October 2017

Global Small Caps Research, LLC

Company Report

Optium Cyber Systems, Inc. (OTC:OCSY)

Summary of Our Research Findings

- This report offers an analysis of Optium Cyber System, Inc. – OTC:OCSY.
- Optium is a new entrant into the cyber security detection and mitigation marketplace.
- Over the past few years, the number of cyber attacks has increased very significantly. Ransomware attacks are costing businesses billions of dollars annually. These companies are more than willing to spend on effective solutions.
- Law enforcement is virtually powerless in detecting cyber attacks as hackers utilize advanced masking techniques to hide IP addresses and utilize virtually un-trackable Bitcoins to collect ransoms.
- Optium Cyber, while still a new company, has already begun to gain traction recently signing a $2.5 million contract in the shipping industry.
- The Company's management team is highly skilled in this particular market sector and has excellent business contacts to facilitate market penetration.
- With very little convertible debt on the balance sheet, a limited stock float, and a conservative market capitalization, we believe the shares are worthy of consideration by risk-averse investors.

Company Report

Optium Cyber Systems, Inc. (OTC:OCSY)

Report Contents:

OPTIUM CYBER SECURITY, INC. (OTC:OCSY)

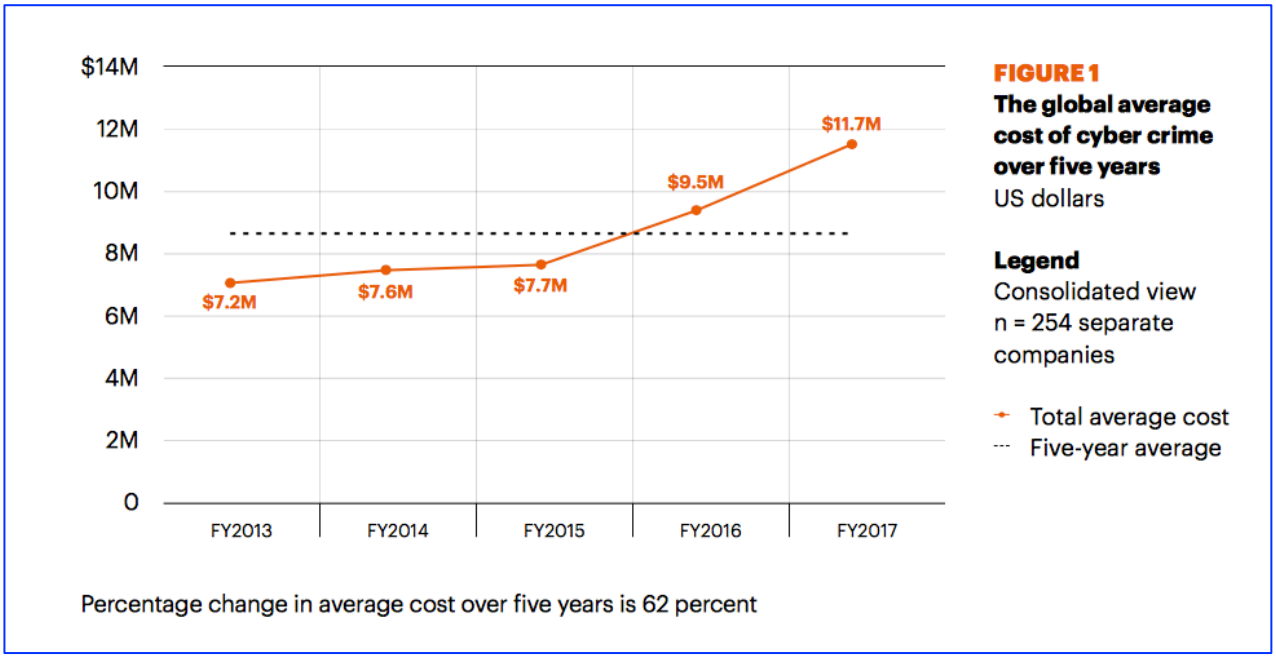
INTRODUCTION

During June of this year, a cyber attack nearly shut down one of the largest ports in the United States – the Port of Los Angeles, which if the busiest container port in the western hemisphere. Ukrainian hackers accessed the computer network of international shipping giant A. P. Moller-Maersk and caused havoc. The hackers accessed through an unsecured "back door" of a little used tax accounting software program Maersk had installed several years before. Not surprisingly, the accounting software was also of Ukrainian origin, likely initially produced and distributed to be later used as an entry point for cyber attacks on corporations.

By the time Maersk figured out what was going on and was able to block further intrusion, between $200 million and $300 million of the Company's profits had vanished.

The costs incurred by Maersk are not typical, but nevertheless the costs are still high for companies that are the victims of cyber attacks. As is outlined in Figure One, the average cyber attack costs a medium to large corporation nearly $12 million in direct costs and lost productivity. These costs are rising rapidly for corporations with the average cost rising over 62% per cyber attack over the past 5 years.

