Is There a Light at the End of the Tunnel? The Outlook for Cybersecurity Insurance and Transit in 2024

Project 2406
April 2024

Scott Belcher and Todd Chollet

Introduction

We begin 2024 with a record January and second highest number of attacks ever, in fact, 130% more than in 2023. Similarly, unreported attacks increased 75% over the previous year.[1]

BlackFog, "The State of Ransomware 2023 Annual Report" reporting that overall cybersecurity attacks continue to increase, despite a dip towards the end of 2022 that will be discussed later in this report.

The cybersecurity threat landscape has changed for public transportation operators and insurance companies in ways they could have never imagined. Not only has the sheer volume of cyberattacks increased exponentially, but the number of successful attacks and the average cost to recover from them has increased as well. Some operators have responded by taking action to shore up their cyber resiliency while others have continued to assume that it will never happen to them. Insurance companies have responded by limiting coverage, adjusting the cost of coverage, tightening underwriting, and even exiting the market. Regulators have responded with increased education, resources, and the imposition of basic cybersecurity requirements.

This White Paper reviews the changes in the risk landscape, the responses of the insurance market and public agencies to these changes, and provides recommendations for how the different segments of the market can continue to help manage the risk of catastrophic loss.

Cybersecurity Attacks Are on the Rise

Over the past few years there has been a significant increase in the number and scale of cybersecurity attacks against companies of all sizes, including public transit agencies. Attacks against large companies tend to receive more coverage in the news. Examples include CNA Financial Corp. Which resulted in a reported $40 million ransom payment;[2] the Colonial Pipeline ransomware attack that caused disruption to the distribution of oil in the U.S.;[3] and the MoveIT campaign that is considered one of the most widespread attacks of 2023 and resulted in ransomware payments between $75 and $100 million.[4]

Cybersecurity attacks on small and mid-size companies are also rampant. As far back as 2014, the National Cybersecurity Institute reported that 50 percent of all small to medium-sized businesses have been the victims of cyberattack.[5] More recent indications that small businesses are not immune can be found in the 2023 NetDiligence Cyber Claims Study that found 98 percent of all cyber claims come from small to medium enterprises.[6]

Cybersecurity attacks and threats to United States critical infrastructure are a major concern as they can have significant economic, national security, and public safety implications. The Cybersecurity Infrastructure & Security Agency (CISA) has identified the Transportation Systems Sector as one of 16 critical infrastructure categories that are considered "assets, systems, and networks that provide functions necessary for our way of life."[7] "Mass Transit and Passenger Rail" is subcategories of the Transportation Systems Sector which is the focus of this report.

Public transit providers have experienced a similar uptick in the frequency and severity of cyber incidents. Check Point Research found that the global transit industry has experienced a 186 percent year-over-year increase in weekly ransomware attacks since June 2020.[8] Examples of transit agencies that have been the subject of recent cybersecurity attacks include the Washington Metropolitan Area Transit Authority, Bay Area Rapid Transit System, Southeast Pennsylvania Transportation Authority, Vancouver's TransLink in British Columbia, New York's Metropolitan Transportation Authority, Dallas Area Rapid Transit, and Santa Clara Valley Transportation Authority, and many others. In fact, it is becoming increasingly difficult to name a transit provider that does not acknowledge having a data breach or other disruptive cyber incident.

This is a changing pattern. In 2020 the Mineta Transportation Institute (MTI) conducted a survey of U.S. transit operators and found that of the 90 agencies that responded to the survey, only 23 (roughly 25 percent) admitted to having experienced a cybersecurity incident where more than 1,000 records were breached, over $10K in losses were incurred, or an operating system was down for more than one hour.[9] By comparison, during the same time period, Dell Technologies surveyed over 1,000 IT professionals from public and private organizations with over 250 employees across various industries and found that 82 percent had suffered a disruptive event (defined as downtime or data loss).[10] Though this comparison is not apples to apples, it does suggest that many public transit agencies that responded to the survey were unaware of cyber intrusion activity that had happened among their systems or chose not to share this information.

Neither the size nor the location of the transit agency makes an operator immune from attack. Perpetrators of ransomware attacks on transit agencies are generally looking for financial payouts—it is a criminal business operation. Examples abound of small agencies with fewer than 20 vehicles that have been the subject of a cyberattack.

In a l MTI study entitled Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges,[11] the authors cited an example of a system breach at a transit agency that viewed itself as an unlikely cybersecurity target as it was part of a Community Action Agency (CAA). CAAs are local public and private non-profit organizations that serve low-income communities by providing everything from transit services to early child development programs like Head Start. As the Executive Director of this particular CAA mused, "we are the good guys, and we have nothing. Why would they hack us?" The transit agency in this case provides roughly 80,000 annual fixed-route, on-demand, and paratransit trips for individuals in need of access to essential services in the community and ended up losing all its customer data because of the breach.

