Gallagher Security Corp.

(formerly Hilltop Cybersecurity Inc.)

MANAGEMENT'S DISCUSSION AND ANALYSIS

FOR THE THREE MONTHS ENDED SEPTEMBER 30, 2019

INTRODUCTION

The following management's discussion and analysis ("MD&A") of the financial condition and results of the operations of Gallagher Security Corp. (formerly Hilltop Cybersecurity Inc.) (the "Company") prepared on November 27, 2019 constitutes management's review of the factors that affected the Company's financial and operating performance for the period ended September 30, 2019. The Company changed its name to Gallagher Security Corp. on June 17, 2019. This discussion should be read in conjunction with the Company's period ended September 30, 2019 financial statements and accompany notes to the financial statements, in addition to the audited year ended June 30, 2019 financial statements and accompany notes.

This MD&A was written to comply with the requirements of National Instrument 51-102 Continuous Disclosure Obligations. The Company's consolidated financial statements have been prepared in accordance with and using accounting policies consistent with International Financial Reporting Standards ("IFRS") as issued by the International Accounting Standards Board ("IASB") and interpretations of the International Financial Reporting Interpretations Committee (IFRIC").

Dollar amounts included are expressed in US dollars except where noted. Statements in this report that are not historically based fact are forward looking statements involving known and unknown risks and uncertainties which could cause actual results to vary considerably from these statements. Readers are cautioned not to place undue reliance on forward-looking statements. In the opinion of management all adjustments considered necessary for a fair presentation have been included. All amounts following are expressed in Canadian dollars unless otherwise stated.

Additional information regarding the Company and its activities is available on SEDAR at www.sedar.com or by requesting further information from the Company's head office located in Kelowna, British Columbia, Canada.

GENERAL OVERVIEW

The Company was incorporated under the provincial laws of British Columbia, Canada, on June 30, 2005. The Company's common shares are listed on the Canadian Securities Exchange ("CSE") under the symbol "GLL".

On December 19, 2017, the Company entered into a definitive agreement (the "Agreement") with Hill Top Security, Inc. ("HTSI"). On February 14, 2018, the Company acquired 25% of HTSI which constituted a fundamental change of the Company within the policies of the CSE. On June 12, 2018, the Company acquired a further 24% of HTSI through the issuance of 420,000 common shares and 4,913,666 convertible common shares (Notes 4 and 9). During the period from June 12, 2018 to September 30, 2018, the Company was a technology company engaged primarily in the development of cyber security and cryptocurrency software. Effective October 1, 2018, the Company determined that HTSI was essentially inactive and that it no longer had control over HTSI. Accordingly, the Company wrote off its investment in HTSI and accounted for the reversal of the reverse take-over transaction as a discontinuance of operations. The Company is now in the process of searching for a new business opportunity.

Quarterly Highlights
Effective October 1, 2018, the Company determined that HTSI had virtually ceased its business operations and the company was essentially inactive. As a result of this, the Company will continue to seek new business opportunities and additional financing.

<u>Overview of the Company's Activities Prior to Discontinuing Operations</u>

The Company has made substantial progress in evolving the technical capabilities of its three core products: the Vauban Cybersecurity Platform, the Enterprise Information Service (now branded **CybrEPM**) and the Cryptocurrency Platform (now branded **CybrKeep)**. The overarching objective has been to enhance the commercial viability of each product while augmenting the security and management of the supporting technical infrastructure. Both the EIS and Cryptocurrency Platform have undergone re-branding initiatives to help tailor the messaging and feature set for commercial customers.

Additionally, the Company has taken the opportunity to integrate unique platform capabilities as services which can be bundled for customers seeking to benefit from a unified offering.

