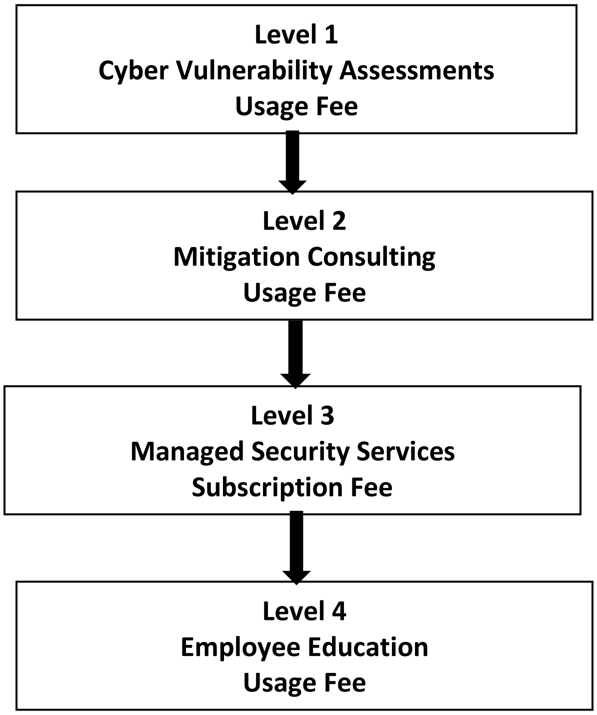
OCSI
Optium Cyber Systems, Inc.

OPTIUM CYBER SYSTEMS RELEASES REVENUE MODEL

THE WOODLANDS, TEXAS, OCTOBER 16, 2017 (OTC MARKETS) – Optium Cyber Systems, Inc. (Ticker: **OCSY**) (the Company or OCSI), would like to share with stockholders, the details of its finalized revenue model for its cyber assessment and monitoring platform that has recently been launched in the health care sector. The strategy to generate income is comprised of four levels or revenue streams. Starting with an initial vulnerability assessment of a client's IT network then leading into a monthly monitoring contract with additional consulting and educational services to be provided on an as needed basis. The following diagram outlines the four levels of the revenue model that will be implemented under a typical client engagement:



Level 1
Cyber Vulnerability Assessments
Usage Fee

Level 2
Mitigation Consulting
Usage Fee

Level 3
Managed Security Services
Subscription Fee

Level 4
Employee Education
Usage Fee

<u>Level 1 - Cyber Vulnerability Assessments</u>

Revenue Stream - Usage Fee
A Cyber Vulnerability Assessment or CVA is the foundation of the work to be performed. It defines, identities and classifies any security holes in a client's network environment. Through the collection of questionnaires and subsequent interviews of the client's IT staff, the parameters of the assessment are determined including a ranking of potential threats in the client's network. During a CVA engagement, one or more security engineers from OCSI will deliver physical equipment to a client's location. These devices gather the data used to locate and categorize potential threats. OCSI engineers will initiate a scan which, depending upon the size and complexity of the environment, can run several days to several weeks. Remote connectivity is setup to monitor the status of the procedure and care is taken as to the 'sensitivity' of the network as some are susceptible to malfunctioning during the scanning process. Once the scan is complete, the data is analyzed and presented in a comprehensive report for the client. The report will be written in a way that focuses on classification and ranking of the risks to the client's environment. Mitigation recommendations (see Level 2) will also be recommended, identifying the most critical vulnerabilities and methods to address these vulnerabilities. Since no IT environment remains static, follow up engagements are also recommended to re-evaluate the environment on a regular basis to determine the effectiveness of the implemented mitigation and look for new vulnerabilities.

Level 2 - Mitigation Consulting

Revenue Stream - Usage Fee
In the process of performing the Cyber Vulnerability Assessments, the need will arise for additional guidance as vulnerabilities are identified and need to be addressed. OCSI engineers will step in to manage this process and provide detailed architecture and implementation guidelines to effectively mitigate any issues discovered during the CVA process.

