FINANCE COMMITTEE REPORT

Report Date	March 24, 2021
Meeting Date	March 31, 2021
Service Area	Strategic Services

Chairman Councillor Merrithew and Members of Finance Committee

SUBJECT: **Cyberattack – Restoration Costs and Projected Recovery Estimate**

OPEN OR CLOSED SESSION

This matter is to be discussed in Finance Committee Open Session.

AUTHORIZATION

Primary Author	Commissioner/Dept. Head	City Manager
Stephanie Rackley-Roach	***Kevin Fudge***	***John Collin***

RECOMMENDATION

The City Manager recommends the Finance Committee:

a) Acknowledge Information Technology ("IT") infrastructure and services procured for response and rebuild of the IT network due to the cyberattack is authorized under the emergency clauses in the Saint John Procurement Act; and

b) Receive and file this report.

EXECUTIVE SUMMARY

On November 13, 2020, the City of Saint John experienced a cyberattack. The scope of the attack was wide-reaching with significant damage caused to the City's IT infrastructure. The need to shut down the network and preserve the compromised environment for forensic investigation impacted business continuity with no ability to reuse the existing information technology equipment. Therefore, consulting and hardware requirements for event management and recovery were acquired under the emergency provisions in the City's Procurement Policy and other related legislation.

The main consulting vendors were engaged through External Counsel approved by the City's Insurer. All major components for the network rebuild were purchased under the emergency provisions. The total projected cost for consulting services, network hardware, licenses and support, vendor and hardware for application restorations, and other costs related to the recovery effort is $2,950,409 plus HST. While the new network is almost complete, there is considerable work remaining for the restoration of all the applications used to deliver efficient public service. Some costs are estimated and will be finalized as more work is completed.

The City has both a property and cyber insurance policy. It is estimated by staff that at least 85% of the recovery costs will be submitted to the Insurer under these two policies.

The amount recoverable will be determined by the Insurer upon receipt of the City's claim. The City is still within the timeframe to finalize the claim and will monitor requirements closely to ensure timelines are met to recover costs. Costs not covered by insurance will be covered by the operating budget or the appropriate reserve fund. Renewal and enhancements of information technology requirements are funded out of the IT reserve, with projects planned and presented within the capital budget annually.

PREVIOUS RESOLUTION

N/A

STRATEGIC ALIGNMENT

Providing an update on the financial and service impacts of the cyberattack recovery efforts supports Common Council's priority of being fiscally responsible. It ensures accountability and transparency to the taxpayers.

REPORT

On November 13, 2020, the City of Saint John experienced a significant ransomware cyberattack. While City staff supported by a third-party vendor worked diligently to shut down the network immediately to mitigate risk, the City's network infrastructure and information systems sustained significant damage. Significant emergency investments were required to recover from the cyberattack.

The City has cyber insurance through AIG for these types of malicious attacks. The City was advised by the Insurer to retain External Counsel. Through External Counsel, Blake, Cassels & Graydon LLP (Blakes) and later Norton Rose Fulbright (Norton Rose) several third-party consultants were engaged to support the City in containment, forensic, and recovery efforts. In the interest of time under the emergency provisions in the Procurement Act, these engagements were approved through the Insurer and signed-off by the City Manager. Formal engagements through External Counsel included the following, with initial cost estimates outlined in Table 1. Agreements with Blakes/Norton Rose for external counsel and Redbrick Communications for public relations support were also executed. The statements of work outlined for these engagements did not include a total estimate. However, as services were required, the estimated costs are outlined in the financial section of the report.

Table 1: Consultants engaged and retained under External Counsel

Consultant	**Role**	**Statement of Work**
FireEye Mandiant (Mandiant)	Forensic Investigation	$162,000 USD + Report TBD + applicable tax
Bulletproof Solutions ULC (Bulletproof)	Containment and Recovery	$489,250 CAD + HST
CYPFER	Ransomware Recovery & Payment Facilitation	$10,250 + applicable tax

The scope of the cyberattack to the City's network, including both the City and Police domains, was wide reaching. It involved encryption to most Windows-based servers and many system endpoints (i.e., laptops and computers). Given the damage to the City's information technology infrastructure, recovery needed to start immediately to ensure continuity in the delivery of critical public services.