Vauban Cybersecurity Platform

In September 2016, the Company released "Vauban" as its Minimum Viable Product ("MVP") offering for security incident response. The Company's military management team identified the vulnerability of national infrastructures and, more particularly, small-to medium-sized businesses ("SMBs") facing the realities of cyber warfare in the 21st century. And in response, the Company developed a unique, military-grade, cyber security platform for SMBs called Vauban. With previous services including software development, big data analytics, project management, system architecture and sustainability, the Company has focused on the Vauban platform as its comprehensive product. It is comprised of blockchain event validation, cyber tagging, incident response and rapid restoration. While Vauban, was originally developed for governments and large businesses, the Company has made it available to the SMB sector.

Vauban is a military-grade security platform for small-to-medium businesses that enables rapid detection and comprehensive response for cyber security incidents. Vauban automates the detection and remediation of network security incidents with patent-pending technology for digital cybertagging™ and security event validation. Vauban also provides end-to-end visibility of security events with role-specific dashboards that enhance situational awareness and collaboration. Vauban is architected as a complete solution for small-to-medium businesses with the options of a cloud-delivered SaaS model, an on-premise service or a hybrid approach. All options provide the same set of comprehensive, integrated capabilities.

The Company's Vauban security platform provides integrated modules that deliver powerful processing capabilities. Business modules may be tailored to specific industries or organizational functions to use data to drive better business performance. The benefit to customers is the ability to process, capture and learn from business processes with a system that is significantly more flexible and cost effective than comparable market offerings. Vauban makes cyber incident detection and response more efficient and more accurate, preventing breaches and avoiding losses.

In terms of distribution, the Vauban SMB Platform is sold as Software as a Service (SaaS) subscriptions on 1, 2, or 3 year contracts with discounts for 2 and 3 year contracts. SaaS is a software distribution model in which a third-party provides customers applications over the Internet.

As of August 2017, HTSI filed a patent titled "Computerized System and Method for Providing Cybersecurity Detection and Response Functionality" for the Vauban platform's sophisticated cybersecurity event processing system. This intellectual property describes novel technology and processes for addressing some of the most relevant issues in computer network security and is, therefore, important in the current market climate. Vauban has been developed by a team of security experts with substantial military and commercial experience and the company holds a top-secret clearance based on the work it currently carries out for the U.S. government.

Development efforts for Vauban include:

- Incorporation of distributed, smart agents which collect and triage security event data at the source. These agents are simple installs for customer endpoints that automatically synchronize findings with the Virtual Private Network (VPN) gateway for analysis and reporting.
- Integration of the Sophos Unified Threat Management suite to evaluate distributed events, incorporate threat intelligence and protect cloud-based assets.
- Enhancements to the centralized alert capture subsystem that provides tailored views of cyberattack tactics, techniques and procedures.
- Customer threat mapping capability which provides customers an ongoing evaluation of environment-specific threats, existing security controls and the associated "heat map" of threat coverage

CybrEPM (formerly Enterprise Information Service (EIS)

CybrEPM is a cloud-based, Federal Information Processing Standard, Financial Information Audit Readiness ("FIPS-FIAR") compliant portfolio management platform. Initially deployed in classified US Department of Defense cloud environments, CybrEPM has received an Authority to Operate ("ATO") in one of the most secure computing environments in the world. The EIS provides risk-aware planning, budgeting, execution, project management, contract management and financial reporting capabilities.

CybrEPM provides additional functionality that allows organizations to transparently manage investments and attain a complete view of their project portfolios. Considering CybrEPM is a U.S. Government specific application for tracking and managing public funds consistent with federal regulations, this product is delivered to government agencies by way of various procurement contracts.

The CybrEPM platform has matured to an commercial enterprise portfolio management tool that exceeds the capabilities of Oracle's Project Portfolio Management product. New development for CybrEPM includes:

- Prioritization of projects and portfolios across an industry-standard set of organizational metrics
- Robust report creation wizards and report customization capabilities
- Customizable dashboards and graph selection functionality
- Custom form design
- Configurable financials that include dimensions of time, budget state, type of money, units of measure and asset category
- Customizable workflows with transactions that can be memorialized on private blockchains
- Integration of business intelligence and project management tools
- Enhanced navigational elements and updated user interface components
- Support for customized invoices and associated workflows

