Information Risk Management: The NHS & WannaCry cyber-attack

SHAKIL IBNE AHSAN, 21055097

1.0 Abstract

NHS continues to experience Cyberattacks, and precisely large-scale attacks have hit many hospitals in the last couple of years. The value of healthcare providers' sensitive information of their clients makes them a striking target for cybercriminals looking to make cash from ransom payments or fraud. By using risk management frameworks, improvements can be completed to its functioning model, safeguarding sensitive user data is kept secure. After analyzing previous incidents, threat actors, and societies, the solution will be identified, and after this, the threat will be measured using a combination of FAIR and the ISO series.

2.0 Introduction

The healthcare industry is uptight with jeopardy today regarding information risk management. According to an NHS report, 61,032,314 Patients Registered at GP practices in England as of 1 August 2021 (NHS Digital, 2021). Confidential patient information identifies the patient and includes their medical condition or treatment. In addition, with each patient on the NHS digital platform, there comes new data, family history, very personal history, emails, addresses, and possible credit card information. These details are very sensitive and have to be measured for potential risk. There is utterly the possibility of them being hacked, whether via an external adversary or an internal threat (William Smart, 2018).

This report will explore a relevant incident to the NHS healthcare system through risk analysis and how it is seen to operate. It will also seek the control measures for a future incident to determine if the company was prepared for an attack of this nature.

3.0 Incidents

On Friday, 12 May 2017, a global ransomware attack, recognized as WannaCry, invaded more than 200,000 computers in 100 countries. The attack predominantly affected the NHS (National Health Service) in the UK, although it was not the definite target. At 4 pm on the same day, NHS England declared the cyberattack a significant incident and implemented emergency arrangements to maintain health and patient care. According to the UK's National Audit Office (NAO), the WannaCry ransomware affected at least 80 out of the 236 trusts across England. They were either infected by the ransomware or turned off their equipment or systems as a provision. An additional 603 primary care and other NHS organizations were infected, including 595 GP practices (Sir Amyas Morse, 2017). WannaCry ransomware attack cost the NHS £92m through services lost during the attack, and IT costs in the aftermath. This attack led to 19,000 appointments being cancelled across one week, with an estimated 1% of all NHS care disrupted. The ransomware worked by causing 200,000 computers to lock out users with red-lettered error messages demanding Bitcoin (National Health Executive, n.d.). The NHS England and the National Crime Agency confirmed that no NHS organization paid the ransom or lost any data (Sir Amyas Morse, 2017).

4.0 Attack vector - potential vulnerabilities

As stated by Microsoft, WannaCrypt's spreading technique is hired out from familiar public SMB exploits, which prepared this typical ransomware with worm-like functionalities, generating an entry vector for machines still unpatched even after the fix had become accessible. Two circumstances that are highly possible enlightenments for the cause of this ransomware:

Over social engineering emails developed to trick users into running the malware and activating the worm-spreading functionality with the SMB exploit.

Infection via SMB exploit when an unpatched computer is addressable from other infected machines.

Hypothesised, the threat arrives as a dropper Trojan that attempts to connect the following domains using the API InternetOpenUrlA():

www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
www[x].iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]test

It may create a randomly named service that has the following associated ImagePath: "cmd.exe /c "<malware working directory>\tasksche.exe”".

It then hunts the whole computer for any file with any of the following file name extensions: .123, .jpeg , .rb , .602 , .jpg , .rtf , .doc , .js , .sch , .3dm , .jsp , .sh , .3ds , .key , .sldm , .3g2 , .lay , .sldm , .3gp , .lay6 , .sldx , .7z , .ldf , .slk , .accdb , .m3u , .sln , .aes , .m4u , .snt , .ai , .max , .sql , .ARC , .mdb , .sqlite3 , .asc , .mdf , .sqlitedb , .asf , .mid , .stc , .asm , .mkv , .std , .asp , .mml , .sti , .avi , .mov , .stw , .backup , .mp3 , .suo , .bak , .mp4 , .svg , .bat , .mpeg , .swf , .bmp , .mpg , .sxc , .brd , .msg , .sxd , .bz2 , .myd , .sxi , .c , .myi , .sxm , .cgm , .nef , .sxw , .class , .odb , .tar , .cmd , .odg , .tbk , .cpp , .odp ,

