2017

# Cyber Threat Intelligence Plan - Report

CYBER THREAT INTELLIGENCE PLAN

CHAD NELLEY

NELLEY CONSULTING | [Company address]

## CLIENT COMPANY OVERVIEW

HIC Med Tech is a mid-tier medical device manufacturer that is developing new technologies in the Health Informatics space, relying on dig data, machine learning and artificial intelligence technologies to develop next gen solutions. HIC MT has been described as an up and comer in the new IoT/IoE space and is operating in a highly competitive and crowded space. HIC employs 75 employees in North America and has manufacturing and fulfillment operations offshore and near shore in Mexico and Vietnam. HIC MT's Board and Executive team have commissioned Nelley Consulting to conduct a comprehensive Cyber Threat Intelligence Plan. This document represents this work and will result in specific cyber threat scenarios and prevention and remediation tactics that can be employed to better understand risks, threats and opportunities as they pertain to the Cyber component of their market protection and growth strategy.

## COMPETITIVE LANDSCAPE

The competitive landscape is crowded in US markets – HIC MT has over 8 direct competitors with corporate headquarters in the United States alone, 4 European based competitors and 3 Asian competitors all competing in the Global marketplace. The market cap opportunity for HIC MT and all competitors is stated at $4B for 2018 and growth projections to $10B by 2025. HIC MT is currently ranked global #5 in the space and comes in at a strong market position #4 in the US Market. Of the $4B Global Market for 2018, US revenues in this space are expected to be better than $2.4B or 60% of the global market share. HIC MT is looking to expand globally and is currently generating revenues in the $250M – 500M range and sees a large growth opportunity in both Asia and the Latin America Markets.

HIC MT sees particularly large opportunities for advancement of global market share in the developing nations of Asia including Malaysia, India, Japan and China. Nelley Consulting has identified significant risk in entering both China and Malaysia, especially from a cyber risk standpoint. The competitive landscape is further complicated by the fact that HIC MT is also amidst a major contracting and procurement arrangement with the United States Government to implement its technologies across Military and Civilian agencies. This proposed contract for services and delivery through the GAO has a year 1 value of $150M alone, which would represent a nearly 30% revenue growth potential for the company on 1 deal, with guaranteed follow-on revenue in years 2-6 of the contract. The total deal value over the next 6 years could be as high as $700M. This increases the likely hood of nation state threats and also brings with it additional scrutiny from local government policing agencies.

Because HIC MT began marketing services and sourcing manufacturing and vendor relations in these regions, prior to bringing Nelley Consulting onboard, we fear that in region competitors may be operating covertly to infiltrate and abscond with critical IP. While our concerns are minimal with regards to US and European market players at this time, Nelley Consulting believes the risk landscape in certain markets within Asia may present a number of cyber challenges in the risk landscape.

## MARKET CONDITIONS

Current market conditions suggest that there will be a strong growth surge over the next 3-5 years in this space and that critical IP and R&D information will have a high black market value, especially for spurious and nefarious operatives in unregulated countries that may look to develop carbon copy

versions of our technology, faster and more cost effectively. Because first mover advantage is so critical to amassing large swaths of market share in the first 18-36 months of a product release and lifecycle, it is critical that HIC MT shore up all of its IP and R&D assets and protect them from Cyber espionage competitive operations and operatives, whomever they may be. For this purpose, Nelley Consulting recommends the following activities to better understand our cyber intelligence position.

## THREAT LANDSCAPE & ENVIRONMENT

**Organized Crime and Cyber-Crime**
Organized crime is primarily about the pursuit of profit and can be understood in terms as a continuation of business by criminal means. Criminal organizations are not the only players in illicit markets, but they are often the most important, not least because of the added "competitiveness" that is provided by the threat of organized violence. Moreover, criminal organizations tend to be exceptionally good at environmental scanning in the search for new criminal enterprises and activities. In this context, the Internet and the continuing growth of electronic commerce offer enormous new opportunities.

Criminal organizations have increasingly hired financial specialists to conduct their money laundering transactions. This adds an extra layer of insulation while utilizing legal and financial experts knowledgeable about the layering of financial transactions and the availability of safe havens in offshore financial jurisdictions. Similarly, organized crime does not need to develop technical expertise about the Internet; it can hire those in the intruder community who do have the expertise, ensuring through a mixture of rewards and threats that they carry out their assigned tasks effectively and efficiently. Organized crime groups typically have a home base in nations that provide safe havens from which they conduct their transnational operations, such as various kinds of trafficking activities. In effect, this provides an added degree of protection against law enforcement and allows them to operate with minimal risk. The inherently transnational nature of the Internet fits perfectly into this model of activity and the effort to maximize profits within an acceptable degree of risk. In the virtual world there are no borders (a characteristics that makes it very attractive for criminal activity); yet when it comes to policing this virtual world borders and national jurisdictions loom large – making large-scale investigation slow and tedious at best, and impossible at worst.

