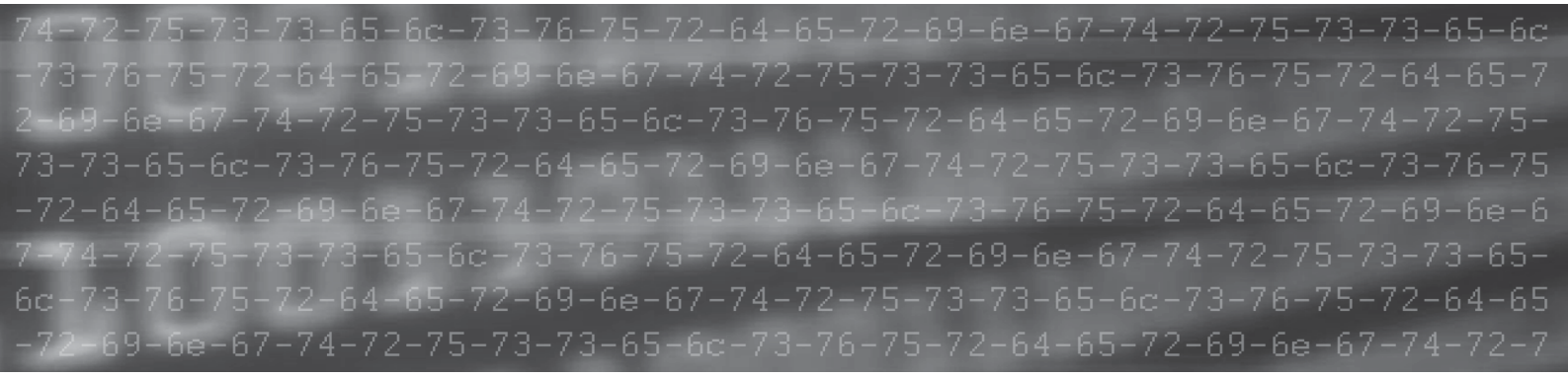
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat against the Danish healthcare sector



Threat Assessment Branch under the Centre for Cyber Security

July 2018

CENTRE FOR CYBER SECURITY

Threat assessment: The cyber threat against the Danish healthcare sector

This threat assessment outlines the cyber threats facing the Danish healthcare sector. The Danish healthcare sector is of vital importance to the functioning, stability and welfare of the Danish society. The purpose of this assessment is to inform the healthcare sector of the potential cyber threats in order to facilitate mitigation. This threat assessment could, for example, be included in the healthcare sector's risk assessment in relation to the Danish cyber and information security strategy.

Key assessment

- The threat from cyber espionage against the Danish healthcare sector is **VERY HIGH**. Some foreign states have an interest in conducting cyber espionage against the healthcare sector in order to steal information on research data and intellectual property.
- The threat from cyber crime is **VERY HIGH**. Cyber crime attacks may disrupt patient care and treatment.
- The threat from cyber activism is **LOW**. Due to the case-by-case nature of cyber activism, the threat from cyber activism against the healthcare sector may increase overnight.
- The threat from cyber terrorism is **LOW**. Even though militant extremists have expressed an interest in conducting cyber terrorism, they currently lack the capabilities to do so.
- Foreign states are less likely to launch destructive cyber attacks against critical infrastructure in Denmark, including the healthcare sector. However, the Danish healthcare sector may become a collateral victim of a destructive cyber attack against targets outside of Denmark.

Introduction

This threat assessment gives an overview of the overall cyber threat against the Danish healthcare sector. The basis for the assessment is primarily Nordic and international examples of cyber attacks against the healthcare sector, which are analysed together with knowledge of the Danish healthcare sector and the threat actors' capabilities and intentions.

The healthcare sector supports functions vital to Danish society. Cyber attacks against the Danish healthcare sector are thus a risk to the functioning, stability and welfare of Danish society, at worst resulting in loss of life, personal injury and loss of public confidence in the healthcare sector. Consequently, it is essential that the healthcare sector is equipped to handle the cyber threat, ensuring instant and stable access to healthcare services without disruption in patient care and treatment.