.tgz , .crt , .ods , .tif , .cs , .odt , .tiff , .csr , .onetoc2 , .txt , .csv , .ost , .uop , .db , .otg , .uot , .dbf , .otp , .vb , .dch , .ots , .vbs , .der" , .ott , .vcd , .dif , .p12 , .vdi , .dip , .PAQ , .vmdk , .djvu , .pas , .vmx , .docb , .pdf , .vob , .docm , .pem , .vsd , .docx , .pfx , .vsdx , .dot , .php , .wav , .dotm , .pl , .wb2 , .dotx , .png , .wk1 , .dwg , .pot , .wks , .edb , .potm , .wma , .eml , .potx , .wmv , .fla , .ppam , .xlc , .flv , .pps , .xlm , .frm , .ppsm , .xls , .gif , .ppsx , .xlsb , .gpg , .ppt , .xlsm , .gz , .pptm , .xlsx , .h , .pptx , .xlt , .hwp , .ps1 , .xltm , .ibd , .psd , .xltx , .iso , .pst , .xlw , .jar , .rar , .zip , .java , .raw.

WannaCry encrypts all files and renames them by joining (.WNCRY) to the file name (Microsoft Defender Security Research Team, 2017).

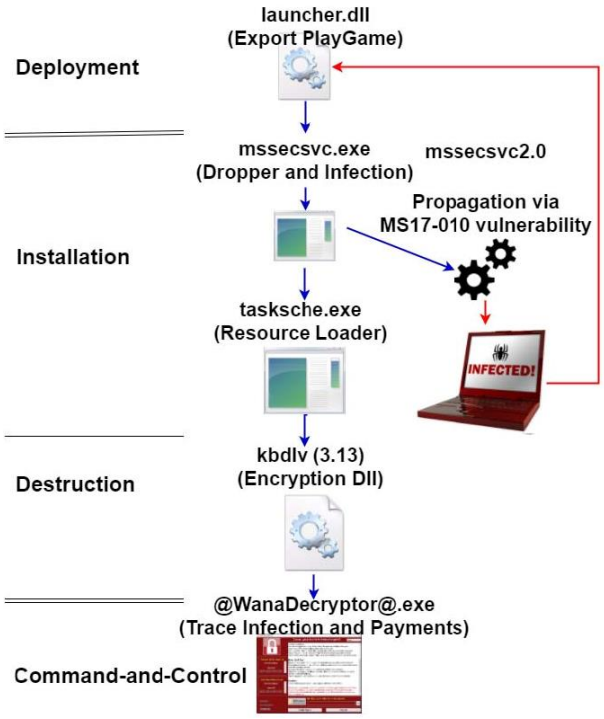

Figure 1. Main execution flow of WannaCry.

4.1 Prevention Methods

Since there is no way to fully protect the NHS organization counter to malware infection, the organization should implement a 'defence-in-depth' approach. It means using layers of defence with some mitigations at each layer. So there have more chances to detect malware and then stop it before it reasons actual harm to the organization. [Appendix: B]

They should undertake that some malware penetrates their organization to limit the effect this would cause and speed up the response. It can take some actions to help prepare the organization for possible malware and ransomware attacks.

4.1.1 Action 1: make regular backups

Up-to-date backups are the most operative way of recovering from a ransomware attack.

Make regular backups of the most important files - it will be different for every organization. Confirm to create offline backups that are kept isolated, in a dissimilar location (ideally offsite), from network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to upsurge the likelihood of payment. Make many copies of files using different backup solutions and storage locations. Rely on having two copies on a single removable drive, not relying on several copies in a single cloud service. Ensure that the devices holding the backup (such as external hard drives and USB sticks) are not eternally connected to the network. Attackers will aim for connected backup devices and solutions to make retrieval more difficult. Ensure that cloud service defends previous versions of the backup from being instantly deleted and allows to restore to them. It will prevent both live and backup data from becoming unreachable - cloud services frequently automatically synchronize after files have been swapped with encrypted copies. Ensure that backups are only connected to known clean devices before starting recovery. Scan backups for malware before restoring files. Ransomware may have infiltrated the network over time and replicated to backups before being discovered. Regularly patch products used for backup so attackers cannot exploit any known vulnerabilities they might contain. In cases, attackers have destroyed copied files or disrupted recovery processes before conducting ransomware attacks. Ideally, backup accounts and solutions should be endangered using Privileged Access Workstations (PAW) and hardware firewalls to enforce IP allow listing. Multi-factor Authentication (MFA) should be enabled, and the MFA method should not be installed on the same device used to administrate backups. Privileged Access Management (PAM) solutions remove the need for administrators to access high-value backup systems directly.