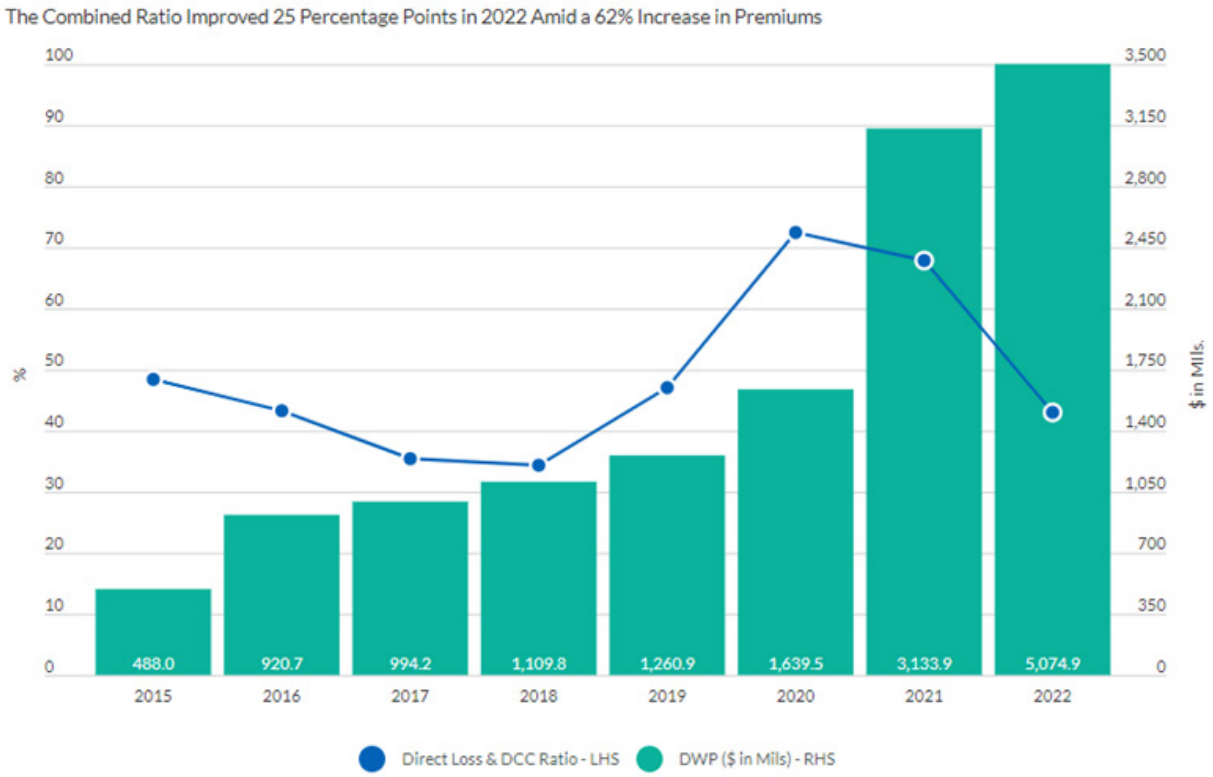
Industry experts cite numerous factors to account for the explosion of cyber breaches. Around 2016, ransomware transitioned from broad scale automated campaigns to more targeted extortion efforts against specific organizations. This switch led to growth in extortion revenues, which fueled

additional ransomware activity.[12] Growth and availability of ransomware-as-a-service (RaaS) decreased the barrier to entry for threat actors. Interconnectivity of devices and automated processes have naturally grown along with advances in technology. The sheer amount of exposed data continues to grow. The COVID-19 pandemic rapidly drove millions to a work-from-home model, which exposed vulnerabilities and lowered cybersecurity defenses associated with remote collaboration tools. Jùrgen Stock, Interpol Secretary General, echoed this in comments he made back in 2020, “Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19.”[13]

The Number of Cybersecurity Insurance Claims Are Rising Commensurately

Along with the growth in cyber attacks, there has been a corresponding rise of cyber insurance claims. NetDiligence publishes an annual study of cyber insurance claims data submitted by major cyber insurance carriers. In the most recent report, the study collected over 9,000 claims submitted between 2018-2022, whereas in 2013 there were less than 150 claims submitted for the analysis.[14] Fitch Ratings also found that cyber claims increased by 100 percent from 2018 to 2021.[15] While criteria utilized to track and report breaches are not consistent across all studies and reports, the increase in incidents, compromises, breaches, or attacks is consistent.

More evidence of increasing cyber insurance claims can be seen in the rapid rise of loss ratios from 2018 to 2020. A loss ratio represents the value insurers spent on claims relative to earned premiums. Commonly, insurers will aim to keep loss ratios under 65 percent. From 2018 to 2020, standalone cyber loss ratios more than doubled from 34 percent to 72 percent.[16]



PC Industry Aggregate. LHS - left-hand side axis. RHS - right-hand side axis. DCC - Defense and Cost Containment incurred. DWP - Direct written premium.
Note: Statutory Cybersecurity and Identity Theft Insurance Coverage Supplement Data.
Source: Fitch Ratings, S&P Global Market Intelligence

Figure 1. Standalone Cyber Risk Direct Loss and DCC Ratios[17]

Many insurance providers and brokers reported a recent change in appetite to insure public agencies starting at the beginning of 2023, when the market seemed to be stabilizing. One broker mused that this might be the result of public agency clients putting basic cyber hygiene protections in place. He noted that his firm was having a much easier time placing policies and, in many cases, without significant premium increases or changes in coverage. His comment was that “this might be the shortest insurance cycle and correction that I have seen in my career.”

