hands of cyber attackers looking to obtain ransoms from cities and states with deep pockets.

Development of Distinct IT Departments and Security Operations Centers

Given the attractiveness of state Departments of Transportation and cyber-attack targets coupled with the great power a cyber-attacker could wield if he or she gain access, each state Department of Transportation should create distinct IT Departments and a Security Operations Center that only serve their cybersecurity needs. A Security Operations Center "is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis."²⁹ A Security Operations Center's "goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes."³⁰

A Security Operations Center, coupled with its own distinct IT department, would allow state Departments of Transportation to have independent committees completely devoted to protecting the departments from cybersecurity threats, as opposed to sharing IT and cybersecurity resources across multiple state and municipal agencies. Moreover, a Security Operations Center would be proactive in their approach to cybersecurity threats as opposed to merely reactive. Security Operations Centers provide continuous monitoring and analysis

of data activity in order to stay on top of threats and shut them down before they can breach an organizations system and/or immediately detect the threat to severely limit the spread of any virus.

Government Collaboration amongst Separate, Distinct IT Departments and Security Operations Centers


While I believe that each state Department of Transportation should have its own independent IT Department and Security Operations Center, I also believe that each state IT Department and Security Operations Center should work together to collaborate against cybersecurity threats that they encounter. Cooperation among the Departments of Transportation would allow the sharing of intelligence about cybersecurity threats and solutions in order to create a beneficial synergy that results in a stronger cybersecurity defense for all. For example, the Colorado Department of Transportation, as noted above, was victim to two separate cyber-attacks at the beginning of this year. The millions they spent in restoring their government servers/systems and placing more robust cybersecurity measures in place no doubt resulted in a deeper understanding of their cybersecurity flaws and strengths, which could be passed to other state Departments of Transportation for the benefit of all.

Conclusion

Our world is continuing to become more and more connected. Every organization's technology infrastructure, especially state Departments of Transportation, are becoming more and more complex, spanning networks of tools and technologies and present cybersecurity risks that could potentially endanger the public at large. To make matters even more difficult, cyber-attackers each year become more and more difficult to detect, requiring cybersecurity defenses to be sophisticated and continually improving to

match the advances of cyber-attackers. Given the rise of cyber-attacks on state and municipal agencies, it is even more pressing that state Departments of Transportation act now to bolster their cybersecurity defenses. In order for state Departments of Transportation to protect their vast critical infrastructures and personal information, they must first and foremost push for and obtain a larger

budget for cybersecurity. A larger budget for cybersecurity is an absolute must, given that large-scale breaches of cybersecurity is one of the five most serious risks facing the world today for organizations. State Departments of Transportation should then use the additional budget for cybersecurity to create individual, distinct IT Departments and Security Operations Centers so that they can have IT and

cybersecurity professionals completely devoted to protecting the departments from cybersecurity threats. Lastly, state Departments of Transportation across the United States should collaborate to share their knowledge and resources to strengthen each department's cybersecurity so that cyber attackers no longer view state Departments of Transportation as easy targets for a quick payday. 

Endnotes

- 1 "State DOT's Responsibilities." *US Department of Transportation*. United States Department of Transportation, 5 Feb. 2016, www.transportation.gov/civil-rights/civil-rights-awareness-enforcement/state-dots-responsibilities.
- 2 Huddleston, John D. "Texas Department of Transportation." *Handbook of Texas Online*, accessed August 06, 2018, <http://www.tshaonline.org/handbook/online/articles/mctgn>.
- 3 "The Global Risks Report 2018." *World Economic Forum*, 2018.
- 4 *Id.*
- 5 *Id.*
- 6 Sheehan, Daniel P. "What Is Emotet? The Virus That Hit Allentown Computers Is Widespread and Dangerous." *The morning call.com*, 22 Feb. 2018, www.mcall.com/news/local/allentown/mc-ews-allentown-virus-follow-20180221-story.html.
- 7 *Id.*
- 8 *Id.*
- 9 *Id.*
- 10 "Government Servers in Savannah, Georgia Hit by Malware Attack." *Insurance Journal*, 21 Feb. 2018, www.insurancejournal.com/news/southeast/2018/02/21/481237.htm.
- 11 *Id.*
- 12 Deere, Stephen. "Cost of City of Atlanta's Cyber Attack: \$2.7 Million—and Rising." *Ajc, The Atlanta Journal-Constitution*, 2 Aug. 2018, www.ajc.com/news/cost-city-atlanta-cyber-attack-million-and-rising/nABZ3K1AXQYvY0vxqfO1F1/?icmp=np_inform_variation-control.
- 13 *Id.*
- 14 *Id.*
- 15 "Cyber Attack Targets State Agencies." *NBC Connecticut*, NBC Connecticut, 19 Mar. 2018, www.nbcconnecticut.com/news/local/Connecticut-State-Agencies-Experience-Cyberattack-475102753.html.
- 16 *Id.*
- 17 *Id.*
- 18 Chuang, Tamara. "Cyber Attack on CDOT Computers Estimated to Cost up to \$1.5 Million so Far." *The Denver Post*, The Denver Post, 6 Apr. 2018, www.denverpost.com/2018/04/05/samsam-ransomware-cdot-cost/.
- 19 *Id.*
- 20 *Id.*
- 21 *Id.*
- 22 *Id.*
- 23 Leyden, John. "Polish Teen Derails Tram after Hacking Train Network." *The Register*®—*Biting the Hand That Feeds IT*, The Register, 11 Jan. 2008, www.theregister.co.uk/2008/01/11/tram_hack/.
- 24 *Id.*
- 25 Weise, Elizabeth. "Ransomware Attack Hit San Francisco Train System." *USA Today*, Gannett Satellite Information Network, 29 Nov. 2016, www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/.
- 26 Bizjak, Tony. "Hackers Attack Sacramento Transit System and Demand \$8,000 Ransom." *Sacbee, The Sacramento Bee*, 20 Nov. 2017, www.sacbee.com/news/local/article185669953.html.
- 27 "Cybersecurity Regained: Preparing to Face Cyber Attacks—20th Global Information Security Survey 2017–18." *Ernst & Young*, 2017.
- 28 *Id.*
- 29 Lord, Nate. "What Is a Security Operations Center (SOC)?" *Digital Guardian*, 11 July 2018, digitalguardian.com/blog/what-security-operations-center-soc.
- 30 *Id.*