The creation of a temporary network required the City to look at building with new hardware for several reasons:

- Requirement to preserve the environment for the forensic investigation.
- Requirement to preserve the environment for the criminal investigation.
- Risk in restoring the City's compromised hardware with the potential that remnants of the malware may continue to reside in the compromised environment and lead to potential reinfection.

With existing hardware not available for immediate rebuild of the network, the City worked through Bulletproof to procure the necessary components. This was based on understanding City and Police infrastructure requirements and designing a system that would meet these needs in the short term. The replacement of network hardware has been right-sized and is scalable for future growth if needed.

The Enterprise Agreement approved by Common Council on April 6, 2020 for Microsoft Office 365 and the estimated percentage of recoverable data from the City's backup systems allowed for the immediate start of the restoration of the City's network.

Costs associated with Bulletproof consulting fees and hardware purchases for the network and backup systems are outlined in the financial section of this report. This includes an estimate of the requirement to procure additional security for the City's network that will be incorporated into the City's Microsoft Enterprise Agreement in the second year of renewal April 1, 2021.

As the City works to restore applications used to deliver services to the public, several additional costs have been projected. While it is critical to get these applications operational as soon as possible, the acquisition of goods and services required for restoration are no longer considered an emergency. For the most part, supply and service agreements have and will be used to ensure timely restoration.

Procurement Policy and Agreements

In order to restore critical public services and facilitate the network rebuild there have been several purchases made under specific provisions in several procurement policies and agreements.

The cyberattack, for the purposes of procurement will be considered as one event and all costs associated with getting a new network in operation will be associated with this event. Under section 5.12 Special Circumstances (Emergency) Purchases, of the City of Saint John Procurement Policy, permits the City to follow a non-competitive bid process to remedy an urgent situation. According to section 5.12(e), the relevant details shall be included in a report submitted to Council at the earliest possible opportunity following the special circumstances.

Section 153.1(e) of the General Procurement Act of New Brunswick also allows the direct purchase of "goods and services that are strictly necessary and, for reasons of urgency brought about by an event unforeseeable by the following entities, cannot be obtained in a timely manner through an open competitive bidding process."

Similarly, Article 19.12(d) of the Comprehensive Economic and Trade Agreement of Canada (CETA) and Article 513(d) of the Canadian Free Trade Agreement (CFTA) allows for limited tendering "if strictly necessary, and for reasons of urgency brought about by events unforeseeable by the procuring entity, the goods and services could not be obtained in time using opening tendering." Limited tendering "means a procurement method whereby the procuring entity contacts a supplier or suppliers of its choice." Furthermore, Article 513.1(i) states that limited tendering is also allowed "if goods or consulting services regarding matters of a confidential or privileged nature are to be purchased and the disclosure of those matters through an open tendering process could reasonably be expected to compromise government confidentiality, result in the waiver of privilege, cause economic disruption, or otherwise be contrary to the public interest." In this case, releasing any information by way of public tender would not be in the best interest of the City or the public given the unlawful nature of the event at hand.

Insurance

The City has two separate insurance policies that give rise to coverage for events such as the cyberattack: property policy and cyber policy.

Cyber Policy

The City's cyber policy is with AIG, one of the world's leading insurance companies for cyber insurance. There are five (5) sub-limits, two (2) are for third-party liability coverage (protection from liability from damages to others) and three (3) are first-party sub-limits (coverage for our own expenses and damages). There is one deductible ($50,000) that applies to an occurrence regardless of which sub-limits are used, and there is one overall limit ($2,000,000) that applies as well.

The two (2) third party sub-limits are for Security and Privacy Liability and Regulatory Action Liability. The three (3) relevant first party sections are:

- **Cyber Extortion** – Monies paid by an Insured, with the Insurer's consent to end a security or privacy threat that would otherwise cause harm to an Insured and the cost to investigate such a threat.

- **Event Management** – Reasonable and necessary expenses incurred within one year of a security or privacy event to conduct investigations (including forensic), crisis management, notification and education services, insurer services, and/or data restoration.

- **Network interruption** – Cost from the time of interruption until the 120th day after the interruption that would not have been incurred but for the interruption.