Figure One – The High Cost of Corporate Cyber Attacks



Source: Center for Cyber Security

In early September of this year, credit-reporting company Equifax announced one of the largest data breaches of all time, which involved the records for 143 million of its customers. The Equifax data breach was particularly worrisome as it included full customer records, including birth dates, addresses, Social Security numbers, and drivers license numbers, along with full credit card numbers. This data immediately hit the dark web with hackers and other criminals bidding on access in order to engage in additional cyber crimes. The full extent of the damage will not be known for years.

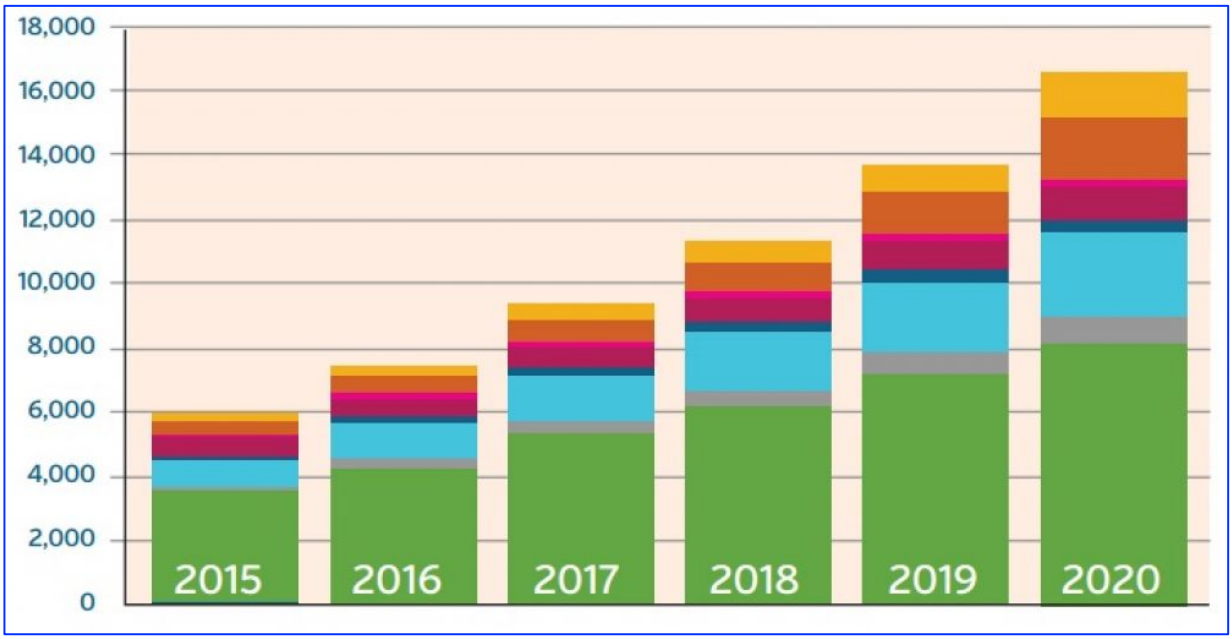
Beginning in mid-2013, a group of hackers managed to breach the server farm of Internet giant Yahoo. The hacker group had access to nearly all of Yahoo's records for an extended period of time. This allowed them ample time to download and copy terabytes of valuable information. Probably the most valuable data stolen from Yahoo were the usernames and passwords for up to 500 million Yahoo mail users. With this information, hackers were be able to comb the e-mails of millions of individuals in order to determine user names and passwords to a host of online assets. This Yahoo breach has been called the largest cyber attack in history.

2016 and Huge Hacking Year – 2017 Likely Even Better

2016 was a banner year for hackers and it appears 2017 will show further growth. According to the Identity Theft Resource Center, incidents of cyber attacks were up more than 40% during 2016. According to the Center, U.S. companies and government agencies reported nearly 1,100 data breaches where hackers were able to acquire specific information on customers or citizens. Many analysts who follow the cyber security sector believe that less than one in three data breaches are actually reported to law enforcement or other governmental agencies. Therefore, the statistic of 1,100 data breaches during 2016 is likely significantly lower than the actual.

What is startling for many industry experts and law enforcement officials is that while there was a 40% increase in 2016, there were also substantial increases in 2015 and 2014, as is outlined in Figure Two.

Figure Two – Cyber Attacks Continue to Rise



Source: Juniper Research, LLC

A Growing Worldwide Issue

Juniper Research, LLC estimates the worldwide problem of cyber crime will get much worse with this leading research firm now estimating that cyber crime will cost the worldwide economy at least $2.5 trillion per year by the year 2020, as is outlined in Figure Three.

While hacking was previously mainly designed to harass companies, the current objective is to line the pockets of hackers and the criminal organizations that hire these individuals.

Ransomware is a relatively new type of malicious software that threatens to publish the victim's computer files or blocks access to the computer files until money is paid to the hackers. Because ransomware is so profitable, new forms of this particularly dangerous hacking technology are rapidly being developed and deployed throughout the Internet.

In particular, ransomware attacks such as WannaCry and GoldenEye have made strong headlines this year and have cost many businesses billions of dollars. A recent report by researchers at anti-hacking software company Carbon Black identified hundreds of ransomware programs available for purchase on the Dark Web. Hackers can simply purchase these programs and then threaten virtually any business they choose.