The healthcare sector consists of several elements with different characteristics and vulnerabilities. This assessment focuses on the cyber threat against the healthcare sector as a whole, from treatment centres such as hospitals, medical practices and dentists to medical suppliers and manufacturers, including the pharmaceutical industry, life science industry, medico industry and providers of IT solutions to treatment centres. Healthcare research organizations, both private and public, as well as public health authorities such as the Danish Ministry of Health are also included as part of the healthcare sector.

In general, this threat assessment provides an overview of the threats against the sector as a whole, only rarely distinguishing between the different components of the sector.

What are cyber threats?
The DDIS Centre for Cyber Security (CFCS) defines cyber threats as threats from cyber attacks in which an actor tries to disrupt or gain unauthorized access to data, systems, digital networks or digital services. Use of the Internet for other purposes that may have negative impacts on society such as online sale of illegal medicine is not included in our definition of cyber threats.

Cyber threats are multi-faceted. In this assessment, we describe and assess activities aimed at cyber espionage, cyber crime, cyber activism or cyber terrorism, focusing on the end goal of these cyber attacks. Also, we assess the potential threat from destructive cyber attacks.

The threat levels in this assessment are based on an analysis of the actors' intention and cyber capabilities. An actor's capabilities can be understood as its available human and material resources, ranging from skilled hackers, malware developers and information on targets that is useful for social engineering to IT infrastructure, time and funds. Thus, the scope of an actor's cyber capabilities depends on available resources as well as the actor's ability to exploit them.

This threat assessment is based on the current threat picture and operates with a warning time frame of 0-2 years. Cyber threats are dynamic and the threat can therefore quickly change, both on a general level and in relation to individual authorities and private companies. The threat and probability levels applied in this assessment are defined at the end of the report.

Cyber espionage

In general, Danish public authorities and private companies are continuously facing cyber espionage attempts, mainly by state-sponsored actors. CFCS assess that the threat from cyber espionage against the Danish healthcare sector is also **VERY HIGH**.

CFCS assess it highly likely that foreign states have the intent and capability to commit cyber espionage against the Danish healthcare sector, targeting, in particular, the units with access to research data or valuable intellectual property as well as large quantities of patient data.

Cyber espionage against, for example, intellectual property in the healthcare sector poses an economic threat to Denmark and may undermine Danish interests. Theft of sensitive patient data may cause the public to lose confidence in the sector's ability to securely and safely handle patient data, potentially jeopardizing the continued digitization of patient treatment.

Research data and intellectual property may be exploited by foreign states to strengthen their national healthcare industry or research and to develop or improve their own healthcare system. State-sponsored hacker groups have been known to target the healthcare sector abroad to steal intellectual property, including intellectual property belonging to private companies involved in bio chemistry, bio technology and pharmaceuticals.

In addition, sensitive information stolen from the healthcare sector may prove valuable to foreign intelligence services. Cyber espionage may provide a foreign state with access to confidential information, allowing it to extort people in prominent positions.

An incident in Norway illustrates that cyber espionage against the healthcare sector is a reality. In January 2018, it was revealed that hackers had breached a IT system at a hospital, gaining access to large amounts of data. The attack was directed at South-Eastern Norway Regional Healthcare Authority (Helse Sør-Øst). The CEO of the South-Eastern Norway Regional Healthcare Authority stated that the hackers had targeted an IT system operated locally by the affected hospital. Subsequently, it was decided that hospitals are no longer allowed to operate their own servers and that Sykehuspartner HF, a subsidiary company under the South-Eastern Norway regional Healthcare Authority, is to take over server operations. The CEO also stated that the hackers had performed vulnerability scans ahead of the attack and that once they had gained access to the systems, they tried to keep activity to a minimum to avoid detection. In its annual risk assessment '*Fokus 2018*', the Norwegian intelligence service described the cyber attack as an intelligence-related activity. The Norwegian intelligence service also used the attack to emphasize the vulnerability of critical infrastructure to cyber attacks.

The threat from cyber espionage against certain segments of the healthcare sector depends on the type and amount of data held by the target. However, the Danish healthcare system is highly digitized and interconnected, allowing an actor to exploit vulnerabilities in one part of the sector to gain access to other targets in the sector.

Cyber espionage against the healthcare sector may also include cyber attacks against suppliers. Hackers can either direct attacks at suppliers in a bid to gain access to information on their end targets or use the attacks to steal client data from the suppliers. Many Danish hospitals allow their suppliers to use a remote access connection to the products or systems they support, which a hacker could potentially use to gain access to the hospital's other systems.

