



Board Report

File #: 2022-0454, File Type: Program

Agenda Number: 13.

FINANCE, BUDGET AND AUDIT COMMITTEE AUGUST 17, 2022

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 \$2.8 million for the 12-month period effective September 1, 2022 to September 1, 2023.

ISSUE

To date, Metro has not purchased an insurance policy to cover our 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 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

Metro's insurance broker, USI Insurance Services ("USI") was requested to market a cybersecurity liability insurance program to qualified insurance carriers. USI partnered with London broker Howden to develop the program of insurance. As a result, we received a quote from a carrier with 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 quoted price expires September 1, 2022.

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 new program. Second, the number allows our broker ample time to continue to negotiate with underwriters to ensure that Metro obtains the most competitive pricing available. 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.

Robert Rosenzweig, a national cyber practice leader for Risk Strategies stated during Advisen's virtual Cyber Risk Insights Conference last October, "Underwriters, unable to ignore increased claim frequency and severity, now need more information from buyers and have been more 'discerning' about where to deploy capital. More data and better correlation from threats to losses is making the difference." He commented, "Risk selection is paramount. It's tougher for insureds to get the capacity they need in the market. If controls aren't there, where you find yourself on the spectrum of average rate increases is going to fluctuate to the high end." At the same conference, Paul Needle, senior vice president of cyber treaty reinsurance at Munich Re concluded, "What the cyber market has going for it right now is a drastic increase in expertise for underwriting. We've come a long way in thinking critically about the controls an insured might have."

Multiple questionnaires and interviews were completed by Metro's information security and Supervisory Control And Data Acquisition (SCADA) team's experts on our systems and network controls. USI and Howden provided a proposal of coverage for cybersecurity liability insurance based on the findings and the insurance carrier's knowledge of Metro's internal controls. The proposed program from carrier BRIT Re, a Lloyds of London consortium, provides up to \$75 million in excess coverage on a claims-made basis with a \$10 million self-insured retention (deductible). Attachment A summarizes the premium options and Attachment B summarizes the coverages. The proposal was reviewed by Risk Management and Information Technology Services (ITS) team members who agree the proposed coverage will help mitigate Metro's financial and reputational risk should the agency experience a cyber-attack event.

According to a report published by S&P Global Ratings in September 2021, "The pandemic caused economic and insured losses from cyber-attacks to skyrocket, which has heightened awareness of the risk and increased demand for cyber insurance. 'Prices in the cyber insurance market could therefore rise sharply over 2021-2023, even doubling in some cases,'" said S&P Global Ratings credit analyst Manuel Adam. "The market faces increasing demand, but limited supply. In our opinion, lack of capacity could be holding back the development of a sustainable cyber insurance

market.” We appreciate the hard work of our Metro team and broker to present this insurance program in a difficult and demanding insurance market.

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 aide 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 of \$2 million for this action is included in the FY23 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, 300055 Gold Line, 300066 Rail Operation - Expo 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 of \$237,000 required to cover premium costs beyond FY23 budgeted amounts will be addressed by fund reallocations during the year.

The remaining two months of premiums will be requested during the FY24 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, 300055 Gold Line, 300066 Rail Operation - Expo 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. This activity will result in an increase in operating costs from the prior fiscal year.

EQUITY PLATFORM

There are no equity impacts anticipated as a result of this action.

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

The Board may choose to continue the past practice of not covering cybersecurity liability risks through an insurance policy. This alternative is not recommended as it can expose Metro to unlimited liability costs for claims resulting from a cybersecurity incident.

Various limits of coverage were considered as outlined in Attachment A for the cybersecurity liability program of insurance. All options include a deductible of \$10 million for the same program. Option A provides \$25 million in coverage, Option B provides \$50 million, and Option C provides \$75 million in coverage.

Option B is recommended as the best value option while retaining a reasonable amount of risk over the coverage limit. Option A, with a premium within the adopted FY23 budget, is not recommended since the double amount of coverage afforded by Option B is more cost effective. Option C is not recommended since the additional premium outweighs the benefit of additional coverage.

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, 2022.

ATTACHMENTS

Attachment A - Coverage Options and Premiums

Attachment B - Coverage Description

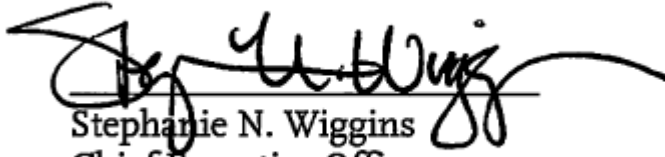
Prepared by: Tim Rosevear, Manager, Risk Financing, (213) 922-6354

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

Robert Bonner, Chief People Officer, (213) 922-3048



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)	Unlimited	\$10 mil	\$10 mil	\$10 mil
Limit of Coverage	None	\$25 mil	\$50 mil	\$75 mil
Premium *		\$1,876,357	\$2,663,635	\$3,431,918
Contingency **		\$123,643	\$136,365	\$68,082
Not to Exceed		\$2,000,000	\$2,800,000	\$3,500,000
Premium per million coverage		\$75,054	\$53,273	\$45,759

* Includes commissions, taxes and fees.

** For carrier and premium adjustments, tax 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.