



Board Report

File #: 2023-0384, File Type: Program

Agenda Number: 5.

FINANCE, BUDGET, AND AUDIT COMMITTEE JULY 19, 2023

SUBJECT: CYBERSECURITY LIABILITY INSURANCE PROGRAM

ACTION: APPROVE RECOMMENDATION

RECOMMENDATION

AUTHORIZE the Chief Executive Officer to negotiate and purchase a cybersecurity liability insurance policy with up to \$50 million in limits at a cost not to exceed \$4 million for the 12-month period effective September 1, 2023, to September 1, 2024.

ISSUE

Metro's cybersecurity liability insurance policy expires on September 1, 2023. Insurance underwriters will not commit to final pricing until three weeks before the current program expires. Consequently, staff requests a not-to-exceed amount for this renewal pending final pricing. Metro purchases an insurance policy to cover cybersecurity liability exposures. Cybersecurity is the practice of being protected against criminal or unauthorized use of systems and electronic data. These exposures include but are not limited to:

- Unavailability of IT systems and networks
- Physical asset damage and associated loss of use
- Loss or deletion of data
- Data corruption or loss of data integrity
- Data breach leading to compromise of third-party confidential/personal data
- Cyber espionage resulting in the release of confidential/sensitive information
- Extortion demands to cease a cyber-attack
- Direct financial loss due to theft
- Damage to reputation
- Bodily injury/property damage to third parties

Without this insurance, Metro is subject to unlimited liability for claims resulting from a cyber-attack or data breach event.

BACKGROUND

FY23 was the first year Metro purchased cybersecurity liability coverage for \$2,663,634.73. For the

first renewal, Metro's insurance broker, USI Insurance Services ("USI"), was requested to market Metro's cybersecurity liability insurance program to qualified insurance carriers. Through its partnership with Howden, a London broker, USI has received quotes from the incumbent carrier, which has A.M. Best ratings indicative of acceptable financial soundness and ability to pay claims. The premium indications below are based on current market expectations. The quotes expire on September 1, 2023.

USI provides a not-to-exceed number that serves three functions. First, the number provides an amount to cover the recommended premium and contingency that Risk Management can bring to the CEO and Board to obtain approval for the binding of the program. Second, the number allows our broker ample time to continue negotiating with underwriters to ensure Metro obtains the most competitive pricing. And third, the not-to-exceed amount allows Metro to secure the quoted premium during the board cycle process prior to quote expiration.

DISCUSSION

Public entities are increasingly coming under cyber-attacks. A robust cybersecurity insurance program could help reduce the number of successful cyber-attacks and financial risks associated with doing business online by 1) promoting the adoption of preventative measures in return for more coverage; and 2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection.

The cyber insurance market has matured somewhat with increased discipline in underwriting and reduced deployment of capacity where controls and security protocols are perceived to be ineffective at adapting to security threats. Those that have implemented stronger cybersecurity measures will see a more mature market with softer price hikes for those clients that can demonstrate strong protocols throughout their systems.

There have been changes in the regulatory environment around cybersecurity, specifically for public transit organizations. In February of 2023, the Federal Transit Administration published a cybersecurity assessment tool for transit agencies to help guide them in identifying and mitigating risk. FTA continues to guide cybersecurity activities and supports the U.S. Department of Homeland Security (DHS) in promoting enhanced security for transit agencies. Additionally, as a condition under 49 U.S.C. 5323(v), rail transit operators must certify that they have a process to develop, maintain, and execute a plan for identifying and reducing cybersecurity risks. The general guidance is built around the National Institute of Standards and Technology (NIST) Cyber Security Framework. With Metro's vast network of third-party service providers, this is a major exposure area that needs to be continually monitored on an ongoing basis.

Multiple questionnaires and interviews are required by Metro's information security and Supervisory Control and Data Acquisition (SCADA) team's experts on the systems and network controls. A proposal of coverage for cybersecurity liability insurance based on the findings and the insurance carrier's knowledge of Metro's internal controls is provided. The proposed program, from carrier BRIT Re, a Lloyds of London consortium, provides up to \$50 million in excess coverage on a claims-made basis with a \$10 million self-insured retention (SIR). Attachment A summarizes the premium options, and Attachment B summarizes the coverages. Risk Management and Information Technology

Services (ITS) team members reviewed the proposal and agree that the proposed coverage will help mitigate Metro's financial and reputational risks should the agency experience a cyber-attack event.