The supplier or manufacturer of medico equipment may also be the end target. If that is the case, hackers may try to compromise treatment centres such as hospitals in a bid to use them as launch pads for gaining access to suppliers or manufacturers.

Cyber espionage can also support other types of cyber attacks and threats, for instance, a foreign state may want to detect vulnerabilities in the healthcare sector in the event of a potential future conflict. This information may be used ahead of a destructive cyber attack, especially if the cyber espionage provides access to critical systems or information relevant to the destructive attack. Cyber espionage

may also give an opponent access to sensitive information that may subsequently be leaked in a bid to sway public opinion. Consequently, a private company or public authority that has already been compromised is more vulnerable to destructive cyber attacks or hack and leak attacks.

Cyber crime

The threat from cyber crime against the Danish healthcare sector is **VERY HIGH**.

The healthcare sector is targeted by cyber criminals due to the potential for financial gain by means of extortion and data theft. Healthcare facilities offering patient treatment are very dependent on their systems and data in order to perform time-sensitive, lifesaving work, making them vulnerable to attempts of ransomware extortion. Also, some parts of the sector have previously been characterised by outdated technology, vulnerable systems and weak cyber security infrastructure, which have rendered them particularly vulnerable to cyber attacks. In addition, the healthcare sector is exposed to random non-sector specific attacks.

Ransomware attack
Like other types of malware, ransomware is often spread via phishing mails or via infected websites. Ransomware renders the victim's computer or systems unavailable and the attacker demands a ransom fee in exchange for making them available again. There are many types of ransomware. Targeted ransomware attacks, for instance, are aimed at compromising administrative networks in specific private companies and public authorities. The healthcare sector abroad, in particular, has fallen victim to targeted ransomware attack resulting in payment of substantial ransoms.

Ransomware may disrupt patient treatment
The healthcare sector worldwide is no stranger to ransomware attacks. Cyber criminals may be motivated by the idea that the sector is more willing to pay ransom as hospitals, in particular, provide time-sensitive critical services.

WannaCry is one of the largest ransomware attacks to date to also hit the healthcare sector abroad and, less so, in Denmark. The impact of WannaCry abroad was particularly serious, illustrating that ransomware may disrupt critical infrastructure. The British healthcare sector, in particular, was affected, leading to thousands of cancelled appointments, including potential urgent cancer-related appointments. The WannaCry attack illustrated how a cyber attack is able to directly affect patient treatment and care. Also, WannaCry is an example of cyber crime widely believed to have been carried out by a state-sponsored actor.

However, in addition to ransomware attacks targeting hospitals and medical practices, attacks against companies that supply medicine to hospitals or medical practices could also impact patient care. Illustrative of this was the so-called NotPetya attack – a destructive cyber attack disguised as a ransomware attack – which disrupted the manufacturing operations of pharmaceutical company Merck & Co. Although hospitals keep emergency stocks of medicine, large-scale attacks against pharmaceutical companies may still jeopardize their supply chains.

Cyber attacks against pharmaceutical companies that cause disruption to production or result in substantial financial losses may also adversely affect the Danish healthcare sector as the pharmaceutical companies may be forced to hike up the price of their drugs. Pharmaceutical companies determine the list price for their drugs and can change the prices every 14th day, when the companies report price changes to the Danish Medicines Agency

A new trend seems to have emerged among cyber criminals behind ransomware attacks: using remote access connections to install ransomware on systems. The hackers steal or use brute force attacks to crack the password of a supplier and then use these to access the healthcare organization's systems by logging in on its remote access portal. Once they have gained access, the hackers are able to install ransomware on the breached systems. Illustrative of this is the January 2018 ransomware attack against US hospital Hancock Health that involved hackers apparently gaining access to the hospital systems by using the hospital's remote access portal. Allegedly, the hackers had also been able to destroy the hospital backups via this remote access. Later that month, US company Allscripts, a provider of electronic healthcare technology solutions, was also compromised by a ransomware attack via remote access hacking.

Brute force attack
An attack in which the attacker, typically using automated software, run a large number of password combinations and login names until the correct combination is found, enabling the attacker to access digital services and systems.