The Internet itself provides opportunities for various kinds of theft. Online thieves can rob online banks or illicitly gain access to intellectual property. The Internet offers new means of committing old crimes such as fraud, and offers new vulnerabilities relating to communications and data that provide attractive targets for extortion, a crime that has always been a staple of organized crime. (Williams, CERT)

To this extent, organized crime outfits operating in and throughout Asia, Russia and Latin America pose significant threat to HIC MT's competitive advantage. HIC MT must develop strategies and implement protective technologies to understand and protect against organized crime operatives attempting to gain access for exfiltration of IP and critical data that can be sold on the black market and dark web. The international component makes legal operations and actions highly suspect and unlikely to warrant any action by hostile governments who do not abide by the legal standards that we have established in the North American and EU markets.

**Nation State Sponsored Cyber Hacking:**

Unlike their criminal world counterparts, nationally backed hackers are frequently part of a country's military or security and intelligence organizations. As the cost of new computer technologies continues to plummet, the bar for nations to enter the cyber realm has lowered considerably leading to an asymmetry that favors the adversary. Cyberspace is seen as an equalizing force, and nations at odds with the U.S. and its allies view cyber operations as an avenue to overwhelm U.S. kinetic military capabilities. Due to the Department of Defense's (DoD) reliance on highly networked communications and weapons systems, a cyber attack is seen as a way of turning the military's greatest asset into a weakness. Beyond military operations, nation state cyberspace organizations perform classic espionage and intelligence operations. Some of these groups are large operations such as the Chinese People's Liberation Army Unit 61398—a secret intelligence gathering organization that has been connected to extensive cyber espionage operations. Nation state hackers work for their respective governments and, as such, are not driven by money but by duty and patriotism. Intelligence organizations seek to steal a range of data and information from U.S. government agencies, defense, and commercial contractors. Targeted data includes diplomatic correspondence from the U.S. State Department, private information about active and former government employees, and unclassified White House email correspondence.

**Advanced Persistent Threats**

Nation state and organized criminal hacking groups present a major challenge to HIC MT network security. These groups seek specific data and are willing to devote considerable time and effort to identify, locate, and access it. IT security organizations refer to these types of attackers as advanced persistent threats (APTs) due to their patience, persistence and capabilities. An APT is an attack in which an unauthorized person gains access to a network and stays there undetected for a long time. They are persistent because they use a command and control system to monitor target networks constantly and extract data, and they are a threat because they are carried out by highly skilled adversaries.

Characteristics of an APT include

> ***The attack is customized for each specific target. This can include the development of specialized software tools and intrusion methods focused on slipping past the target's network defenses.***
>
> ***Extensive research is conducted on the target prior to the attack. This consists of mapping out network topologies, domains, servers, and internal IP addresses. The more the attackers learn about the target's network, the greater their chances of success.***
>
> ***Patience and stealth are key features. A typical APT operation occurs cautiously over a period of weeks or months so as not to draw attention to the operation.***
>
> ***Once inside a system, the attackers will steal user credentials to gain further entry into the network. They will then escalate their privileges to access high-value data.***
>
> ***This is espionage. Unlike a criminal operation, which seeks to access money or fungible data quickly, such as credit card numbers, an APT seeks selected information for intelligence purposes. It may steal data or plant software to spy on internal communications.***
>
> ***After a network has been breached, APT operations are coordinated remotely via "command***

***and control" communications between the attackers and infiltrated systems.***

***Once target information has been located, it is modified or exfiltrated. This is commonly done by collecting data, archiving it, and then compressing and encrypting the archive. This hides the archive's content from deep packet inspection and data loss prevention methods. The stolen data is then broken up into data packets and then camouflaged as normal traffic with specialized software tools.***

***APTs are selective. While organized criminal hackers may infiltrate a network in a similar manner, they usually seek a wider range of targets in an organization, such as financial data or intellectual property. APTs often target key individuals or parts of organizations, looking for sensitive high-level operational or diplomatic data. (HPE Whitepaper)***

Because APT's are the primary tools of both organized crime units and government sponsored hacking tactics into environments, it will be critical to implement technologies specifically designed and engineered to thwart the APT phenomena at the perimeter and at the end point.

**Key Players & Adversaries for Hire (By the competition)**

Chinese cyber operations have typically been economically driven, often with a pure profit motive. Several top technology, aerospace, and defense companies have been breached by Chinese state-sponsored hackers, often in what appears to be an effort to steal intellectual property and identities. China's approach follows the same guiding philosophy the Chinese Army uses: throw as many people at the problem as possible, regardless of talent or training, and eventually you're bound to get something. These groups include Deep Panda, Putter Panda/PLA Unit 61398, Hidden Lynx, APT1/Comment Crew, Axiom, and many more.