The Cost of Responding to These Cybersecurity Breaches is Also Increasing

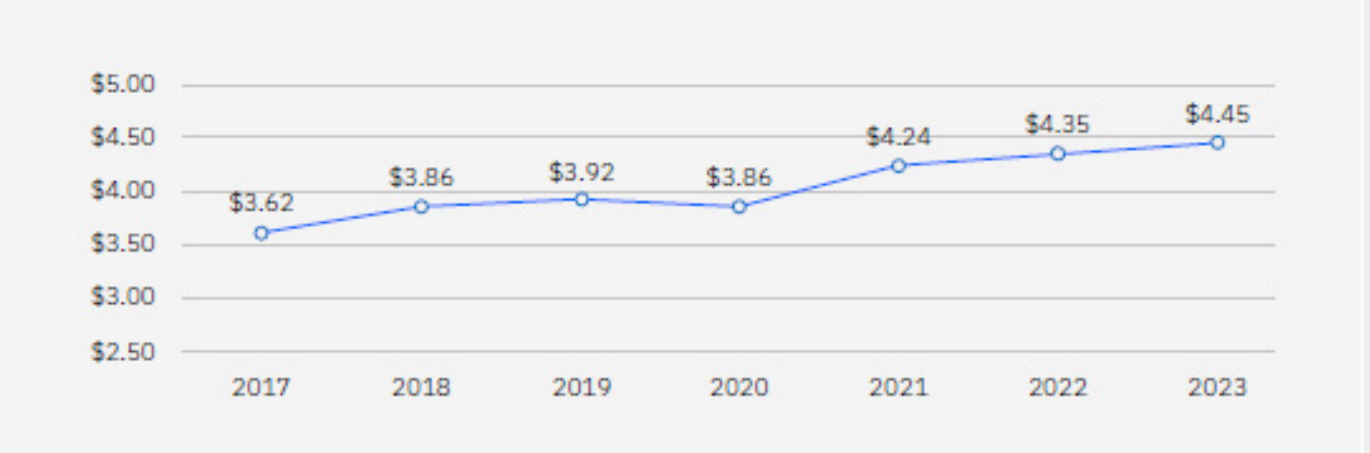


Figure 2. Total Cost of a Data Breach[18]

The average cost of a data breach is now $4.45 million.[19] This is a 2.3 percent increase from the 2022 IBM report and a 15.3 percent increase from the 2020 report. This cost is divided across four different cost categories: lost business, detection and escalation, post-breach response, and notification expense.

- Lost business costs represent 29 percent of the total cost of a breach and include activities that attempt to minimize loss of customers, business disruption, and revenue losses.
- Detection and escalation are reportedly the costliest and include expenses such as forensic and investigative activities, assessment and audit services, crisis management, and communications to executives and boards.
- Post-breach response costs include activities to help victims of a breach communicate with the company and conduct redress activities to victims and regulators.
- Notification costs encompass activities that enable a company to notify data subjects, data protection regulators, and other third parties.[20]

Ransomware payments in 2023 surpassed $1 billion, the highest number ever observed.[21] Ransomware is still one of the main drivers of insurance claims loss for small and medium enterprises including public transportation according to the recent NetDiligence Cyber Claims Study. Ransomware cyber incident costs for small to medium enterprises have increased substantially from $152,000 in 2018 to $865,000 in 2022 as noted in the chart below.[22]