<u>CybrKeep (formerly named the Cryptocurrency Platform)</u>

CybrKeep has evolved to support secure, end-to-end cryptocurrency transactions as well as enabling asset-backed tokenization of reserve-style assets. New developments for CybrKeep include:

- Colds storage of private cryptographic keys
- A hierarchical cryptocurrency 'hard-wallet' which supports trading of 10 different cryptocurrencies
- Third party verification service of wallet user identity for restoration of lost or damaged accounts
- Geofencing of cryptocurrency transactions to limit the permissible range of transaction inception
- A distributable Android app supporting wallet functionality
- Substantial improvements to user experience design and branding

Selected Annual Information

For the years ended June 30,	**2019**	**2018**	**2017**
	$	$	$
Net loss and comprehensive loss	(4,644,975)	(11,893,913)	(164,277)
Total assets	30,745	801,857	59,167
Total liabilities	338,809	878,355	268,844
Shareholders' equity (deficiency)	(308,064)	(76,498)	(209,677)
Basic and diluted loss per common share	($0.64)	($40.16)	($727.86)

Summary of Quarterly Results

	Q1 2020	Q4 2019	Q3 2019	Q2 2019	Q1 2019	Q4 2018	Q3 2018	Q2 2018
	$	$	$	$	$	$	$	$
Net (loss) income	(39,799)	(2,955,783)	(80,931)	(371,870)	(1,236,391)	(9,319,352)	(1,046,232)	(1,276,209)
Basic/Diluted (loss) income per share	(0.00)	(0.62)	(0.00)	(0.00)	(0.02)	(31.46)	(3.50)	(4.70)

For the Three Months Ended September 30, 2019
The Company realized a net loss of $39,799 for the three months ended September 30, 2019, respectively compared to $1,232,391 net loss for the same prior comparable period. The current year net loss includes a net loss from discontinued operations of $623,798. The overall decrease in net loss is attributed to scale down and eventual discontinuance of operations. Management expects to keep overhead expenses at a minimum level in comparison to prior periods while evaluating new business opportunities moving forward.

Related Party Transactions

Compensation of Key Management Personnel

Amounts paid to key management personnel and/or entities over which they have control during the period ended September 30, 2019 and 2018 are as follows:

	2019	2018
	$	$
Consulting fees	34,066	7,500

Balances Payable

At September 30, 2019, the Company owed the following balances to related parties and/or entities over which they have control:

- $111,483 (2019 - $147,737) in consulting fees and reimbursable expenses to a company controlled by the Company's CEO;
- $24,944 (2019 - $13,708) in consulting fees to a company controlled by the Company's CFO.
- $7,949 (2019 - $Ni;) in consulting fees to a director of the Company.

Outstanding Share Data

As at the date of this document, the Company had 9,431,518, common shares issued and outstanding, 55,000 share purchase options issued and outstanding, and 3,081,128 share purchase warrants issued and outstanding.

<u>For the period ended September 30, 2019</u>

On August 21, 2019, the Company entered into a Debt Settlement Agreement with a company controlled by the CEO of the Company to settle $70,050 ($91,725 CDN) by issuing 1,834,500 Units at a deemed price of $0.05 CDN per unit. Each unit comprises one common share and one share purchase warrant exercisable at $0.05 CDN per share for two years from the date of issue.

Liquidity and Capital Resources

The Company was a technology company engaged primarily in the development of cyber security and cryptocurrency software. The Company expects to rely upon equity financing and related party loans to seek new business opportunities.

The accompanying consolidated financial statements for the period ended September 30, 2019 have been prepared on a going concern basis which assumes that the Company will be able to realize its assets and discharge its liabilities in the normal course of business for the foreseeable future. The Company's ability to continue as a going concern is dependent upon successful completion of additional financing and upon its ability to attain profitable operations. There can be no assurances that this capital will be available in amounts or on terms acceptable to the Company, or at all. This creates material uncertainty which casts significant doubt about the Company's ability to continue as a going concern.

The Company is actively pursuing joint venture partners and has minimized its exploration activities and over-all operations in an effort to conserve cash.