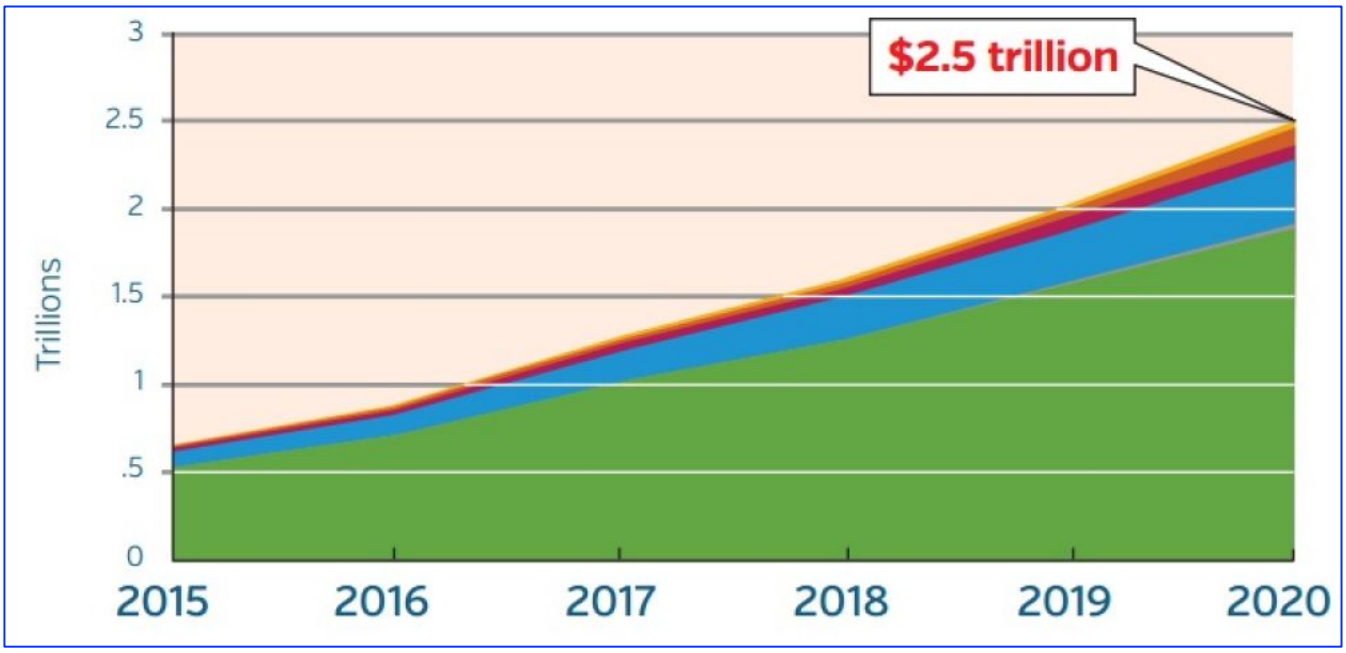
The issue of ransomware is further complicated by the degree of difficulty for law enforcement to identify the perpetrators. Most ransomware hackers utilize Internet technologies such as proxy servers and Tor browsers which mask their IP addresses, making it virtually impossible for law enforcement to not only identify the hacker, but to even identify the country of origin. Additionally, ransoms for such attacks are not paid in cash, but are typically paid for through the Dark Web using cryotocurrencies, such as Bitcoin.

With little information concerning the origin of the attacks and the inability to trace the payments, law enforcement and governmental anti-cyber crime units are virtually powerless.

Therefore, with ransomware attacks on the rise and little hope to recover paid ransoms, most in the IT industry and in law enforcement are recommending that business significantly increase their cyber attack defenses.

Even the U.S. Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) have been sounding the alarm recently. The FBI has added additional resources to track down hackers and organized crime organizations that are engaging in cyber attacks and even issued a rare public statement that both private companies and government organization should increased their cyber attack defense capabilities. The joint alert issued by the FBI and DHS provided recommendations to prevent and mitigate malicious cyber activity targeting multiple sectors while emphasizing the DHS commitment to remain vigilant against new threats.

Figure Three – Cyber Crime Cost are Expected To Grow Significantly Over the Coming Years.



Source: Juniper Research, LLC - A study conducted by leading global market analyst Juniper Research has indicated that rapid digitization of consumers' lives and enterprise records will increase cost of data breaches to approximately $2.5 trillion globally—almost four times the estimated cost of breaches in 2015.

The Maersk breach, outlined above, cost the Company a considerable amount of money, but Maersk is a huge international corporation and while profits will be affected over the short term, it will almost assuredly survive. The Equifax and Yahoo breaches, also outlined above, will likely hit both consumers and businesses to the tune of billions of dollars when everything is said and done. There will also be countless other data breaches and cyber attacks that will cost the overall worldwide economy trillions of dollars, as is outlined in Figure three.

However, while all of these breaches will have strong economic ramifications, the majority of the costs are simply economic.