4.1.2 Action 2: prevent malware from being delivered and spreading to devices

It can reduce the likelihood of malicious content reaching the devices through a combination of:

- Filtering only to allow file types
- Blocking websites that are known to be malicious
- Actively inspecting the content
- Using signatures to block known malicious code

These are typically done by network services rather than users' devices. Ransomware is increasingly deployed by attackers who have gained access remotely via exposed services such as Remote Desktop Protocol (RDP) or unpatched remote access devices. To prevent this, organizations should:

- Disable RDP if it is not needed
- Enable MFA at all remote access points into the network, and enforce IP allow listing using hardware firewalls
- Use a VPN that meets regulations for remote access to services; Software as a Service or other services exposed to the internet should use Single Sign-On (SSO) where access policies can be defined (for more information, read our blogpost on protecting management interfaces)
- Use the most miniature privilege model for providing remote access - use low privilege accounts to authenticate, and provide an audited process to allow a user to escalate their privileges within the remote session where necessary
- The patch is known vulnerabilities in all remote access and external-facing devices immediately (referring to our guidance on how to manage vulnerabilities within the organization if necessary), and follow vendor remediation guidance, including the installation of new patches as soon as they become available

Prevent malware from spreading across the organization by following:

- Use MFA to authenticate users so that if malware steals credentials, they cannot easily be reused ensure obsolete platforms (Operating Systems (OS) and apps) are appropriately segregated from the rest of the network.
- Regularly review and remove user permissions that are no longer required to limit the malware's ability to spread
- Ensure system administrators avoid using their accounts for email and web browsing (to prevent malware from being able to run with their high level of system privilege)
- Practice good asset management, including keeping track of which versions of the software are installed on the devices so that can target security updates quickly
- Keep devices and infrastructure patched, especially security-enforcing devices on the network boundary (such as firewalls and VPN products)

4.1.3 Action 3: prevent malware from running on devices

A 'defence depth' approach assumes that malware will reach the devices. It should therefore take steps to prevent malware from running. The measures required will vary for each device type, OS, and version. Organizations should:

- Centrally manage devices in order only to permit applications trusted by the enterprise to run on devices, using technologies including AppLocker, or from trusted app stores (or other trusted locations) consider whether enterprise antivirus or anti-malware products are necessary, and keep the software (and its definition files) up to date
- Provide security education and awareness training to the people, for example, NHS's Top Tips for Staff
- Disable or constrain scripting environments and macros by enforcing PowerShell Constrained Language mode via a User Mode Code Integrity (UMCI) policy - use AppLocker as an interface to UMCI to automatically apply Constrained Language mode
- Protecting the systems from malicious Microsoft Office macros
- Disable autorun for mounted media (prevent the use of removable media if it is not needed)

4.1.4 Action 4: prepare for an incident

The following will help to ensure the organization can recover quickly.

- Identify critical assets and determine their impact if they were affected by a malware attack.
- Plan for an attack, even if all think it is unlikely.
- Develop an internal and external communication strategy.
- Determine how to respond to the ransom demand and the threat of publishing the organization’s data.
- Ensure that incident management playbooks and supporting resources such as checklists and contact details are available if anyone does not access their computer systems.
- Identify the legal obligations regarding reporting incidents to regulators, and understand how to approach this.
- Exercise the incident management plan. It helps clarify staff and third parties' roles and responsibilities and prioritize system recovery.

5.0 NHS Strategic Context

The Strategic objective of Cyberdefense is to defeat any cyber incident against the organizational infrastructure, capability, services, and applications,

which leads to an effect upon Privacy, Integrity, and/or Accessibility, resulting in compact flexibility, reduced safety, ineffective proficiencies, loss of business services, financial impact and reputational damage to NHS. As a community, cyber is for everyone. There is no unique technique for finding threats and risks and implementing controls; consequently, combining them as appropriate in the industry is the most operative method for developing a system that works for us. We will use the FAIR model (2005) to identify threats and risks on this occasion since FAIR has its basis in analyzing threat actors, communities, estimating risk. Besides, we will be utilizing ISO270001 to determine implementable controls as it details broad-spectrum controls that it deems relevant to every industry.

First, the NHS should strengthen their technologies critical to cyber; second; They should limit their reliance on individual suppliers or technologies developed under regimes that do not share the same values.

6.0 Threat Actors

The first type of threat to look at is an external one, cybercriminals. The cybercriminals' threat society is highly diverse, presenting difficulty when analyzing them. The basis of cybercriminals we might encounter would be comparable to that of "Lizard Squad," where the prime intent is to cause distraction and chaos. They have no outside dependencies, their favourite target is infrastructure, and their target style is whatever will gain them acknowledgement. A deviancy of this type of threat community could be motivated by ideology.