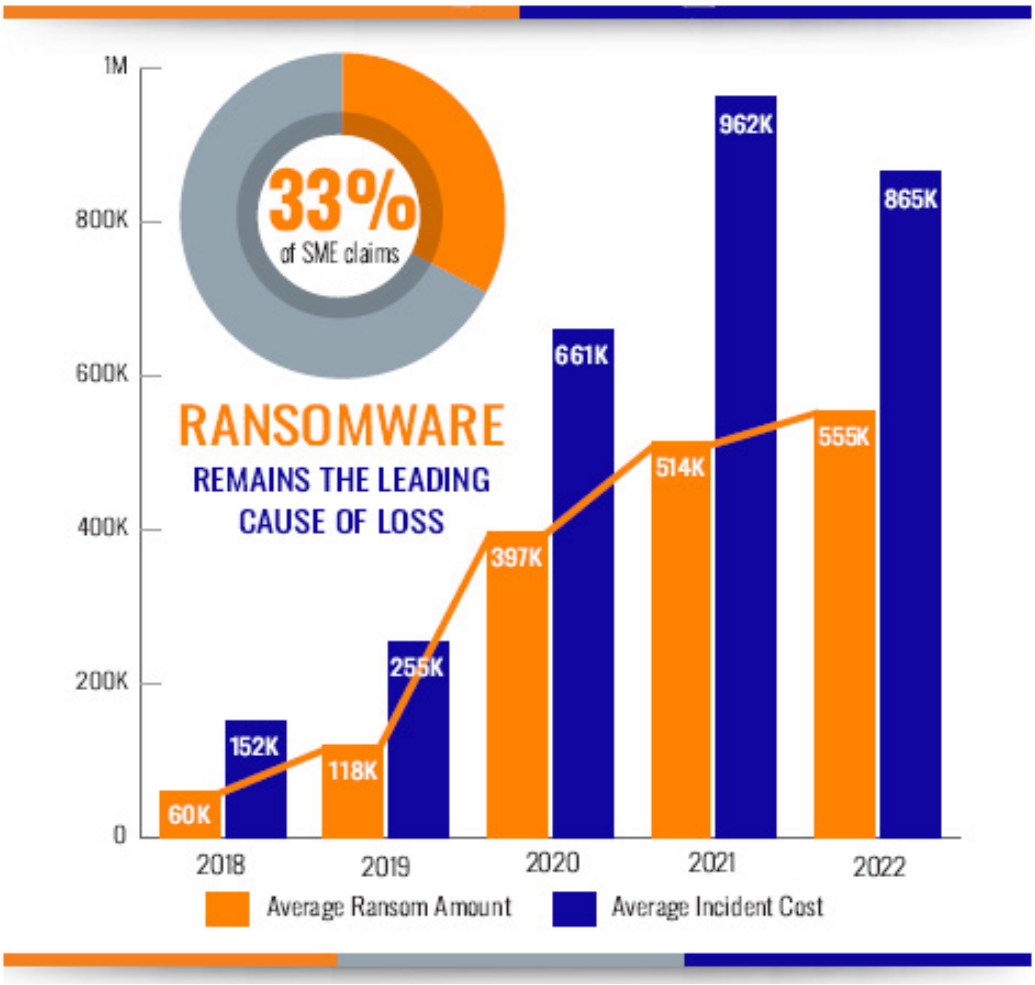


Figure 3. Average Costs for Ransomware[23]

Some of the increase in the cost of a breach can also be attributed to inflationary pressures on contributing costs, such as attorney's and IT professional's fees, period of downtime, lost intellectual property, and reputational damage.

Because of This Perfect Storm, Cybersecurity Insurance Underwriting Practices Are Adapting

Historically, insurance underwriters requested minimal information to offer cybersecurity coverage. In some cases, company name, revenues, and a website would complete an application. As cyber attacks have increased, insurers have been put under pressure to determine how to profitably underwrite cyber risk. Insurers were no longer accepting that their coverage was the sole cyber-readiness plan and began requiring an increasing amount of underwriting information about a company's cybersecurity program.

In a study published by the Journal of Cybersecurity, the researchers found from 2007 to 2017 in state filings that cyber insurers were pricing coverage in one of five methods: 1) estimated or guessed; 2) looked to competitors; 3) relied on external sources; 4) adapted prices from other insurance lines; and 5) leveraged the experience of their own underwriters.[24]

Because historical cyber claims data are relatively limited, and data samples can be less reliable because of the dynamic nature of cyber breaches, it's not surprising that underwriting changes have had to adapt.

Around 2020, insurers tightened underwriting standards, directly requiring insureds to bring their technological, operational, and people practice standards up to speed with the current state of cyber risk. Candace Whitmill, a broker with CRC's Executive Professional Practice Group, noted that these changes are timestamped on July 1, 2020, when Travelers began requiring Multi-Factor Authentication.[25]

Insurers also focused on removing their "silent cyber" exposure from other lines of coverage. Doing so has contributed to the growth of cyber-specific coverage. In 2017, NotPetya (a global cyber attack that hit millions of targets, the majority of which were in Ukraine along with numerous other countries, encrypted and corrupted files many of which were unrecoverable) caused billions of dollars in insurance losses. Reportedly, 85 percent of these were claims against property policies that did not specifically exclude or include cyberattacks.[26] Changes in cybersecurity coverage and cost within the transit industry are no different. Every operator interviewed said their coverage costs increased between 100 percent to 200 percent after 2020.

> One government contractor recounted that his company had recently responded to a Request for Proposal requiring a $50 million cybersecurity policy on a contract that was valued at less than $10 million over three years. He described the contract as a basic technology services contract no different from their other projects of this size, where the amount of cybersecurity coverage required would typically be about $2 million per year. After unsuccessfully questioning the need for that level of coverage, the contractor got bids to provide the level of coverage, which averaged $500,000 in annual premiums. Each insurer the company spoke with agreed that this was an unnecessary and unreasonable amount of coverage for the contract. The only way the contractor was able to bid on the contract was to build these costs into their unsuccessful proposal.

The confluence of these cyber events has presented a challenging environment for policyholders and other stakeholders in the industry to navigate. In addition to increased application questions, cyber insurers also began changing terms, pricing, available limits, adding coinsurances, and increasing deductibles, which narrowed industry appetites to maintain cyber insurance. Many policyholders tell stories of year-over-year premiums increasing by more than 100 percent. The market was changing so rapidly that it was difficult to anticipate renewal terms.

While the number of breaches continues to increase and take new shapes and the cost of cyber breaches also increases, the investment in cyber hygiene by insureds as well as modified underwriting standards seems to have made a positive impact on the direction of the cyber insurance industry.

For example, Microsoft found that the implementation of Multifactor Authentication "reduces the risk of compromise by 99.22 percent across the entire population and by 98.56 percent in cases of leaked credentials."[27]

In 2022, there was a slowdown in cyber claims frequency and severity.[28] Loss ratios declined in 2022 to 43 percent and average renewal pricing was down considerably to 15 percent at the end of 2022.[29] John Hennessy, Regional Vice President, Underwriting at Cowbell commented that they have identified the most important risk controls to have in place today, and the brevity of their application is reflective of this.

As a result, in 2023 the cyber market softened considerably in response to the lull of attacks in 2022. Whitmill noted that in 2023 insureds were able to double their coverage limits without a change in premium and if the insured received a large increase, marketing the coverage for alternative options was a must.