As if these cyber attacks, outlined above, are not malicious enough, a new type of cyber attack is looming that will not only cause major economic havoc, but will also directly affect people's health and their lives.

That threat is healthcare related cyber attacks.

Cyber Attack in Health Care – A Growing Threat

In May of this year, the healthcare industry was rocked by a series of cyber attacks on U.S. hospitals. While hospitals had been victims of cyber attacks in the past, the vast majority of these attacks were corporate in nature where the hackers accessed corporate records, credit card information, and patient records. The attacks in May of 2017, however, were very different in that medical devices were specifically targeted.

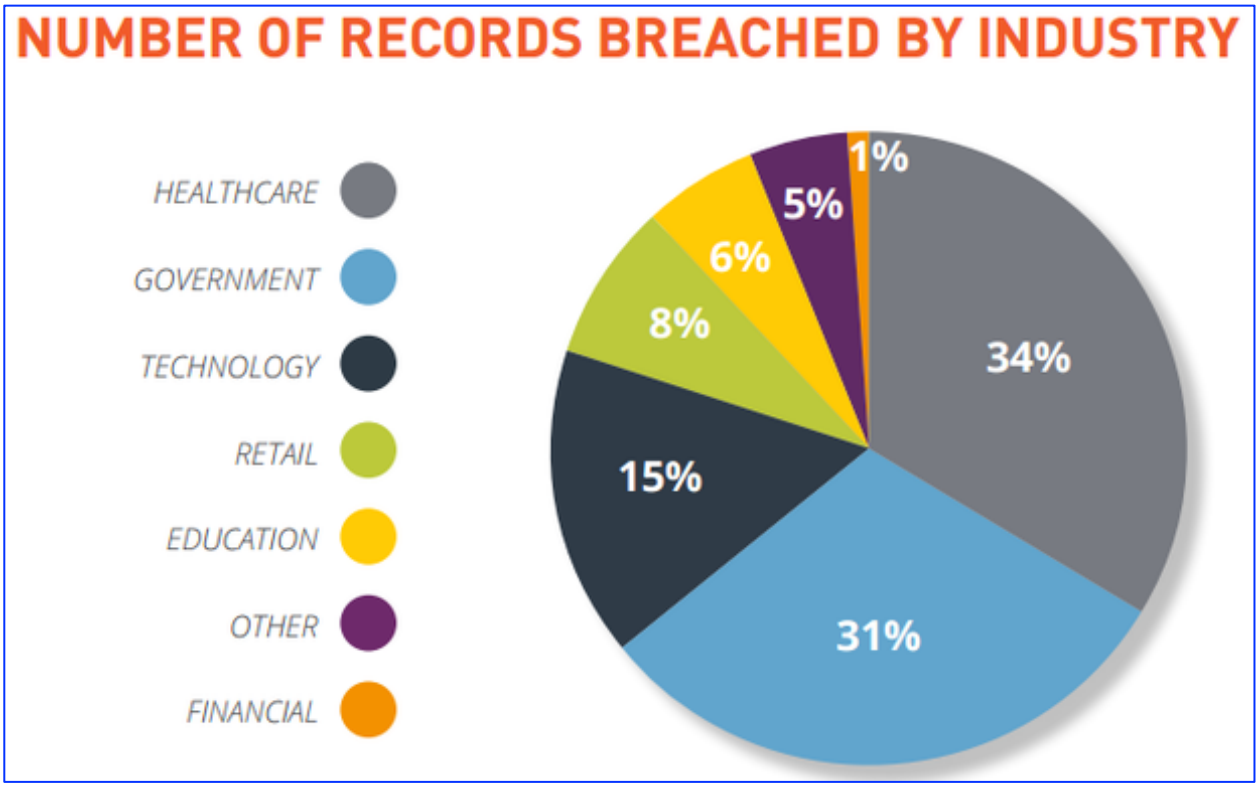
It appears hackers used the infamous WannaCry virus in order to control radiological equipment used for magnetic resonance imaging (MRIs). Fortunately, the viruses only affected the operation of the MRI machines, so therefore patient safety was not directly impacted. In another attack on Hollywood Presbyterian Hospital, located in Los Angeles, administrators were forced to pay $17,000 to hackers after they took control of the hospital's computers.

These growing number of healthcare related attacks are not limited to the United States. For example, in April of 2017, a cyber attack shutdown 65 hospitals in the United Kingdom. The UK attack was so thorough that even the computers that control the hospitals refrigerated storage were affected.

While the above attacks did not involve any loss of human life, hospital administrators and law enforcement have quickly realized that the healthcare industry might not incur such good luck in the future. The shockwave sent through the healthcare industry that has come about as a result of these attacks has been a true wake-up call for this industry.

Unfortunately, the healthcare industry has the dubious distinction of being the industry that suffers the most data breaches and has the most records stolen. As is outlined in Figure Four, the healthcare industry even receives more cyber attack attention than do government organizations, which is truly amazing considering the antiquated technologies that most governmental organizations still have deployed.

Figure Four – Healthcare Industry – A Hacker Favorite



Source: Center for Internet Security Policy

The healthcare industry, in particular within the United States, has several structural aspects that make it particularly vulnerable to hacker attack.