However, there are different types of cyber threat actors. Considerate their drives will help us know which of these might get you like a bull's eye and then the level of risk the organization could be visible. The ordinary inspiration for a cyber attack is for money or gaining something that can be traded for money, such as data, intellectual property rights (IPR), credentials, bank, or credit card details (Northern Ireland Cyber Security Centre, 2022).

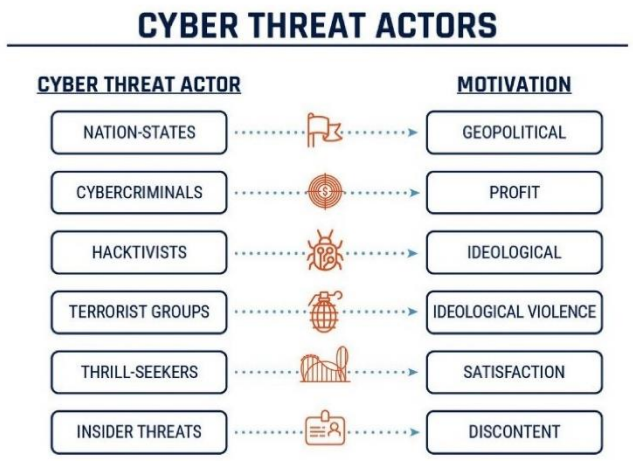

Figure 2. Cyber Threat Actors and Motivation.

7.0 Assets and Personnel

One of the critical assets we must acknowledge is a collective. The data centres and standalone servers host NHS Digital and patients' data. These servers present the most risk of all assets, albeit in different forms. The data centres, mobile devices, and standalone PCs could come under great forms of attack, distributed denial of service, insider threats, and external hacking movements. All of these pose an extraordinary opportunity to breach the NHS services' confidentiality, integrity, and availability.

Consequently, they must be of the most severe concern when safeguarding the assets, a lesson to be learned from the WannaCry hack mentioned prior. If such an attack was performed on the system to a similar degree, the results could be shocking. Subsequently, first and foremost, one must focus on securing the network and creating a plan to recover and resurge if such an attack occurs. The physical security assets must be sensibly measured; their placement and routine updating are critical to ensuring data security. The machines on these internal networks can be threatened through unnecessary high privileges and programs. Furthermore, the personnel that works in the data centres or with systems related to it need to be identified and take appropriate actions to secure the operations they perform. Additionally, another type of personnel must be acknowledged as a fairly significant security risk, those being external personnel.

Recently, most of the leaks have allegedly come from external contracts rather than direct employees. These differ slightly from the average insider threat in dealing with them and the difficulties they can create.

8.0 Risk Measurement and Evaluation

To enlighten the WannaCry attack, several reports from the US and UK accused North Korea of being

behind the ransomware, and one source suggested 'Lazarus,' a hacking group in North Korea, led the attack. The ransomware demands bitcoin payment, proposing financial gain as the primary motive. As North Korea was also under high tensions with chemical warfare, it could be said that North Korea was trying to test cyber warfare as another alternative (BBC, 2017).

Figure 3. Risk Management Basic Framework.

The best cybersecurity defence is to build a risk management program with a firm and robust foundation. When classifying a risk, consideration should be given to what could pose a potential threat (or opportunity) to assets of the organization.
Assets can be considered as:
• Information assets as identified on the asset register
• Business processes, objectives, and KPI's
• All staffs
Risks might happen and stop us from achieving aims or otherwise affect the organization's achievement. Incidents/issues have happened, were not planned, and need management actions must be reported as suitable and where required in line with the Incident Reporting Policy and Procedure. Once identified, the risk is clearly defined to guarantee that the risk is understood. Once acknowledged and defined, the risk should be added to the risk register and scored—guidance on how to write a risk to identify the cause, the event, and the effect.

A risk assessment is a qualitative or quantitative assessment of the nature and extent of the risk. The assessment is completed by scoring the likelihood of the risk occurring and the impact should it occur; an appropriate table can set out NHS Resolution's scoring matrix, which is based on a scale of 1 - 5, and the risk rating matrix, which gives the scoring a RAG status (O'sullivan and Evans, 2020).

The risk evaluation involves deciding what should be done with the risk. It includes determining appropriate controls and/or treatments for the risk and what level of risk can be tolerated within the organization's risk appetite.
• A Control is an existing strategy and process, such as systems, policies, procedures, standard business processes, practices.
• A Treatment is an additional strategy/activity NHS needs to develop and implement.
There are generally four options:
Treat – modify the risk's likelihood and/or impact, typically by implementing security controls.
Tolerate – make an active decision to retain the risk (e.g., it falls within the established risk acceptance criteria).
Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.
Transfer – share the risk with another party, usually outsourcing or taking out insurance.