Financial Instruments

The Company is exposed through its operations to the following financial risks:

- Market risk
- Credit risk
- Liquidity risk

In common with all other businesses, the Company is exposed to risks that arise from its use of financial instruments. This note describes the Company's objectives, policies and processes for managing those risks and the methods used to measure them. Further quantitative information in respect of these risks is presented throughout these consolidated financial statements.

General Objectives, Policies, and Processes

The Board of Directors of the Company has overall responsibility for the determination of the Company's risk management objectives and policies and, while retaining ultimate responsibility for them, it has delegated the authority for designing and operating processes that ensure the effective implementation of the objectives and policies to senior management. The overall objective of the Board of Directors is to set policies that seek to reduce risk as far as possible without unduly affecting the Company's competitiveness and flexibility. Further details regarding these policies are set out below.

Market Risk

Market risk is the risk that the fair value of future cash flows of a financial instrument will fluctuate because of changes in market prices. Market prices are comprised of four types of risk: foreign currency risk, interest rate risk, commodity price risk and equity price risk. The Company is not currently exposed to foreign currency risk, interest rate risk or commodity price risk.

Credit Risk

Credit risk is the risk of financial loss to the Company if a customer or counterparty to a financial instrument fails to meet its contractual obligations. The financial instruments that are potentially subject to credit risk are cash and amounts receivable (excluding GST). The carrying amounts of these financial assets represent their maximum credit exposure. Cash is maintained with a financial institution of reputable credit and may be redeemed upon demand.

Liquidity Risk

Liquidity risk is the risk that the Company will not be able to meet its financial obligations as they become due. The Company's policy is to ensure that it will always have sufficient cash to allow it to meet its liabilities when they become due, under both normal and stressed conditions, without incurring unacceptable losses or risking damage to the Company's reputation. The key to success in managing liquidity is the degree of certainty in the cash flow projections. If future cash flows are fairly uncertain, the liquidity risk increases.

Determination of Fair Value

IFRS 7 establishes a fair value hierarchy that prioritizes the input to valuation techniques used to measure fair value as follows:

Level 1 – quoted prices (unadjusted) in active markets for identical assets or liabilities;
Level 2 – inputs other than quoted prices included in Level 1 that are observable for the asset or liability, either directly (i.e. as prices) or indirectly (i.e. derived from prices); and
Level 3 – inputs for the asset or liability that are not based on observable market data (unobservable inputs).

The Company's derivative liability – warrants is the only financial instruments on the statement of financial position measured at fair value. There were no transfers between Level 1, 2 or 3 during the years ended June 30, 2019 and 2018.

Critical Accounting Estimates

The preparation of consolidated financial statements in conformity with IAS 3 requires management to make judgments, estimates and assumptions that affect the application of policies and the reported amounts of assets and liabilities, income and expenses. Actual results may differ from these estimates.

Accounts that require significant estimates as the basis for determining the stated amounts include exploration and evaluation assets and share-based compensation. The assessment of any impairment of exploration and evaluation assets is based on the estimated recovery of future exploitation or sale where the activities have not reached a stage which permits a reasonable assessment of existence of reserves. Share-based compensation expense is calculated using Black-Scholes valuation model which requires significant judgment as to considerations such as stock option lives and stock volatility.

Significant Accounting Policies

A summary of the Company's significant accounting policies is included in Note 3 of the audited consolidated financial statements for the year ended June 30, 2019.

Risks and Uncertainties

Regulatory Risks

The activities of the Company will be subject to regulation by governmental authorities. Achievement of the Company's business objectives are contingent, in part, upon compliance with regulatory requirements enacted by these governmental authorities and obtaining all regulatory approvals. The Company cannot predict the time required to secure all appropriate regulatory approvals for its products, or the extent of testing and documentation that may be required by governmental authorities. Any delays in obtaining, or failure to obtain regulatory approvals could have a material adverse effect on the business, results of operations and financial condition of the Company.