These include:

- Small Market Size - There are only about 6,000 hospitals in the United States. This means that there are many computer hardware and software companies that only have a few thousand customers. Larger markets typically receive more emphasis on software updates, security, and security patches than do the smaller industries such as hospitals and clinics. So, while the sector generates billions in revenue, there are other industries that are much larger and thus receive more attention from the IT industry.

- Lack of Top Down Control - Many hospitals organize around the medical practices of physicians. Each of these physician groups acts somewhat autonomously installing their own computer systems and security measures. This lack of top down control has lead to many different types of computer hardware and software being installed. As each of these systems is connected to the hospital network, many poorly secured entry points are created for hackers. This is a recipe for disaster for many hospitals and the sector is paying the price in a very big way.

- Intolerance for Downtime - Hospitals are notorious for not wanting to shut down computer systems to enable upgrades. Whereas a non-healthcare company would simply shut down operations for a few days in order to install new computer systems, this is often not a viable option for hospitals and clinics. Therefore, security upgrades and new hardware implementations often get delayed or do not get done at all. This is especially an issue relative to ransomware. Microsoft has recently issued software patches to close back doors in order operating systems. Many in the healthcare industry have simple ignored these updates and have not updated their systems simply because the IT managers do not want shut down system in order to update.

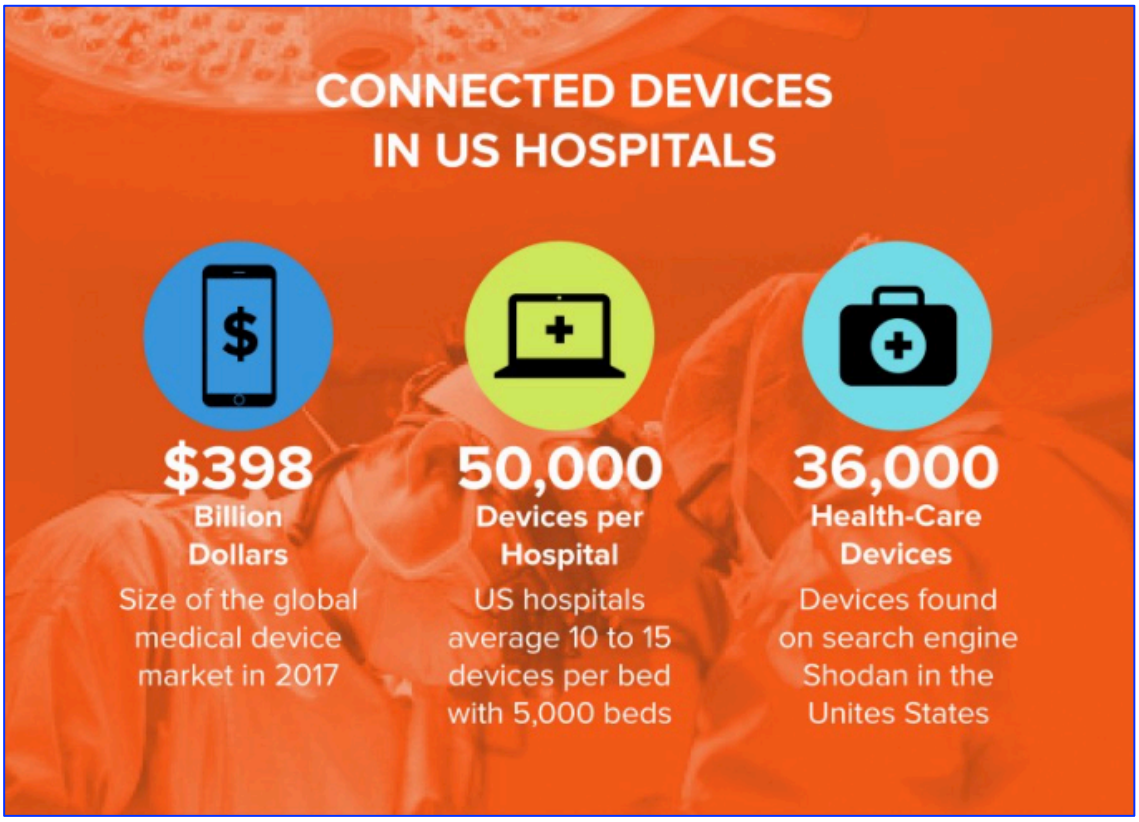
- Conductivity of Medical Devices - As is discussed below, manufacturers and systems integrators have made great strides in interconnecting medical devices into the Internet of things. While this has increased convenience, this increase in connectivity has created security breach avenues for hackers.

Cyber Attacks on Medical Devices - A Looming Disaster for Healthcare and Patients

Imagine the following scenario – You or someone in your family develops a heart condition and receives and implanted defibrillator device, in order to correct abnormal heart rhythms. The devices are remarkable in that these are implanted and are almost unnoticeable by the wearer, allowing the patient to return to near normal lifestyle. There are also features built into the defibrillator that allows data to be uploaded and downloaded so that doctors can update and monitor the device and receive updates on the patient's progress. The wireless conductivity also allows the healthcare professional to adjust and fine-tune the implanted device without invasive procedures.