Cyber criminals target healthcare sector data

CFCS assess that cyber criminals have the intent and capability to commit data theft against the Danish healthcare sector. The sector holds large amounts of data that criminals may sell or exploit for extortion, including patient or research data or information on equipment or products used by the sector.

Some cyber criminals try to blackmail organizations by threatening to leak hacked patient data. One group in particular, often referring to itself as "The Dark Overlord", has extorted healthcare providers across the United States and the United Kingdom. Danish nationals have also been affected by similar attacks abroad. Criminals hacked and leaked photos of patients, including Danish ones, of a foreign plastic surgery clinic. Danish health clinics or treatment centres may also be the targets of hacking or extortion attempts by cyber criminals.

Also, there is a risk that cyber criminals may try to exploit the new General Data Protection Regulation in order to extort public authorities and private companies, threatening to hack the organization unless ransom is paid, or demanding ransom in exchange for not leaking stolen data and not revealing that the company has been compromised.

The healthcare sector also includes services paid for by the patient, leaving the patients open to credit card information theft. In certain cases, personal data may also be exploited for identity theft or insurance fraud purposes. However, insurance fraud is not as widespread in Denmark as it is in the

United States, where patients rely on healthcare insurance, and where the market for sale of healthcare data is larger.

Cyber criminals may also steal information from the healthcare sector in order to sell these. Targeted information could be research data or intellectual property such as information on formulas for next-generation drugs and information on equipment or software used in the healthcare sector.

In 2016, a hacker stole the source code to software developed by PilotFish Technology for the integration of various medical devices. Initially, the hacker put the stolen code up for sale and subsequently tried to extort PilotFish Technology by threatening to leak the stolen data. The hacker also claimed that he could access all of the company's clients' electronic health records by installing a backdoor into updates to the software from PilotFish Technology. As the Danish healthcare sector extensively uses suppliers of software solutions, a similar attack may occur in Denmark, illustrating the importance of incorporating cyber security measures when selecting suppliers and forging agreements.

A group known as Orange Worm is another example of a hacker group that have targeted the health care sector, possibly in order to steal information for financial gain. According to IT security companies, Orangeworm has specifically targeted the healthcare sector, including hospitals and their suppliers, and has successfully been able to spread malware to medical scanning equipment like X-ray and MRI machines.

Cyber criminals may also launch data theft campaigns in connection with stock speculations. Given the major costs associated with research and development of new products within the pharmaceutical and biotech industry, one single successful or failed product may have a significant impact on company share prices. Consequently, information on trial products and whether their clinical trial phases are successful could potentially be exploited for stock market speculation.

Rising trend of cryptocurrency mining malware

Cryptocurrency mining malware is gaining traction among cyber criminals who use the malware to steal the computing power of victim devices to mine cryptocurrencies such as Bitcoins. No industry or sector is immune to the risk of cryptocurrency mining malware, including the healthcare sector.

Cryptocurrency mining is a resource-intensive task that typically requires a massive amount of computing power from the infected devices, potentially causing operational disruptions. Medical devices and software may be particularly sensitive to cryptocurrency mining malware, as medical equipment is usually designed to operate under specific conditions, raising the risk of causing collateral damage.

Cryptocurrency mining attacks against the healthcare sector present a problem, even if they do not cause operational disruptions. The malware may have adverse impact on the devices it infects or consume so many computational resources that it warrants a major investigation by the IT department. In addition, the process of removing the malware may be time-consuming and arduous, rendering the infected systems temporarily unavailable.

Cyber criminals may subsequently use the malware and access to the targeted system for other purposes besides cryptocurrency mining or to cause collateral damage. For instance, in September 2017, a hospital in Tennessee experienced a security incident in which its electronic medical record system was infected with cryptocurrency mining malware, forcing the hospital to inform more than 20,000 patients that their medical records might have been compromised.

DDoS attacks seen as less serious threat

Some cyber criminals use Distributed Denial of Service (DDoS) attacks as a means of extortion, threatening to overload website servers or other services unless ransom is paid. In some cases, the attackers are not actually capable of launching a DDoS attack but hope that the mere threat from a DDoS attack scares the target enough to pay the ransom.

In our assessment, it is difficult to cause serious disruptions to healthcare services by means of DDoS attacks. Critical patient treatment services are connected to internal networks, making it difficult for cyber criminals to target these services with DDoS attacks.