Level 3 - Managed Security Services

Revenue Stream – Subscription Fee
Once the Cyber Vulnerability Assessment has been run and any vulnerabilities mitigated, OCSI will implement a real-time monitoring system comprised of software, strategically located sensors and a team working in four-hour shifts. OCSI will be responsible for overseeing activities of a client's network and to notify the client when there is a breach of a set of pre-defined conditions. This will allow the OCSI team and the client to immediately address any questions activities and mitigate potential damage. Monthly reports will also be provided to inform the client of any non-critical information gathered and to highlight anything that needs addressing by their internal IT team.

Level 4 - Employee Education

Revenue Stream - Usage Fee or Subscription Fee
An integral part of risk reduction strategy is keeping track of the likelihood that employees are going to be susceptible to social engineering attacks such as e-mail phishing campaigns or ransomware attacks. The majority of cyber-attacks begin with an e-mail so clients must know who in their organizations are likely to unwittingly opening a malicious payload. The solution is to implement and employee education strategy designed to 'test' users in real world scenarios that allow harmless but 'teachable moments' for those who click on baited messages. The statistics on click rates are tracked so measurable results can be delivered and the necessary steps take to educate the vulnerably employee(s). OCSI will provide the employee education platform under three different scenarios:

1. A usage fee service where OCSI will run periodic testing of the client email network with reports generated to identify which employees 'passed' or 'failed'.
2. As a standalone subscription service which can be managed internally by the client.
3. As a part of a comprehensive MSSP engagement. This option may be provided as a managed or standalone offering.

OCSI will offer to their customers a guarantee to pay the crypto-ransom for anyone hit by ransomware while all users are participating in the education program platform.

Other - Third Party Licensing Agreements

Revenue Stream - Licensing
In addition to the above, the management of OCSI is exploring the possibility of licensing the platform to third parties for application in specific industries.

About Optium Cyber Systems, Inc.
OCSI has developed a proprietary process to analyze, identify and address cyber security vulnerabilities in an organization's critical IT infrastructure which is scalable to any size organization in any industry. OCSI has recently launched in the health care sector, focusing on protecting health care facilities including hospitals, nursing homes and doctor's offices from cyberthreats such as the manipulation of medical devices or theft of patient records. OCSI is a publicly traded company having its common shares quoted on the OTC Markets under the symbol "OCSY".

CONTACT

Investor Relations
Ten Associates LLC
11529 N. 120th St.
Scottsdale, Arizona
85259 USA
Telephone: 480-326-8577
Contact: Thomas E. Nelson
Email: tenassociates33@gmail.com

Optium Cyber Systems, Inc.
8350 Ashlane Way, Suite 104
The Woodlands, Texas
77382 USA
Telephone: 936-559-7407
Web: www.optiumcyber.com
Email: info@optiumcyber.com
Twitter: https://twitter.com/OCSI4INVESTOR
Facebook: https://www.facebook.com/OCSI4INVESTOR

Forward-Looking Statements

Except for the historical information contained herein, the matters discussed in this press release are forward-looking statements. Actual results may differ materially from those described in forward-looking statements and are subject to risks and uncertainties. See Cre8tive Works, Inc.'s filings with OTC Markets which may identify specific factors that may cause actual results or events to differ materially from those described in the forward-looking statements.

Safe Harbor Statement

This release includes forward-looking statements, which are based on certain assumptions and reflects management's current expectations. These forward-looking statements are subject to a number of risks and uncertainties that could cause actual results or events to differ materially from current expectations. Some of these factors include: general global economic conditions; general industry and market conditions, sector changes and growth rates; uncertainty as to whether our strategies and business plans will yield the expected benefits; increasing competition; availability and cost of capital; the ability to identify and develop and achieve commercial success; the level of expenditures necessary to maintain and improve the quality of services; changes in the economy; changes in laws and regulations, including codes and standards, intellectual property rights, and tax matters; or other matters not anticipated; our ability to secure and maintain strategic relationships and distribution agreements. The Company disclaims any intention or obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.