While the wireless conductivity certainly has its benefits, there are also very significant drawbacks. The same wireless conductivity that allows monitoring, also allows an entry point for hackers who could gain control the device, causing serious health consequences for you or a family member – in theory, a hacker could even power down the device, which could kill the patient.

Figure Five – Each Hospital Bed Utilizes 10 to 15 Networked Medical Devices



Source: Zingbox Consulting, LLC

While there has been a lot of press about the potential for implanted medical devices to be hacked, implanted medical devices represent only a small fraction of the total risk. As is outlined in Figure Five, according to a study conducted by healthcare security firm Zingbox, U.S. hospitals average 10 to 15 medical devices for each hospital bed. Considering there are nearly 300 hospitals in the United States with more than 500 beds, each of these hospitals likely has 50,000 medical devices that could be subject to security breaches. The number of devices across North America that are subject to hacking is likely measured in the ten of millions.

While it is clear that a hacker who hijacks one of these devices could easily place a patient at risk, there is even a wider risk that is only now being discussed within the healthcare industry. Because each of these individual devices is connected to the hospital's IT infrastructure and also to the Internet, a hacker could, in theory, target an individual device in order to gain control of the entire network to gain access to the hospital or clinic's entire network. The hacker could then get access to most of the other devises and other equipment connected to the network and even access the entire corporate database, which holds patient records, credit card information, security numbers, etc.

Introduction to Optium Cyber Systems, Inc.

Optium Cyber Systems, Inc. is a new entrant into the world of cyber risk solutions.

The Company plans to specialize in the healthcare industry due to the management team's specific experience and due to the large market opportunity that exists. However, management also points out that its cyber threat solutions can be applied to almost any industry.

Optium Cyber is headquartered in the Houston, Texas area and trades on the over-the-counter market under the symbol OCSY.

The Company has developed a specialized process to assist businesses in preventing cyber security threats. The Company specializes in analyzing and identifying security vulnerabilities. After a thorough assessment is performed, specific recommendations to address the vulnerabilities are offered to the client company. This allows the healthcare organization to better protect critical IT infrastructures.

The Company's main process is as follows:

Threat Detection - The first step of an engagement with Optium Cyber will involve a very thorough examination of the entire IT infrastructure of the client. An emphasis is placed on identifying the most vulnerable areas for hacker attack and on which areas of the IT infrastructure if attacked would cause the most damage to the client's organization. Much of this threat detection task involves the installation of very specialized equipment at the client's location. This equipment then scans the network for at least several days in order to develop and overall threat detection profile. While this equipment gathers data, it can be remotely monitored by Optium Cyber personnel.

After this threat detection analysis is completed, the team then comes up with an action plan to mitigate the vulnerabilities.

> **Threat Mitigation** - After the assessment is completed, the team then turns toward designing a system to mitigate the identified vulnerabilities. Specific recommendations are made ranging from simply removing ultra-vulnerable devices and to installing new types of software tools that will alert IT managers when threats are detected.
>
> **Remediation** - One of the most important steps in any cyber security prevention program is remediation. Once an adequate system to detect security vulnerabilities is set up, a plan can be developed so that when threats are detected either a manual intervention or a software routine can be invoked in order to neutralize the threat and to prevent the threat from reoccurring.
>
> **Education** - It is a simple fact that hackers understand that computer users are human and are prone to making errors and that they often deviate from security policies. Hackers rely on these factors in order to gain access to vital information and to facilitate ramsonware attacks. Therefore, vital to any cyber security mitigation plan is a strong campaign to educate computer and network users on behaviors that might make it easier for hackers to gain entry to the systems. An important part of Optium Cyber's cyber risk solution is to thoroughly educate the client's employees to ensure that sound security practices are always followed.

The revenue model for an educational program involves usage fees where the Company will run periodic testing of the client e-mail network with reports that will identify the employees that either met or failed to meet the parameters of the outlined security program. Additionally, it is likely a monthly service subscription will be charged for both ongoing educational programs and for ongoing monitoring.

Optium Cyber's revenue model is to charge usage fees at each of the above outlined steps. The Company plans to generate income upon the completion of each of these tasks and upon completion to sign contracts with clients for monthly monitoring services. Additionally, revenues will be gained through add on services as the team becomes increasingly familiar with the clients IT infrastructure

Recent Progress at The Company

While Optium Cyber Systems is still a very new company, it is already begun to show successes in gaining new clients.

The Company recently announced it had entered into negotiations to license its analysis and monitoring platform to a company involved in the shipping industry. This would likely allow the Company to open up an additional revenue stream additive to the services outlined above. It appears the negotiations proved successful with the Optium Cyber announcing a $2.5 million licensing agreement to Mobile Security Agency, Inc. for use in the shipping industry.

Under the terms of the deal, Optium will allow Global Security to sublicense the technology to multiple players in the global shipping industry. It appears a $2.5 million fee will be paid to the company 90 days after the signing of the licensing agreement, which will be payable via the issuance of 10 million common shares of Global Security stock.