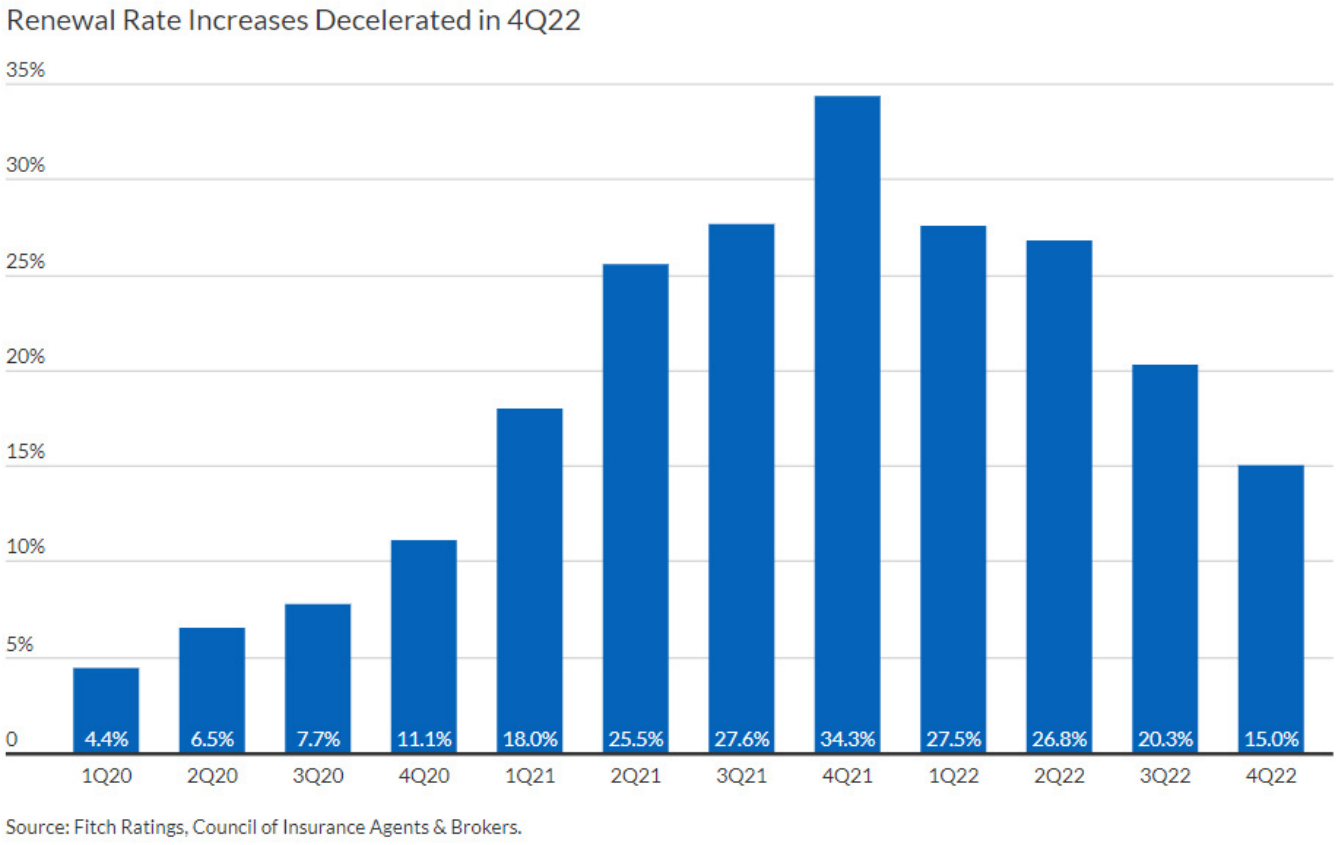


Figure 4. Cyber Insurance Renewal Premium Rates QoQ Change[30]

Anecdotal examples of this in transit abound. For example, after experiencing a significant year-over-year cyber insurance increase and cuts to policy limits in 2023, the Rock Island County Metro Mass Transit District was able to double their limits and reduce annual premiums. Similarly, the Washington State Transit Insurance Pool (WSTIP) reported a 0 percent change in cyber premiums from 2022 to 2023.

Based on the studies cited above and our interview, it appears that this apparent reprieve might be short lived. A leading cybersecurity incident response service stated that:

> Yes, there was a slowdown in the number of attacks at the beginning of the year [2023], but this was the result of the cyber criminals recalibrating their attack tools in response the actions being taken to defend against attacks. They are now using machine learning and artificial intelligence to work around multifactor authentication and endpoint detection and response. In the last half of the year [2023], the number of incidents that I have had to respond to has been climbing.[31]

This observation is supported by a recent study by Armis entitled *Anatomy of Cybersecurity: A Dissection of the 2023 Threat* Landscape that saw a 104 percent increase year-over-year in 2023.[32] Clearly, the market is continuing to evolve as organizations react to an ever-changing threat landscape. Unfortunately, the industry seems to be in a vicious cycle where as soon as an organization adapts to the latest type of cybersecurity threat, the cyber criminals evolve accordingly. While this cycle plays out, the insurance market will remain in a somewhat reactionary mode.

Responding to the Changing Threat Environment

> "There is nothing like experiencing a cybersecurity breach to incentivize you to get your cybersecurity house in order. We suffered a breach three years ago and had to rebuild our IT systems, move storage to the cloud, segregate our networks, and put the basic policies and procedures in place. Sometimes it feels like overkill, but the recovery costs were so high, and our cyber insurance coverage limited, that we could not risk being unprepared for another breach."

This anecdote, provided by another government contractor, represents a recurring theme in this research. The individual acknowledged that while the firm continues to face regular cybersecurity threats, she believes that if, and when, there is another attack, the company will be far less exposed and better able to recover quickly.