Russian cyber operations enjoy a unique distinction from the other groups because they are more broadly used to collect intelligence, and like Chinese hackers are also involved in profit-motivated cyber crime. The Russians also have a history of aggressive offensive operations such as the Estonian cyber attacks of 2007 that swamped websites of Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's disagreement with Russia about the relocation of a statue, and more recent cyber attacks directed at Poland.

Unlike Chinese counterparts, Russian hackers also like to spread ideological influence, a discipline known as "Information Operations" within the intelligence community. This includes "troll farms" staffed with hundreds whose job is to spread ideas and cause the appearance of consensus across online forums and social media. Russian state-sponsored cyber efforts are also unique in that they are known to provide training and mercenary-style hacker-for-hire services to other countries -- possibly even North Korea's Bureau 121 and Iran's IRGC.

Some notorious non-state actors have been working hard to reach levels of sophistication similar to these state-sponsored groups. There have been many reports of mysteriously unattributed and extremely sophisticated hacker recruiting drives across the deep web. (Dark Reading)

## OPPORTUNITIES TO DISRUPT – DEFENSIVE & OFFENSIVE MEASURES

Because our operations are based and headquartered in the United States of America, we are limited in our ability to execute offensive tactics in the event we find through our Cyber Intelligence operations that we are being targeted or are actually under cyber attack. So, for purposes of this plan, all of our methodologies will be based on defensive measure and best practices. However, I will be recommending the development of a "Red Team" specifically established to perpetrate offensive tactics against the environment to test against security implements we put in place.

Fortunately, these attacks are detectable and preventable. The business and cyber operations group must make use of layered defenses comprised of human-monitored intrusion detection with behavioral analysis integrated with routine security testing, predictive threat intelligence, and education in order to stay secure.

**How our offshore threats and competitors will likely commission attacks:**

We have reason to believe that our competitors in markets like China, Russia, North Korea, India, Pakistan and the Middle East will incorporate any number of the tactics outlined above – contracting individual and organized crime groups for hacking activities, using tools and tactics that include prolific leveraging of APT techniques. Further we believe that given our impending government contract opportunity will make us a greater target for exploit and that the attempts against our measures will be constant, often and relentless as our competitors and potential enemies of State will also target our environments for exploit.

## RECOMMENDATIONS

The primary objective of this plan is to put forth a set of recommendations to ensure that HIC MT has an appropriate plan in place to conduct active threat intelligence operations that incorporates both human resources and technical resources. Here are my recommendations for immediate implementation over the next 6-18 months and ideally in place prior to conducting any further business operations in geographies outside of the US and Canada borders.

1. Formalization of a CISO role, reporting directly to the CEO
2. Formulation of a Cybersecurity Business Unit (3-5 Cyber Operatives)
3. Formulation of a Cyber Red Team (3-5 White Hat Hackers, Intel & Penetration Experts)
4. Mandated top down, employee training on current social engineering, spear phishing tactics and general cyber hygiene – Cyber is everyone's responsibility
5. Implementation of a robust toolset for active monitoring and protection of all electronic environments to include perimeter tools, end point solutions, encryption technologies and continuous monitoring technologies that leverage machine learning and AI to actively learn and protect these environments.
6. Implement regular policies and procedures that migrate and mature with cybercrime and cyber industry trends and that emphasize a need for constant vigil on Cyber Threat Intelligence monitoring, remediation and breach prevention.
7. Shift Board and Executive mindset to be proactively discussing and reviewing cyber operations for the organization.
8. Retain Nelley Consulting to continue work in establishing Cyber Threat Intelligence tactical model in tandem with identified CISO.
9. Year 1 Investments:

Headcount & HR Overheads – $2.5M
Systems, Technologies & CAPEX - $1.0M
Training & Services – $250K
Total Year 1 Investment – $3.75M
ROI = Government Deal Potential Yr1 = $150M, 6 yr Projected $700M; Yr1 ROI = 40x.
Terms of Govt Contract call for proper Cyber security & Intelligence Operations in place

**Process for Cyber Threat Intelligence Planning**

Another essential recommendation here-in is in a process to implement and build a constant vigilance and emphasis on Cyber Threat Intelligence Operations. Below is a sample diagram of one particular approach that Nelley Consulting would recommend as a method and approach:

## REFERENCES

Williams, CERT
https://docs.google.com/viewer?a=v&pid=forums&srcid=MDY4NDM1NzM3NzA2MjI3MjE2MjYBMDg2NjAxMzE4OTY0NTQxNDQ5NDYBalBnaGhjb3pPYzhKATAuMQEBdjI

http://h20195.www2.hpe.com/v2/getpdf.aspx/4AA6-6901ENW.pdf?ver=1.0

http://www.darkreading.com/vulnerabilities---threats/state-sponsored-cybercrime-a-growing-business-threat/a/d-id/1320555