This young company has also recently announced it has been engaged by a large Texas hospital system to conduct vulnerability assessments of the internal information technology infrastructure. Management of the Company recently stated it expects the vulnerability assessment task to take only approximately one week and that completion could easily lead to an ongoing monitoring contract for the company.

Corporate Revenue Plan

While, as we stated above, Optium's marketplace extends well beyond the healthcare industry, we believe this Company can be successful even if it targets a single sector, such as healthcare.

Below is an analysis leading to a potential revenue model for the Company if it should have successes in the healthcare industry.

With just under 5,600 hospitals and other medical facilities in the United States, a 1% penetration rate would equal approximately 55 such facilities. If each facility generated only $20,000 in upfront revenues for the Company, which we believe is a conservative estimate, total initial usage fees would easily top $1 million.

By charging these facilities additional recurring monthly fees, which is very common and acceptable in the healthcare industry, Optium could easily generate an additional up to $10 million per year of revenues, based on only a 1% market share.

Combined with the upfront fees, we could envision an $11 million per year total revenue stream by the company based on this 1% share.

A potential revenue model based on the 1% and other market share percentages is outlined Figure Six.

Figure Six - A Large Revenue Opportunity Even With a Very Small Market share

US DOMESTIC					
# of US Domestic Medical Facilities [1]	5,564	5,564	5,564	5,564	5,564
Projected Market Penetration (Percentage)	**0.5%**	**1.0%**	**2.5%**	**5.0%**	**10.0%**
Market Penetration (# Installations) [2]	25	55	140	275	550
Estimated Usage Fees Generated Per Installation [3]	$20,000	$20,000	$20,000	$20,000	$20,000
Total Estimated Annual Usage Fees [4]	$500,000	$1,100,000	$2,800,000	$5,500,000	$11,000,000
Estimated Recurring Monthly Fee (Per Installation) [5]	$15,000	$15,000	$15,000	$15,000	$15,000
Total Estimated Annual Recurring Monthly Fees [6]	$4,500,000	$9,900,000	$25,200,000	$49,500,000	$99,000,000
Total Annual Gross Revenue [7]	$5,000,000	$11,000,000	$25,200,000	$55,000,000	$110,000,000

1 AHA Hospital Statistics – 2017 Fast Facts on US Hospitals
2 # US Domestic Medical Facilities X Projected Market Penetration - Percentage ~
3 Includes: Critical Vulnerability Assessments, Mitigation Consulting & Employee Education services
4 Market Penetration (# Installations) X Estimated Usage Fees Generated Per Installation
5 Includes: Monitoring Fees & Employee Education Programs
6 Market Penetration (# Installations) X Estimated Recurring Monthly Fees X 12 Months
7 Total Estimated Annual Usage Fees + Total Estimated Annual Recurring Monthly Fees

Share Structure and Prospects for the Future

There are approximately 4.9 million shares outstanding and 2.4 million shares in restricted status. Based on the current trading range, the total market capitalization for the Company is still well under $1 million.

While this is clearly a start up company, it appears the Company is targeting a very lucrative market sector. It is clear the healthcare industry is in desperate need of improved cyber security assessment and mitigation capabilities and this management team seems to have specific expertise in this area.

We also think it is exciting that we are already seeing some traction with contracts and that it appears likely additional news will be forthcoming.

We also like the fact there is very little convertible debt on the Company's balance sheet. This will likely prevent excessive dilution for the short-term and medium-term.

We believe it is also worth pointing out the Company's business model is not capital intensive and instead relies on proprietary technologies and knowledge of the corporate staff. This means that the Company will likely not have to raise large amounts of capital - which could result shareholder dilution - in order to meet its business targets moving forward.

We are looking forward to Optium Cyber making additional disclosures relative to its financials.

Based on our initial analysis, it appears and that that the share counts will be rather limited little to no dilution will be demonstrated.

MANAGEMENT TEAM

Optimum Cyber headed by a highly experienced management team with extensive experience in cyber threat detection and mitigation.

Below are the bios for the main team members:

GEORGE M. RUTHERFORD - PRESIDENT

George M. Rutherford, age 72, is a Security Solutions and Risk Management Specialist. He has over 40 years experience providing individuals, corporation and governments with security risk analysis and crisis response planning. From 1993 to 2001 Mr. Rutherford was the Chief Executive Officer and Managing Director of CPR Ltd. and was responsible for security of its mining operations in Asia and East Africa. Mr. Rutherford started his career serving with the US Navy from 1962 to 1970 with the Naval Special Operations Unit.

MICHAEL T. RUTHERFORD – CHIEF EXECUTIVE OFFICER

Michael Todd Rutherford, age 47, is an Information Technology professional with over 25 years of experience with a specialized focus on IT security. His work experience includes IT system development, operations and management for banking, mortgage lending, telecommunications, healthcare, and real estate companies. Mr. Rutherford was involved with software development initiatives for loan origination systems for Bank of America and Lomas Mortgage. He has served numerous systems management functions on Department of Defense research projects and in the last 15 years, Mr. Rutherford has been specializing in architecting, securing and operating healthcare information technology systems. He is currently Director of IT for an industry-leading medical software company.

