OPTIUM CYBER SYSTEMS HIGHLIGHTS CYBER VULNERABILITY IN HEALTH CARE INDUSTRY

THE WOODLANDS, TEXAS, OCTOBER 05, 2017 (OTC MARKETS) – Optium Cyber Systems, Inc. (the "Company") (Ticker: "OCSY") would like to highlight for its shareholders, the cyber vulnerabilities existing today in the health care industry and briefly discuss its newly launched platform tailored to address these issues.

CYBER CRIME – HEALTHCARE INDUSTRY

According to the 2015 Cyber Security Intelligence Index published by IBM, the healthcare industry sustained the most cyber attacks, far more than any other industry or sector. This same report claimed that nearly 8 out of 10 healthcare institutions were hit and that it is only going to get worse. In a recent article published by CSO it was stated that ransomware attacks on healthcare organizations will quadruple by 2020. According to the Verizon 2016 Data Breach Investigations Report, the healthcare sector is 30 percent more likely than the financial sector to have a breach of an internal network with the average cost of a healthcare breach estimated to be more than $2.2 million. But, not only does a cybersecurity threat pose a financial risk, but creates a situation of life and death.

CYBER CRIME – MEDICAL DEVICES

Medical devices can be extremely vulnerable to security breaches potentially impacting the safety and effectiveness of the device. Researchers in Belgium and the UK have demonstrated that it is possible to transmit life-threatening signals to implanted medical devices. Dick Cheney ordered a change to his pacemaker to better protect it from hackers. Last year, Johnson & Johnson warned customers about a security bug in one of its insulin pumps. As hackers increasingly take advantage of historically lax security on embedded devices, defending medical instruments has taken on new urgency. Implanted medical device hacks are so memorable because they're so personal. You wouldn't want something inside your body or on your skin to be remote-controlled by a criminal. Unfortunately, many types of these devices are broadly vulnerable to attack and are ssusceptible to cyber manipulation. These devices include not limited to:

- Drug infusion pumps
- Insulin pumps
- X-ray systems
- Cardioverter defibrillators
- CT Scanners
- Refrigeration units

There are estimated to be 15 million medical devices in use in U.S. hospitals today with the average bed utilizing 10 to 15 machines. An average size hospital with 500 beds would have a total of 7,500 machines. There's a need to protect patients, so that attackers can't hack an insulin pump to administer a fatal dose. And vulnerable medical devices also connect to a huge array of sensors and monitors, making them potential entry points to larger hospital networks.

THE OCSI SOLUTION

OCSI has developed a proprietary process to analyze, identify and address vulnerabilities in an organizations critical IT infrastructure with its first application being tailored specifically for the health care industry. This process is broken down into four steps:

Detect – Mitigate – Remediate – Educate

Detect: OCSI will perform a comprehensive structured analysis to identify high risk areas within an organization's network allowing OCSI to address and secure these areas.

Mitigate: Much like a home alarm, OCSI will implement a monitoring system designed to detect, alert and effectively mitigate any pending threats.

Remediate: Once a vulnerability is identified, OCSI will provide a roadmap for the organization's IT staff to effectively manage or negate the threat.

Educate: Many security threats rely upon employee's lack of cyber security awareness. OCSI will provide an organization's employees cyber security awareness training on how to spot security threats and effectively deal with them.

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".

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
Email: info@optiumcyber.com

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.