The implementation of the risk treatment plan must be kept under review along with the risk score to measure its effectiveness; if the treatment is not reducing the risk, a new treatment plan should be considered.

FAIR can be used with data or without it. While the FAIR model presents a fantastic way to formulate threat and risk analyses, it does little to inform users of controls to be implemented, and where it does, it is rather vague. The BSI Standards ISO/IEC 27000/1 can be utilized to offer FAIR inverse. The standards detail Information Security Management Systems with a heavy focus on the implementation but not on identifying and analyzing threats and risks. There is nothing within the standards that detail threats and risk; the problem is that it does not provide a particular method of quantifying them and provides very little on anything like the concept of threat agents and communities. The FAIR model was utilized to identify and analyze threats and risks; then, the ISO/IEC 27001 was used to identify relevant controls. Using a hybrid of the two methodologies in vital areas creates a more robust, unified implementation.

9.0 Conclusion

To conclude, exploiting a combination of methodologies in order to cover all of the advantages and limitations of each other appears to be the best way to approach information risk management, this way you can have in-depth analyses while also complying with the international standards and all in all making your business secure.

Appendix: A

Likelihood scores for the risk occurring:

Likelihood Score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Certain**
Frequency	Not expected to happen for years	Expected to occur at least once the year	Expected to occur up to once a month)	Expected to occur at least weekly	This type of event will happen frequently

RAG status for the risk:

Impact	Likelihood				
	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Certain
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Insignificant	1	2	3	4	5

Appendix: B

Measures	Description	Prevention/ Detection/ Mitigation technique
Update computer software and OS	Affected computers were the ones that did not update MS OS and thus did not benefit from security patches released by Microsoft before the attack. Patch removed SMBv1 vulnerability (Multi State Information Sharing and Analysis Center, 2019).	Preventive Mitigation
Consistent backups of critical data	Reduce the impact of data loss and speed up the recovery process in an attack. Several copies of high valued data should be stored online, offline, and offsite (Cisco, 2021).	Recovery
Anomaly-based Intrusion detection and Intrusion Data Sources tools (IDS)	E.g., Snort analyses network traffic at the packet level and identify network anomalies. IDS analyses data sources from the host system and the network to detect insider and external attacks.	Detection
Track Least Privilege Principle	Access controls including file, directory, and sharing permissions should permanently be configured so that the user is given the minimum levels of permissions needed to do his/her job	Prevention Mitigation
Have an incident response plan	Be aware of the procedures to follow if an attack happens, how to restore backup solutions	Recovery

References:

BBC (December 19th, 2017) Cyber-attack: US and UK blame North Korea for WannaCry *© 2022 BBC.* . [online]. Available from: https://www.bbc.co.uk/news/world-us-canada-42407488 [Accessed 27 February 2022].

Cisco (2021) *Cisco Breach Defense Design Guide* [online]. Available from: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/breach-defense-design-guide.html [Accessed 27 February 2022].

Microsoft Defender Security Research Team (2017) *WannaCrypt ransomware worm targets out-of-date systems Microsoft Security Blog*.May 12, 2017

Multi State Information Sharing and Analysis Center (2019) *EternalBlue* [online]. Available from: https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf [Accessed 27 February 2022].

National Health Executive (no date) WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled *Cognitive Publishing Ltd*. [online]. Available from: https://www.nationalhealthexecutive.com/News/wannacry-cyber-attack-cost-the-nhs-92m-after-19000-appointments-were-cancelled [Accessed 27 February 2022].

NHS Digital (2021) Patients Registered at a GP Practice August 2021. [online]. pp.1–2. Available from: https://digital.nhs.uk/data-and-information/publications/statistical/patients-registered-at-a-gp-practice/august-2021# [Accessed 26 February 2022].

Northern Ireland Cyber Security Centre (2022) *Advice and Guidance - NI Cyber Strategy* [online]. Available from: https://www.nicybersecuritycentre.gov.uk/cyber-threats [Accessed 26 March 2022].

O'sullivan, C. and Evans, J. (2020) *Risk Management Policy and Procedure CG04* [online]. Available from: https://resolution.nhs.uk/wp-content/uploads/2020/12/CG04-Risk-Management-Policy-and-Procedure.pdf [Accessed 27 February 2022].

Sir Amyas Morse (2017) *Investigation: WannaCry cyber attack and the NHS* [online]. Available from: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/ [Accessed 26 February 2022].

William Smart (2018) *Lessons learned review of the WannaCry Ransomware Cyber Attack* [online]. Available from: www.nationalarchives.gov.uk/doc/open-government-licence/.