Mr. Rutherford holds a degree in Information Systems Management from Southern Methodist University's Cox School of Business and is a member of the FBI InfraGard and the Health Information Management Systems Society.

DOUG A. BINENTI – CHIEF TECHNOLOGY OFFICER

Doug A. Binenti, age 48, is a Security Engineer with over 20 years experience in IT, specializing in providing security consultancy services to large corporations and governments. Past clients include Dell, AT&T, Clemson University and a number of Cisco partner organizations. Mr. Binenti has worked in research & development, premarketing and post marketing implementation and has experience in Cisco enterprise networking, security and unified communication architecture. His past clients include telecommunications, oil & gas, energy, hospitals and a number of governmental agencies.

Mr. Binenti is a United State Navy veteran and holds a degree in Computer Engineering and Mathematics from Clemson University. He also has completed multiple Cisco certifications and is a member of the FBI InfraGard.

Disclosures

We do not own these shares and have no plans to acquire, purchase, sell, trade or transfer these shares in any manner.

We have no association with anyone, or any group, with any plan to acquire, purchase, sell, trade or transfer these shares.

Any opinions we may offer about the Company are solely our own, and are made in reliance upon our rights under the First Amendment to the U.S. Constitution, and are provided solely for the general opinionated discussion of our readers. Our opinions should not be considered to be complete, precise, accurate, or current investment advice. Such information and the opinions expressed are subject to change without notice. Separate from the factual content of our articles about the Company, we may from time to time include our own opinions about the Company, its business, markets and opportunities.

The information used and statements of fact made have been obtained from sources considered reliable but we neither guarantee nor represent the completeness or accuracy. We did not make an independent investigation or inquiry as to the accuracy of any information published by the Company, or other firms. The author relied solely upon information published by the Company through its filings, press releases, presentations, and through its own internal due diligence for accuracy and completeness. Statements herein may contain forward-looking statements and are subject to significant risks and uncertainties affecting results.

This report or article is not intended as an offering, recommendation, or a solicitation of an offer to buy or sell the securities mentioned or discussed. This publication does not take into account the investment objectives, financial situation, or particular needs of any particular person. This publication does not provide all information material to an investor's decision about whether or not to make any investment. Any discussion of risks in this presentation is not a disclosure of all risks or a complete discussion of the risks mentioned. We are not registered as a securities broker-dealer or an investment adviser with FINRA, the U.S. Securities and Exchange Commission or with any state securities regulatory authority.

ALL INFORMATION IN THIS REPORT IS PROVIDED "AS IS" WITHOUT WARRANTIES, EXPRESSED OR IMPLIED, OR REPRESENTATIONS OF ANY KIND. TO THE FULLEST EXTENT PERMISSIBLE UNDER APPLICABLE LAW, TWO TRIANGLE CONSULTING GROUP, LLC WILL NOT BE LIABLE FOR THE QUALITY, ACCURACY, COMPLETENESS, RELIABILITY OR TIMELINESS OF THIS INFORMATION, OR FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL OR PUNITIVE DAMAGES THAT MAY ARISE OUT OF THE USE OF THIS INFORMATION BY YOU OR ANYONE ELSE (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOSS OF OPPORTUNITIES, TRADING LOSSES, AND DAMAGES THAT MAY RESULT FROM ANY INACCURACY OR INCOMPLETENESS OF THIS INFORMATION). TO THE FULLEST EXTENT PERMITTED BY LAW, TWO TRIANGLE CONSULTING GROUP, LLC WILL NOT BE LIABLE TO YOU OR ANYONE ELSE UNDER ANY TORT, CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCTS LIABILITY, OR OTHER THEORY WITH RESPECT TO THIS PRESENTATION OF INFORMATION.

Information, opinions, or recommendations contained in this report are submitted solely for informational purposes. The information used in statements of fact made has been obtained from sources considered reliable, but we neither guarantee nor represent their completeness or accuracy. Such information and the opinions expressed are subject to change without notice. This research report is not intended as an offering or a solicitation of any offer to buy or sell the securities mentioned or discussed. The firm, its principles, or the assigned analyst may or may not own or trade shares, options, or warrants of this covered Company. We have received compensation of $2,000 to cover out distribution and production of this report. If additional compensation is received, future version of the report will be updated to reflect this compensation. Global Small Caps Research, has not in the past received compensation for the production of previous reports. The party responsible for the production of this report owns no common stock and/or warrants in the subject Company, in any way, shape, or form. The views expressed in this research Company report accurately reflect the analyst's personal views about any or all of the subject securities or issuers referred to in this Company report, and no part of the analyst's or the firm's compensation was, or will be directly or indirectly related to the specific recommendation or views expressed in this report. Opinions expressed herein reflect the opinion of Global Small Caps Research and are subject to change without notice. We claim no responsibility to update the information contained in this report. Investors should consider the suitability of any particular investment based on their ability to accept certain levels of risk, and should not rely solely on this report for information pertaining to the Company covered. We can be contacted at info@globesmallcap.com.