In the complex and changing cyber security insurance market, transit agencies are faced with making difficult decisions about how to protect themselves. Many have decided to scale back coverage, reduce their premiums, and/or obtain less coverage. Some have gone the route of creating insurance pools with many agencies buying into coverage that provides some level of help. A few have decided to self-insure, which means they conducted a financial analysis and concluded that the cost of recovering from a breach (and the frequency) is less expensive than the combined premiums would be. Still others forego cyber insurance entirely because they either don't understand the risks, don't believe they can afford the premiums, or don't think it will happen to them. Staff at one agency that experienced two significant events in the span of a year stated that they were not going to apply for cyber coverage until the following year when they had completed several of the recommendations coming out of a recent cybersecurity assessment. They stated that they didn't believe they could obtain coverage until they had taken action to shore up their risk profile.

One way transit agencies have worked to manage the cost of cyber insurance coverage is through insurance pools. One of the most sophisticated insurance pools is the Washington State Transit

Insurance Pool (WSTIP). WSTIP represents 25/26 transit agencies in the state of Washington. Around 2011, when WSTIP started including cyber insurance in its pool, the cost to the pool was approximately $8,000 for all 25 of its members and provided each member with $2M in cyber coverage. In its 2022 renewal, the cost of cyber insurance had increased year-over-year from $28,000 to about $50,000, with no change in coverages. While the increases have been significant, the cost of providing this level of coverage for 25 agencies is minimal. It is important to understand that WSTIP has been very vigilant about cybersecurity for the past 12 years because its Board understood the risks that cybersecurity posed and strongly urged WSITP to require cybersecurity hygiene of all its members. Since that time, WSTIP has provided cybersecurity training, best practices, and tools for its members.

Other transit risk pools have had varying levels of success. For example, the Iowa, Illinois, and Ohio insurance pools do not provide cybersecurity coverage to their members. This is because the agencies do not equally appreciate their cyber risk and consequently, the more risk averse agencies prefer to insure for cybersecurity independently and not further expose themselves to the additional risks associated with other agencies.

Recommendations

Although adjustments have been made, the cybersecurity insurance industry is still in the early stages of adapting to this rapidly changing environment. Swiss Re Institute estimates that only 55 percent of businesses carry cyber coverage,[33] and Fitch Ratings estimates that cyber insurance premiums in 2022 accounted for less than 1 percent of property and casualty premiums in the U.S.[34]

Set forth below are a series of recommendations that could continue to improve the cybersecurity posture for public transportation.

- **Public Transportation.** Those public transportation agencies that are not currently taking cybersecurity risks seriously must invest in understanding their exposure and take action to build more resilient cybersecurity programs. This means they must recognize cyber risk as part of their overall enterprise risk management. Doing so starts with basic actions that include conducting regular cyber assessments; maintaining an up-to-date cyber response plan; developing and following written policies and procedures on basic operations such as password protection, multifactor authentication, training, asset management, log maintenance, etc. These policies and procedures need to not only be written down but followed. Conducting regular penetration testing and/or ongoing threat assessments is also key. Many of these basic tasks are not expensive but require a commitment of time and attention from all levels within the agency.

  Funds and services are available to help. For example, most formula and discretionary grant programs allow funds to be spent on cybersecurity activities[35] and there are cybersecurity grant funds available for many agencies such as the TSA Transportation Security Grant program[36] and the Cybersecurity and Infrastructure Security Agency (CISA) State and Local Cybersecurity grant program.[37] State DOTs should consider providing training, cybersecurity assessments, and policy and procedure development help to the smaller

transit agencies that they typically oversee the funding of. This will go a long way towards accountability and help these agencies that may not have the funding and support to implement cybersecurity hygiene.

There are also several free services provided such as the FTA Cyber Assessment Tool for Transit (CATT),[38] the National Institute of Standards and Technology (NIST) Cybersecurity Framework and its guidelines and best practices,[39] and the TSA Surface Transportation Cybersecurity Toolkit,[40] to name a few. These programs and others work to enhance cybersecurity and protect critical infrastructure. Public and private sector collaboration, information sharing, and cybersecurity best practices are crucial for defending against these threats.

States or small agencies that have not considered creating pooled fund insurance programs should consider this risk management tool. Those pooled fund insurance programs that do not include cyber insurance should seek help from an existing pool, broker, or insurer to help their members get to a stage of cybersecurity maturity that would make sense to collectively seek this coverage and better spread their risk and mitigate the volatility of premiums.

- **Cybersecurity Insurance Industry.** The cyber insurance industry should continue to work towards establishing consistent, understandable, and affordable cybersecurity insurance products. While consistency of policy language, definitions, and terminology has improved greatly over the past few years, inconsistencies across applications and policies remain that can lead to confusion with insureds. Insureds comment that application questions are not always applicable or are confusing and difficult to answer. If questions can be simplified in a manner that still provides the desired information, policyholders' concern that they might not be answering accurately, or that their answer would be held against them in the event of a claim, would be mitigated. Also, variations in coverages and nuances with each policy can be difficult to identify and compare. It is imperative to work with a broker that understands the product to be able to accurately evaluate and advise on variations between applications and policies.

