Implications of the Sunburst Cybersecurity Attack on the Transit Industry

Project 2111
January 2021

Scott Belcher, JD, MPP and Brandon Thomas, MBA

In December 2020, the United States experienced its worst cyber-attack in reported history. The scale, breadth and depth of the Sunburst cyber-attack is still emerging. The attack, originally detected by the cybersecurity firm FireEye, was discovered because of a breach of their internal systems that was traced to the IT management software they used, supplied by SolarWinds. Since the discovery, the investigation has uncovered that over 18,000 organizations may have been breached as far back as March 2020. Entry points have been found beyond SolarWinds, further expanding the attack's reach. Impacted organizations include government and corporate behemoths, from the Department of Defense to chipmaker Intel. Though the details are still coming to light, one thing is already very clear: every public and private organization, both in the United States and abroad, must focus on its cybersecurity program. These organizations must ensure they understand program vulnerabilities and have a plan in place to address them on an on-going basis.

Though the impact of Sunburst on public transit agencies is not yet known, several other recent cyber-attacks confirm that the transit industry is already a cyber target. Recent attacks on public transit agencies include the Southwestern Pennsylvania Transportation Authority (SEPTA) in Philadelphia, which is still recovering from a malware attack last August that took down their critical systems for weeks.[1] And in Vancouver, the transit system is in the midst of recovering from and assessing the damage of a ransomware attack just a few weeks ago.[2] To avoid similar results, cybersecurity preparedness must become an immediate priority for all leaders in public transit.

Public transit is part of the U.S.' Transportation Security Sector, one of 16 sectors deemed critical to national security.[3] In October 2020, the Mineta Transportation Institute published *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendation to Enhance Surface Transit Cyber Preparedness* (the Study) which found that most public transit agencies are woefully unprepared when facing cybersecurity threats. The Study assessed the readiness of U.S. transit agencies to address, mitigate, and respond to the growing number of cybersecurity threats, with responses from agencies that serve nearly a third of the U.S. population. Over 80% reported that they were prepared for a cybersecurity threat, yet only 60% had a cybersecurity program in place. This disconnect is very concerning in its own right and is made even more so given that the respondents were not aware of the SolarWinds breach at the time of the Study.

The Study findings make clear that cybersecurity has not been a priority for many agencies in the public transit industry. Even though there are numerous resources available from Federal agencies and industry associations, the data suggests that these resources are not always taken advantage of because of competing priorities, lack of internal resources, or focus. Even following a cyber-attack, transit agencies are not necessarily investing in a cybersecurity culture. The

authors saw no difference in cybersecurity budgets and staffing between agencies that never suffered an attack versus those that had.

However, as a result of Sunburst, the authors anticipate that regulatory agencies will be far more motivated to ensure that all agencies engage in cybersecurity preparedness. The incoming Biden Administration has already indicated they would play a more deliberate and expansive role in upgrading the nation's cybersecurity posture. For example, the Federal Transit Administration has indicated that it intends to include cybersecurity as part of its tri-annual audits.

The coming pressure to improve the cybersecurity posture will mean that that agencies will need to invest more broadly in their cybersecurity infrastructure, not just their IT security team. As defined in the National Institute of Standards and Technology (NIST) cybersecurity framework —the backbone of all U.S. cybersecurity policy— an effective cyber risk management program leverages technology, but also requires cultural and process changes as well. The errant click of a malicious email link can cause as much harm as an inadvertently accessible server. Every person in the organization needs to be vigilant to the risk (and this vigilance needs to be taught on a regular cadence).

Securing the transit agency's systems from cyber-attack is one thing; agencies must also ensure their vendor supply chain is doing its part as well by including language in vendor contracts requiring vendors to manage their cyber risk. Supply chain control and understanding is more important than ever, as exemplified by SolarWinds' role in the Sunburst attack.

Given that most public transit agencies have limited cybersecurity programs in place, it is unlikely the vendors that serve them have been asked about their practices, let alone required to meet at least some basic levels of cybersecurity preparedness. This is not a one-time conversation. This too must change, and quickly, given the Sunburst attack.

And, as recent events confirm, it is critical not just to defend against attacks but to also prepare for the inevitable breaches that will occur. This means having the right response plans in place and practicing the response so that the organization is ready when the inevitable happens (over two thirds of agencies surveyed did not have a crisis communications plan in place, let alone had it been practiced). Having the right log maintenance schedules in place so that agencies can quickly ascertain the reach of a breach is one of many steps required to

NIST Framework

Identify: develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities;

Protect: develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services;

Detect: develop and implement the appropriate activities to identify the occurrence of a cybersecurity event;

Respond: develop and implement the appropriate activities to take action regarding a detected cybersecurity event;

Recover: develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

ensure effective cyber risk management (only 50% of public transit agencies surveyed meet this most basic requirement; 12% don't keep logs at all).

The transformation of the public transit sector from its current unprepared state will not happen overnight. It will take concerted effort from agency leadership, regulators and industry experts to ensure the right systems are in place, the right behaviors are taught, and the right policies are documented, audited, and practiced. The Sunburst attack has further reinforced the fact that transit agencies need to start now to improve their cybersecurity posture, lest these attacks become more brazen, more widespread, and more costly in the future.

The United States has never publicly acknowledged a breach of the scale of Sunburst before. It is clear that the new Administration will need to focus much more intensely on cybersecurity and put additional resources and focus behind this issue. This attention will very quickly make its way to operating entities. The transportation industry needs to prepare itself for the coming attention and resulting change in business practice.

Endnotes

1. https://www.govtech.com/security/Pennsylvania-Transit-Agency-Still-Recovering-from-Cyberattack.html

2. https://www.zdnet.com/article/ransomware-attack-cripples-vancouver-public-transportation-agency/

3. https://www.cisa.gov/critical-infrastructure-sectors

About the Authors

Scott Belcher, JD, MPP, is the CEO of SFB Consulting, LLC. Prior to founding SFB Consulting, LLC he served for two years as the CEO of the Telecommunications Industry Association and for seven years as the CEO of the Intelligent Transportation Society of America. Brandon Thomas is a Partner at Grayline Group, a firm focused on helping organizations understand and manage for disruption, as well as a Managing Partner of Blockview Partners, a firm focused on understanding the emerging blockchain and cryptocurrency space.

This report can be accessed at transweb.sjsu.edu/research/2111

MTI is a University Transportation Center sponsored by the U.S. Department of Transportation's Office of the Assistant Secretary for Research and Technology and by Caltrans. The Institute is located within San José State University's Lucas Graduate School of Business.