The business of the Company is subject to rapid regulatory changes. Failure to keep up with such changes may adversely affect the business of the Company. Failure to follow regulatory requirements will have a detrimental impact on the business. Changes in legislation cannot be predicted and could irreparably harm the business.

Lack of Demand

A failure in the demand for the Company's products or services to materialize as a result of competition, technological change or other factors could have a material adverse effect on the business, results of operations and financial condition of the Company.

Reliance on Management and Key Personnel

The success of the Company is dependent upon the ability, expertise, judgment, discretion and good faith of its senior management. While employment agreements are customarily used as a primary method of retaining the services of key employees, these agreements cannot assure the continued services of such employees. The Company attempts to enhance its management and technical expertise by recruiting qualified individuals who possess desired skills and experience in certain targeted areas. The Company's inability to retain employees and attract and retain sufficient additional employees as well as, engineering, and technical support resources could have a material adverse impact on the Company's financial condition and results of operation. Any loss of the services of such individuals could have a material adverse effect on the Company's business, operating results or financial condition.

Additional Financing

The Company's future capital requirements depend on many factors, including its ability to market products successfully, cash flows from operations, locating and retaining talent, and competing market developments. Based on the Company's current financial situation, the Company may have difficulty continuing operations at the current level, or at all, if it does not raise additional financing in the near future.

Conflicts of Interest

Certain of the directors and officers of the Company are also directors and officers of other companies, and conflicts of interest may arise between their duties as officers and directors of the Company and as officers and directors of such other companies.

Limited Market for Securities

Upon completion of the Initial Acquisition, the Company Shares will be listed on the CSE, however, there can be no assurance that an active and liquid market for the Company Shares will develop or be maintained and an investor may find it difficult to resell any securities of the Company.

Going Concern Risk

The financial statements have been prepared on a going concern basis under which an entity is considered to be able to realize its assets and satisfy its liabilities in the ordinary course of business. The Company's future operations are dependent upon the identification and successful completion of equity or debt financing and the achievement of profitable operations at an indeterminate time in the future. There can be no assurances that the Company will be successful in completing an equity or debt financing or in achieving profitability.

The financial statements do not give effect to any adjustments relating to the carrying values and classification of assets and liabilities that would be necessary should the Company be unable to continue as a going concern.

Disclosure of Internal Controls

Management has established processes which are in place to provide them sufficient knowledge to support management representations that they have exercised reasonable diligence that (i) the audited consolidated financial statements do not contain any untrue statement of material fact or omit to state a material fact required to be stated or that is necessary to make a statement not misleading in light of the circumstances under which it is made, as of the date of and for the periods presented by the audited consolidated financial statements; and (ii) the audited consolidated financial statements fairly present all material respects the financial condition, results of the operations and cash flows of the Company, as of the date of and for the periods presented by the audited consolidated financial statements.

In contrast to the certificate required under National Instrument 52-109 Certification of Disclosure in Issuer's Annual and Interim Filings (NI 52-109), the Company utilizes the Venture Issuer Basic Certificate which does not include representations relating to the establishment and maintenance of disclosure controls and procedures (DC&P) and internal control over financial reporting (ICFR), as defined in NI 52-109. In particular, the certifying officers filing the Certificate are not making any representations relating to the establishment and maintenance of: (i**)** controls and other procedures designed to provide reasonable assurance that information required to be disclosed by the issuer its annual filings, interim filings or other reports filed or submitted under securities legislation is recorded, processed, summarized and reported within the time periods specified in securities legislation; and (ii) a process to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with the issuer's GAAP and IFRS. The Company's certifying officers are responsible for ensuring that processes are in place to provide them with sufficient knowledge to support the representations they are making in this certificate. Investors should be aware that inherent limitations on the ability of certifying officers of a venture issuer to design and implement on a cost effective basis DC&P and ICFR as defined in NI 52-109 may result in additional risks to the quality, reliability, transparency and timeliness of interim and annual filings and other reports provided under securities legislation.

ADDITIONAL INFORMATION

Additional information relating to the Company can be found on SEDAR at www.sedar.com.