  Cyber insurers, brokers, and insureds should also continue to develop their relationships into a more collaborative partnership. Cyber insurance brokers will often require that an insured complete a cyber assessment and adopt basic cybersecurity practices such as the adoption of multi-factor authentication or training before shopping applications to cyber insurers. Cyber insurers offer incentive programs, cybersecurity tools and resources, and even provide funding towards cybersecurity mitigation that go unused by policyholders. A more collaborative partnership between the insured and insurer would increase utilization of cyber resources offered, reduce unnecessary duplications, and allow cyber loss control engineers to identify solutions, which can subsequently bolster cyber resiliency and reduce claims.

- **Administration.** As described above, the Federal Government has made significant progress supporting public agencies in meeting their cybersecurity obligations. In addition to providing funding availability through existing formula and new discretionary grant programs, the U.S. Department of Transportation is now requiring all new discretionary grant programs include the following language:

> It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats, consistent with Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience and the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. Each applicant selected for Federal funding under this notice must demonstrate, prior to the signing of the grant agreement, effort to consider and address physical and cybersecurity risks relevant to the transportation mode and type and scale of the project. Projects that have not appropriately considered and addressed physical and cybersecurity and resilience in their planning, design, and project oversight, as determined by the Department and the Department of Homeland Security, will be required to do so before receiving funds or will be required to complete related actions as part of the project. [41]

This requirement is a great step in the right direction. Imposing a similar requirement on formula grant programs would encourage smaller agencies that don't generally apply for discretionary grant programs to adopt cybersecurity programs. These requirements also need to be communicated to the agencies that are receiving the grants. Many transit agencies applying for discretionary grant programs are not aware of this new requirement.

The Federal Transit Administration intends to take another important step by including similar cybersecurity language in the updated triennial audit manual. Once this document is released, the cybersecurity requirements that transit agencies will be audited against can be communicated. This will be another forcing function for those agencies that need prodding.

Finally, the Federal Government's Cybersecurity Strategic Plan discusses the possibility of establishing a backstop for cybersecurity insurance.[42] Doing so would go a long way towards calming the cybersecurity insurance market, attracting additional providers and potentially driving down costs for operators.

Endnotes

1. BlackFog, "The State of Ransomware 2023 Annual Report," January 2024, https://www.blackfog.com/2023-ransomware-attack-report/ (accessed February 13, 2024)

2. Kartikay Mehrota, William Turton, "CNA Financial Paid $40 Million in Ransom After March Cyberattack, Bloomberg, March 20, 2021. https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack?embedded-checkout=true (accessed February 2, 2024)

3. Joe Panettieri, "Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recover Details" MSSP Alert, May 9, 2021, https://www.msspalert.com/news/colonial-pipeline-investigation (accessed February 2, 2024)

4. Kyle Alspach, "10 Major Cyberattacks and Data Breaches in 2023," CRN, December 13, 2023, https://www.crn.com/news/security/10-major-cyberattacks-and-data-breaches-in-2023?page=5&itc=refresh (accessed February 12, 2024)

5. SBIR-STTR America's Seed Fund Powered by SBA, Course 10, Tutorial 1, The Impact of Cybersecurity on Small Business, 1, https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial1.pdf (accessed April 2, 2024)

6. Net Diligence, Cyber Claims Study 2023 Report, 2, https://netdiligence.com/cyber-claims-study-2023-report-thank-you/?submissionGuid=6de16f6f-cc09-490a-9d80-fcf7e1e25622

7. CISA, "Critical Infrastructure Security and Resilience" https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector (accessed February 2, 2024)

8. Checkpoint "Ransomware Attacks Continue to Surge, Hitting a 93% Increase Year over Year" June 14, 2021, https://blog.checkpoint.com/security/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year/ (accessed February 2, 2024)

9. Scott Belcher, Terri Belcher, Eric Greenwald, Brandon Thomas, "Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness" Mineta Transportation Institute, DOI 10.31979/mti.2020.1939, September 2020, 63, https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness

10. Ibid 15 – the original source material is no longer accessible

11. Scott Belcher, Terri Belcher, Kathryn Seckman, Brandon Thomas, Homayun Yaqub, "Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges," 19, Mineta Transportation Institute, DOI: 10.31979/mti.2022.2113, July 2022 "https://transweb.sjsu.edu/research/2113-Cybersecurity-Ransomware-Public-Transit

12. Carrier Chronicles, "The Past, Present and Future of Cyber Liability Insurance," February 24,

2023, 3, https://carrierchronicles.com/the-past-present-and-future-of-cyber-liability-insurance/ (accessed February 7, 2024)

13. Interpol, "Interpol Report Showing Alarming Rate of Internet Attacks in 2020," August 4, 2020, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (accessed February 20, 2024)

14. Net Diligence, Cyber Claims Study 2023 Report, 2023, 1, https://netdiligence.com/cyber-claims-study-2023-report-thank-you/?submissionGuid=6de16f6f-cc09-490a-9d80-fcf7e1e25622

15. Fitch Ratings "U.S. Cyber Insurance Payouts Increase Amid Rising Claims, Premium Hikes, May 6, 2022 https://www.fitchratings.com/research/insurance/us-cyber-insurance-payouts-increase-amid-rising-claims-premium-hikes-06-05-2022 (accessed October 24, 2023)

16. Fitch Ratings "U.S. Cyber Insurance Payouts Increase Amid Rising Claims, Premium Hikes," May 6, 2022 https://www.fitchratings.com/research/insurance/us-cyber-insurance-payouts-increase-amid-rising-claims-premium-hikes-06-05-2022 (accessed October 24, 2023)