DDoS attacks
Distributed Denial of Service (DDoS) is a cyber attack in which the attacker exploits compromised devices to generate an overwhelming amount of data traffic against a website (web server) or network, rendering it unusable.

However, cyber criminals may cause inconvenience by rendering the website of a local medical practice unavailable. However, CFCS do not believe that cyber criminals will be able to launch DDoS attacks that have the propensity to overall affect critical healthcare services.

Business Email Compromise (BEC) scams still a challenge

So-called BEC scams are aimed at defrauding companies and authorities of money by sending false requests for wire transfers purporting to be from a senior corporate executive in an attempt to trick employees into transferring funds. This type of scam is often called CEO fraud or fake president tricks.

The false emails are often sent from overseas email accounts, but hackers have also been known to use compromised email accounts belonging to senior corporate executives to send fake emails, increasing the likelihood of a successful fraud attempt. CFCS have information that the Danish healthcare sector, like the rest of Denmark is the frequent target of sophisticated BEC scams attempts.

Cyber activism

Cyber activists use cyber attacks as a tool to communicate an ideological or political statement. Cyber activists may target individuals, organizations or companies which they deem opponents to their cause.

The threat from cyber activism against the Danish healthcare sector is **LOW**. However, the threat level may suddenly increase, if the Danish healthcare sector becomes embroiled in single issues that land it in the crosshairs of cyber activists.

Cyber activists have some capacity to target public healthcare websites with DDoS attacks or so-called defacement attacks in which a hacked website may be defaced with a political message. However, CFCS assess that such attacks would have little effect on critical healthcare services. In addition, some cyber activists have even spoken against attacks on the healthcare sector as they jeopardize patient safety, and globally, cyber activist attacks on the healthcare sector have been scarce.

A popular tactic among cyber activists is the hack and leak of data in a bid to put the victim in a bad light. Healthcare data may become the target of such attacks as this kind of information is sensitive and could attract attention. In addition, cyber activists may use information harvested from the healthcare sector to bolster their message, as was the case when a hacker gained access to a system used to book appointments in the UK healthcare system to support his criticism of the healthcare sector's IT security.

As cyber activists use cyber attacks to communicate a message, it is vital that the intended recipient understands what message they are trying to convey. Thus, cyber activist attacks are often linked to specific high-profile media cases.

In this vein, activists seized control of investor Martin Shkreli's social media accounts following allegations that he had hiked up the price of life-saving drugs. Another example illustrating the importance of media to cyber activists is an operation called #OpJustina launched by the activist group Anonymous. In 2014, members of Anonymous launched an attack on Boston Children's Hospital over a case involving 15-year-old Justina Pelletier, who had been admitted against her parents' will. She had been hospitalized for over a year when the attacks occurred.

Cyber activists thus adapt their methods to the specific message they want to convey, and they try to exploit the media coverage that will promote their cause the best.

Cyber terrorism

The threat from cyber terrorism against the Danish healthcare sector is **LOW**.

CFCS assess that at present militant extremists lack the capability to launch cyber attacks with the same serious potential as more conventional terrorist attacks.

However, the ability to respond to a terrorist attack rests on a robust healthcare system. Thus, terrorists may try to bolster the effect of a conventional terrorist attack by launching parallel simple cyber attacks against the healthcare sector.

TDoS
Telephony Denial of Service (TDoS) is a cyber attack that targets telephone networks by flooding the system with bogus calls, effectively tying up the system and preventing legitimate calls from getting through. For example, the attacker may infect a large number of mobile phones with malware, causing them to flood a specific number with calls.

Thus, it is important ensure that the Danish health care sectors emergency response is resilient and able to handle cyberattacks. If cyber security is not made a top priority, simple cyber attacks may have a negative impact on the healthcare preparedness, as was the case in the United States when, in 2016, an 18-year-old hacker launched a TDoS attack against several emergency call centres. The teen wrote and shared a piece of code that caused target iPhones to continually dial 911 emergency services. He had not, however, anticipated the mass dissemination of the link. The call volumes shut down several emergency call centres. The feature exploited in the incident has subsequently been removed from iPhone.

Destructive cyber attacks

A number of countries have access to destructive cyber capabilities that could potentially be used against critical infrastructure such as the healthcare sector.