DETERMINATION OF SAFETY IMPACT

Approval of this recommendation to purchase a cybersecurity liability insurance policy will not directly impact the safety of Metro's patrons or employees. The policy will limit Metro's liability for claims resulting from a cyber-attack or data breach event. Additionally, the policy will aid in Metro's recovery and moderate financial losses as well as harm to Metro's reputation resulting from cyber events and incidents.

FINANCIAL IMPACT

Funding for ten months, or \$3,333,333, for this action is included in the FY24 Budget in cost center 0531, Risk Management -- Non-Departmental Costs, under projects 100001 - General Overhead, 300022 - Rail Operations - Blue Line, 300033 - Rail Operations - Green Line, 300044 - Rail Operations - Red Line, 300066 - Rail Operations - Expo Line, 300077 - Crenshaw Line, 301012 - Metro Orange Line, 306001 - Operations Transportation, 306002 - Operations Maintenance, 320011 - Union Station and 610061 - Owned Property in account 50699 (Ins Prem For Other Ins). Additional funding to cover premium costs beyond FY24 budgeted amounts will be addressed by fund reallocations during the year.

The remaining two months of premium will be requested during the FY25 Budget development cycle, cost center 0531, Risk Management -- Non-Departmental Costs, under projects 100001 - General Overhead, 300022 - Rail Operations - Blue Line, 300033 - Rail Operations - Green Line, 300044 - Rail Operations - Red Line, 300066 - Rail Operations - Expo Line, 300077 - Crenshaw Line, 301012 - Metro Orange Line, 306001 - Operations Transportation, 306002 - Operations Maintenance, 320011 - Union Station and 610061 - Owned Property in account 50699 (Ins Prem For Other Ins).

Impact to Budget

The current fiscal year funding for this action will come from the Enterprise, General, and Internal Service funds, paralleling funding for the actual benefiting projects charged. These funds are eligible for bus and rail operating and capital expenses.

EQUITY PLATFORM

The proposed action supports Metro's ability to safely serve the communities and customers who rely on Metro's transportation services and assets by providing insurance coverage that will allow Metro to more quickly resume operations in the event of a cybersecurity breach.

IMPLEMENTATION OF STRATEGIC PLAN GOALS

The recommendation supports strategic plan goal # 5 "Provide responsive, accountable, and trustworthy governance within the LA Metro organization." The responsible administration of Metro's risk management programs includes the use of insurance to mitigate large financial risks resulting

from cybersecurity events.

ALTERNATIVES CONSIDERED

Various limits of coverage were considered, as outlined in Attachment A for the cybersecurity liability insurance program. All options include a SIR of \$10 million for the same program. Option A, Metro's current limit, provides \$50 million in coverage, Option B provides \$75 million, and Option C provides \$100 million in coverage.

Option A is recommended as the best value option while retaining a reasonable amount of risk over the coverage limit.

NEXT STEPS

Upon Board approval of this action, staff will advise USI to proceed with the placement of the cybersecurity liability insurance program outlined herein, effective September 1, 2023.

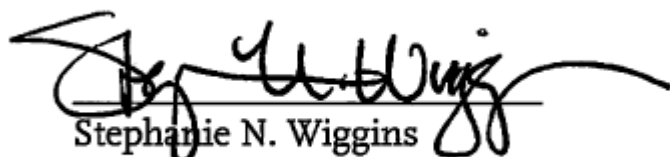
ATTACHMENTS

Attachment A - Coverage Options and Premiums

Attachment B - Coverage Description

Prepared by: Claudia Castillo del Muro, Executive Officer, Risk Management, (213) 922-4518
Kenneth Hernandez, Deputy Chief Risk, Safety, and Asset Management Officer, (213) 922-2990
Bryan Sastokas, Deputy Chief Information Technology Officer, (213) 922-5510

Reviewed by: Gina L. Osborn, Chief Safety Officer, (213) 922-3055


Stephanie N. Wiggins
Chief Executive Officer

Coverage Options and Premiums

Carrier: BRIT Re

Cyber Security Insurance Program Premium and Proposed Options

	CURRENT PROGRAM	OPTIONS		
		A	B	C
Self-Insured Retention (SIR)	\$10M	\$10 mil	\$10 mil	\$10 mil
Limit of Coverage	\$50	\$50 mil	\$75 mil	\$100 mil
Premium *	\$2,663,635	\$4,000,000	\$6,100,000	\$7,600,000

Not to Exceed	\$4,000,000	\$6,100,000	\$7,600,000
Premium per mil coverage \$53,273	\$80,000	\$81,333	\$76,000

* Includes commissions, taxes and fees.