17. Fitch Ratings" U.S. Cyber Insurers See Favorable Premium Growth, Results in 2023," April 13, 2023, 2, https://www.fitchratings.com/research/insurance/us-cyber-insurers-see-favorable-premium-growth-results-in-2023-13-04-2023 (accessed October 24, 2023)

18. IBM, "Cost of a Data Breach Report 2023," 10, https://www.ibm.com/reports/data-breach

19. Ibid 5

20. Ibid 72

21. Chainalysis, "Ransomware Payment Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," February 7, 2024, https://www.chainalysis.com/blog/ransomware-2024/ (accessed February 11, 2024)

22. Net Diligence Cyber Claims Study 2023 Report, 2023, 3, https://netdiligence.com/cyber-claims-study-2023-report-thank-you/?submissionGuid=6de16f6f-cc09-490a-9d80-fcf7e1e25622

23. Ibid

24. Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones, "Content analysis of cyber insurance policies: how do carriers price cyber risk?" Journal of Cybersecurity, 2019, 1-19, 12, Doi: 10.1093/cybsec/tyz002 https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419?login=false

25. Author Interviews - CRC broker, Candace Funsch 10/30/23

26. Swiss Re Institute, "Cyber Insurance: strengthening resilience for the digital transformation" November 2022, 23, https://www.swissre.com/institute/research/topics-and-risk-dialogues/digital-business-model-and-cyber-risk/cyber-insurance-strengthening-resilience.html

27. Lucas A. Meyer, Sergio Romero, Gabriele Bertoli, Tom Burt Alex Weinert, Juan M. Lavista Ferres, How Effective is Multifactor Authentication at Detering Cyberattacks? May 1, 2023, 4 (accessed February 13, 2024) https://arxiv.org/pdf/2305.00945.pdf

28. Coalition, "2023 Cyber Claims Report Mid-year Update," 2023, 5, https://info.coalitioninc.com/download-2023-cyber-claims-report-mid-year-update.html (accessed October 24, 2023)

29. Fitch Ratings, "U.S. Cyber Insurers See Favorable Premium Growth, Results in 2023," April 13, 2023, 2, https://www.fitchratings.com/research/insurance/us-cyber-insurers-see-favorable-premium-growth-results-in-2023-13-04-2023 (accessed October 24, 2023)

30. Fitch Ratings, "U.S. Cyber Insurers See Favorable Premium Growth, Results in 2023," April 13, 2023, 3 https://www.fitchratings.com/research/insurance/us-cyber-insurers-see-favorable-premium-growth-results-in-2023-13-04-2023 (accessed October 24, 2023)

31. Author Interview, Leading Industry Cybersecurity Response Provider

32. Armis, "Anatomy of Cybersecurity: A Dissection of the 2023 Threat Landscape, https://www.armis.com/anatomy-of-cybersecurity

33. Swiss Re Institute, "Cyber Insurance: strengthening resilience for the digital transformation" November 2022, 2, https://www.swissre.com/institute/research/topics-and-risk-dialogues/digital-business-model-and-cyber-risk/cyber-insurance-strengthening-resilience.html

34. Fitch Ratings, "US Cyber Insurance Sharp Price Increases, Profit Improvement to Moderate," May 12, 2023, 1, https://www.fitchratings.com/research/insurance/us-cyber-insurance-sharp-price-increases-profit-improvement-to-moderate-12-05-2023 (accessed October 24, 2023)

35. FTA "Cybersecurity Resources for Transit Agencies," https://www.transit.dot.gov/regulations-and-programs/safety/cybersecurity-resources-transit-agencies (accessed February 2, 2024)

36. FEMA "Transit Security Grant Program," https://www.fema.gov/grants/preparedness/transit-security (accessed February 2, 20224)

37. CISA "State and Local Cybersecurity Grant Program" https://www.cisa.gov/state-and-local-cybersecurity-grant-program (accessed February 2, 2024)

38. FTA "Cybersecurity Assessment Tool for Transit (CATT)" https://www.transit.dot.gov/research-innovation/cybersecurity-assessment-tool-transit-catt (accessed February 2, 2024)

39. NIST "Cybersecurity Framework" https://www.nist.gov/cyberframework (accessed February 2, 2024)

40. TSA "Surface Transportation Cybersecurity Toolkit," https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit (accessed February 2, 2024)

41. FY23 SMART Stage 1 Notice of Funding Opportunity (NOFO), page 30, August 25, 2023, https://

www.transportation.gov/grants/smart/fy23-smart-stage-1-notice-funding-opportunity-nofo See also National Cybersecurity Strategy, March 2023, Strategic Objective 3.4: Use Federal Grants and Other Incentives to Build in Security, 21, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

42. National Cybersecurity Strategy March 2023, Strategic Objective 3.6: explore a federal cyber insurance backstop, 26, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Acknowledgement

The authors thank Lisa Rose, for editorial services, as well as MTI staff, including Executive Director Karen Philbrick, PhD; Deputy Executive Director Hilary Nixon, PhD; Director of Operations Alverina Eka Weinardy, and Graphic Design Assistant Minhvy Tran.

About the Authors

Scott Belcher is a Mineta Transportation Institute Research Associate; Co-Founder of Cybrbase, LLC; and the Chief Executive of SFB Consulting, LLC.

Todd Chollet is a Risk Advisor and Cyber Practice Leader at Sunstar Insurance Group.

This report can be accessed at transweb.sjsu.edu/research/2406

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.