Property Policy

Within the City's property policy with AIG there is coverage for damage to our computer systems. This includes replacement of hardware and the cost to restore the data with a limit of $6 Million. The deductible is $1,000. No exclusions apply.

The policies have separate coverages; however, the Cyber policy can "stack" upon the property policy. In this case, the property coverage would respond first to the property damage (hardware) and data recovery. The cyber policy would cover any excess over this property policy, also bringing in those other coverages such as the cost of extortion, event management, and service interruption.

The determination as to what the Insurer deems as recoverable will not be confirmed or finalized until the City submits the final claim. The City is still within the timeframe to submit the Proof of Loss and will monitor requirements to ensure timelines are met to recover costs.

SERVICE AND FINANCIAL OUTCOMES

Since the cyberattack on November 13, 2020, the City with the support third party vendors has made tremendous progress. The most significant work was the rebuild of the network and backup requirements. Bulletproof led the design and build with support of the City's IT team. With the urgency to implement a secure network, Bulletproof leveraged supply agreements from several municipalities and governments to procure the components required. Procurement of these requirements were done under emergency and necessary clauses outlined in the City's Procurement Policy, General Procurement Act of New Brunswick, Comprehensive Economic and Trade Agreement of Canada (CETA), and the Canadian Free Trade Agreement (CFTA).

Actual and projected consulting and material costs related to Bulletproof are outlined in Tables 2 and 3. Costs are presented without tax.

Table 2: Bulletproof Solutions ULC consulting costs

Bulletproof Solutions ULC Consulting	**Original SOW**	**Actual Cost as of Feb 28**	**Estimated Remaining**	**Total Projected**	**Funding to be submitted**
Recovery Activities	$444,250	$629,273	$257,133	$886,406	Insurance
Forensic Investigation Activities	$45,000	$72,000	$0	$72,000	Insurance
Projected Total	**$489,250**	**$701,273**	**$257,133**	**$958,406**	

Table 3: Bulletproof Solutions ULC material costs

Bulletproof Solutions ULC Hardware, Licenses, Support	Actual Costs as of Feb 28	Projected Costs	Total Costs	Funding to be Submitted
Network Hardware Equipment	$325,516	$0	$325,516	Insurance
Server Storage Hardware Equipment	$148,206	$0	$148,206	Insurance
Backup Hardware Equipment	$323,282	$0	$323,282	Insurance
Support / License - Network	$87,532	$0	$87,532	Operating Reserve
Support / License - Server / Storage	$2,938	$0	$2,938	Operating Reserve
Support / License - Backup	$228,725	$0	$228,725	Operating Reserve
Additional Fire Walls / Switches	0	$69,199	$69,199	IT Reserve
Totals	**$1,116,199**	**$69,199**	**$1,185,398**	

Mandiant with support from Bulletproof completed a forensic investigation of the City's compromised network in February 2021. Costs related to Mandiant include both consulting and technology fees related to remote access to the compromised network. The necessary technology was implemented by Bulletproof. The investigation involved a review of all the logs from the Bulletproof security operations center generated from the City's SIEM (Security Information and Event Management) solution. Actual costs are noted in Table 4.

Table 4: FireEye Mandiant goods and services costs

FireEye Mandiant	Original SOW	Actual Costs as of Feb 28	Projected Cost	Total Projected Costs	Funding to be Submitted
Incident response activities	$100,000	$139,200	$0	$139,200	Insurance
Incident remediation planning and support	$40,000	$0	$0	$0	Insurance
Reporting	TBD	$24,000	$0	$24,000	Insurance
Endpoint Incident Response Technology	$9,000	$9,000	$0	$9,000	Insurance
Network Incident Response Technology	$12,000	$0	$0	$0	N/A
Other	$1,000	$0	$0	$0	N/A
Totals USD	**$162,000**	**$172,200**	**$0**	**$172,200**	
Estimated CAD	**$210,600**	**$223,860**	**$0**	**$223,860**	

Remaining consulting and material costs related to network recovery and event management are outlined in Table 5.