Coverage Description

USI provided a proposal of coverage for cyber liability insurance. The following summarizes the coverages and exclusions:

Included Coverage

Exposure	Brief Description
SECURITY AND PRIVACY LIABILITY (INCLUDING EMPLOYEE PRIVACY)	Covers the insured's liability for damages resulting from a data breach. Such liability most often results from (1) loss, theft, or unauthorized disclosure of personally identifiable information (PII) in the insured's care, custody, and control; (2) damage to data stored in the insured's computer systems belonging to a third party; (3) transmission of malicious code or denial of service to a third party's computer system; (4) failure to timely disclose a data breach; (5) failure of the insured to comply with its own privacy policy prohibiting disclosure or sharing of PII; and (6) failure to administer an identity theft program required by governmental regulation or to take necessary actions to prevent identity theft. In addition, this insuring agreement covers the cost of defending claims associated with each of these circumstances
SECURITY BREACH RESPONSE COVERAGE	Coverage for the expenses involved in responding to a data breach. These include legal expenses, forensic experts, costs to notify affected parties and provide credit monitoring, and public relations expenses to mitigate reputational damage.
PRIVACY REGULATORY CLAIMS COVERAGE	The insuring agreement covers the costs of dealing with state and federal regulatory agencies (which oversee data breach laws and regulations), including (1) the costs of hiring attorneys to consult with regulators during investigations and (2) the payment of regulatory fines and penalties that are levied against the insured (as a result of the breach).
PCI-DSS ASSESSMENT COVERAGE	Payment Card Industry Data Security Standard (PCI DSS) was formed around 2004 by the major credit card companies to establish guidelines in the handling and processing of transactions including personal information. The policy will provide coverage for assessments, fines or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry

	Data Security Standard (PCI DSS) or payment card company rules.
CYBER EXTORTION COVERAGE	Cyber extortion is an online crime in which hackers hold your data, website, computer systems, or other sensitive information hostage until you meet their demands for payment. The policy will cover the cost to investigate a ransomware attack and negotiate with the hackers.
MULTIMEDIA LIABILITY	Multimedia Liability provides coverage for third-party liability claims alleging damage resulting from dissemination of media material. This covers both electronic and non-electronic media material and may include claims of copyright or trademark infringement. libel.
DIGITAL ASSET RESTORATION COSTS	Digital assets loss occurs when company data or software is corrupted or destroyed because of a network security failure. This type of loss can come because of an outside network breach or an inside job carried out by an employee. The policy covers the reasonable and necessary cost to replace, restore or re-collect digital property from written or electronic records. Additionally, investigation expenses such as disaster recovery and computer forensics is also covered.
BUSINESS INCOME LOSS RESULTING FROM A NETWORK DISRUPTION	Business Interruption covers business income loss and extra expenses incurred during a computer network outage. The coverage applies to outages of <i>internally managed IT</i> , such as employee devices or internal networks or databases -- not a cloud computing provider or other type of third-party IT vendor.
Bodily Injury	Injury to persons (including death)

Excluded Coverage

The proposal of coverage also indicates various exclusions or exposures that will not be covered:

Exposure	Brief Description
BUSINESS INCOME LOSS (Physical Damage)	Some insurers have brought forward business interruption coverage as part of cyber insurance or as stand-alone business interruption insurance policies. There doesn't have to be a complete shutdown to trigger the coverage. Instead, a system slowdown due to network issues or malicious elements can also be classified as a trigger.

	However, the proposal indicates there will be no coverage for physical damage BI claims.
ENSUING PROPERTY DAMAGE LOSS	Exception to an exclusion in a first-party property policy that applies in a special type of fact pattern where the damage caused by an excluded peril operates as a link in the "chain of events" that enables a covered peril to damage other property. (proximate cause) Symbolically, a classic ensuing loss fact pattern can be represented as follows: <i>excluded peril</i> → <i>excluded damage</i> → <i>covered peril</i> → <i>ensuing damage</i> . Note that there must be two kinds of damages—an initial loss and an ensuing loss. Most courts will not apply an ensuing loss provision if an excluded peril caused a covered peril that results in only one kind of damage.
Inspection and Loss Prevention/Mitigation Expense	Loss prevention aims to reduce the possibility of damage and lessen the severity if such a loss should occur.
Debris Removal	Debris removal insurance is a section of a property insurance policy that provides reimbursement for clean-up costs associated with damage to property.