CFCS assess it less likely that foreign states will launch destructive cyber attacks against critical infrastructure in Denmark, including the healthcare sector. The threat may increase, though, if a political or military conflict in which Denmark is involved escalates.

Destructive cyber attacks
CFCS define destructive cyber attacks as attacks where the expected result is death, personal injury, property damage, or destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

At present, destructive cyber attacks against targets outside of Denmark may have negative spillover effects on Danish companies and public authorities, especially on those operating in conflict areas where foreign states or organized hacker groups with strong cyber capabilities have vested interests to defend, for example in parts of Eastern Europe, the Middle East and Southeast Asia.

However, if foreign states become willing to use destructive cyber attacks against critical infrastructure in Denmark, such attacks could have a devastating impact on the healthcare sector. In addition,

destructive cyber attacks launched against other critical sectors such as the energy sector could have a negative spillover effect on the healthcare sector.

Cyberespionage often facilitates destructive cyber attacks. Compromised organizations are thus more vulnerable to the potential threat from destructive cyber attacks.

Healthcare sector trends impacting the cyber threat

There are a number of factors that can influence the cyber security of the healthcare sector. The healthcare sector is vulnerable to cyber attacks facilitated by employees who deliberately or negligently disregard cyber security. In order to provide treatment, the healthcare sector has become increasingly dependent on constantly evolving technical medical equipment and IT systems. In addition, technological development in the medical field will entail changes in treatment procedures.

Patients put above IT security

Many cyber attacks are successful because employees often unwittingly give hackers access, for instance by downloading files from phishing emails or by using easy-to-crack passwords. Doctors, nurses and other healthcare professionals work in a time-sensitive environment where patient care takes precedence over cyber security. Consequently, staff can be willing to overlook cyber security measures if they believe these practices hamper patient care or if they can save time by bypassing the procedures. It is however important that everyone in the healthcare sector is focused on cyber security as successful cyber attacks could affect patient treatment.

Patient treatment at home

Telemedicine has become a popular tool for healthcare facilities as it allows the use of digital media such as email, video, pictures and sound over the Internet to provide healthcare from a distance. Telemedicine reduces hospital admission rates and ambulance transportation, allowing doctors to manage more patients with fewer resources. However, telehealth also adds a new dimension to cyber threats as it may provide hackers with new ways to gain access to treatment facility networks. In addition, telemedicine solutions are potentially vulnerable to DDoS or TDoS attacks. Moreover, patients run the risk of their telehealth systems being infected by malware. Such malware may potentially spread to the treatment facility networks, for example if malware has been installed at the computer of a patient communicating with his/her doctor, the malware may spread to the doctor’s computer and email contacts.

Internet of Things at hospitals

The "Internet of Things" (IoT) is the interconnection via the Internet of electronic devices, a trend that has also spread to hospitals, though the electronic devices are usually connected to the hospitals’ internal networks. In addition, the devices are often equipped with automatic data collection sensors. The IoT-connected devices carry a lot of advantages as they may provide doctors with additional patient information, facilitate data exchange and help keep a sterile environment, because the doctors have less need to physically touch the devices.

However, a lot of these devices have no built-in cyber security features possibly as a result of the manufacturer spending more time working on diminishing the size of the device, extending battery

lifespan or improving manufacturer support services. Not only may the poor security in IoT-connected devices provide hackers with access, the wireless data sharing between the devices may also make it easier for hackers to steal non-encrypted data. The fact that medical devices are increasingly interconnected could potentially jeopardize patient security.

Security experts have repeatedly demonstrated how compromised medical equipment constitutes a patient safety risk. For example, researchers have shown how a hacker could gain access to a drug pump, allowing them to administer dosage levels

The introduction of IoT-connected devices at hospitals and other treatment facilities has presented their IT departments with a new challenge. Though many IoT-connected devices are easy to activate, they require extensive security protocols. There is also a risk that employees at clinics and hospitals may purchase or bring their own IoT-connected devices which are installed without involving the IT department. Consequently, it is vital to pre-empt the risk that hackers use these devices as platforms for access to the healthcare sector.

Threat levels

The Danish Defence Intelligence Service (DDIS) uses the following threat levels, ranging from **none** to **very high**.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.

Below is the scale of probability the DDIS applies