Table 5: Consulting/Vendor goods and services costs

Consultant / Vendor	Service	Actual Costs as of Feb 28	Projected Cost	Total Projected Costs	Funding to be Submitted
Anisoft	Backup Recovery	$16,278		$16,277	Insurance
Ivan's Audio and Visual	Council Chamber Support	$1,806		$1,806	Insurance
Blakes / Norton Rose	External Counsel		$24,000	$24,000	Insurance
CYPFER	Ransomware Recovery / Cyber Advisory Services	$10,250		$10,250	Insurance
Total Projected		**$28,334**	**$24,000**	**$52,334**	

With the backup in place, the City's IT Team is moving on to application restores. Several financial and public safety applications have already been restored. Microsoft Office 365 has been implemented providing users with email, administrative applications, and collaboration tools. Applications have been prioritized for restoration based on service impact, vendor availability, and the City's IT Team resource capacity. Estimates for the recovery are being developed as application restoration facilitators work through a seven-step process that includes defining requirements, designing, and planning steps. Estimated vendor and hardware costs related to application restores is $458,290 plus HST. Agreements and equipment purchases will be brought forward to Common Council for approval as required by the City's Procurement Policy.

Table 6 outlines miscellaneous costs related to support the recovery and ensure business continuity in the delivery of public services.

Table 6: Incident response actual and projected costs

Incident Response Costs	Actual Costs as of Feb 28	Projected Cost	Total Projected Costs	Funding to be Submitted
Business Continuity - Service Interruption	$6,543		$6,543	Insurance
Service Interruption – HVAC 120 days	$7,691		$7,691	Insurance
Communications	$171		$171	Insurance
Forensics	$94		$94	Insurance
Recovery	$3,743		$3,743	Insurance
Response	$10,681		$10,681	Insurance
City Overtime - Recovery	$33,198	$10,000	$43,198	Insurance
Total Costs	**$62,121**	**$10,000**	**$72,121**	

Overall actual and total projected costs are presented in Table 7. While a significant portion of the network rebuild has been completed, significant costs remain for the application restores. The estimate provided for application restores should consider a contingency of plus or minus twenty percent (+/- 20%).

Of the total projected costs in the amount of $2.95 Million, the City's response team estimates that at least 85% ($2.5 Million) of total costs should be recoverable through the City's two insurance policies. Actual costs incurred and whether they will be covered under the cyber policy cannot be confirmed until the insurer provides their written position following the City's submission of Proof of Loss. The remaining costs that could range between $400,000 and $500,000 will either be absorbed into IT operating budget or applicable reserves. Renewal and enhancements of information technology requirements are funded out of the IT reserve, with projects planned and presented within the capital budget annually.

Table 7: Overall projected recovery and event management costs related to the cyberattack.

Response Component	Actuals	Projected	Total Projected
Bulletproof Consulting	$701,273	$257,133	$958,406
Bulletproof Hardware/Licenses/Support	$1,116,199	$69,199	$1,185,398
FireEye Mandiant	$223,860	$0	$223,860
Anisoft	$16,277	$0	$16,277
Ivan's Audio and Visual	$1,806	$0	$1,806
Blakes / Norton Rose	$0	$24,000	$24,000
CYPFER	$10,250	$0	$10,250
Vendor Support Application Restores	0	$458,291	$458,291
Incident Response Costs	$62,121	$10,000	$72,121
Projected Totals	**$2,131,786**	**$818,623**	**$2,950,409**

A final cost component of the City's network rebuild is Microsoft licensing for security. The Enterprise Agreement approved by Common Council did not include security costs for moving to Office 365 as the initial plan was to implement a hybrid system of a hosted and on-premise solution over the three-year life of the agreement. Security is currently being purchased through Bulletproof and will transition to Microsoft with the year one reconciliation of licensing needs in April of 2021. Security costs are based on a per user basis. The estimated cost of security is $195,000 plus HST. As with all licenses related to users, these costs are charged back to the respective service areas as an operating cost. These funds are not included in the 2021 budget; however, they will be incorporated into future operating budgets. The installation of Microsoft security features is an industry best practice and significantly improves the City's cyber security risk profile.

INPUT FROM OTHER SERVICE AREAS AND STAKEHOLDERS

This report was prepared in collaboration with the City's Finance Team, Supply Chain Management Team, Risk Management Team, and the Information Technology Team.

ATTACHMENTS

None