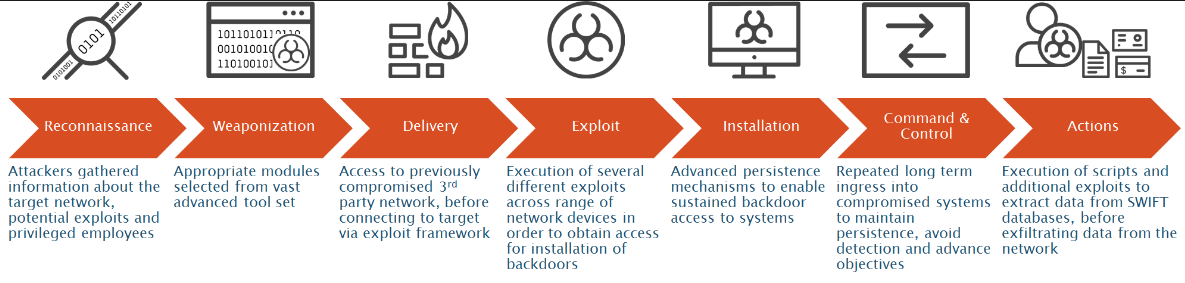
Information -Society and Security 40161070 Adam Blance

**1.Threat Context**

**1.1 Introduction**

Agri-Marine Robotics (AMR) is a privately-owned technology and manufacturing firm that specializes in autonomous agricultural and underwater robots. As it is the market leader it must consider security at all levels, therefore an attack and defence model will be created to protect the firm. Both of the models follow a simplified version of the Cyber Kill Chain, this was created to help company’s like AMR think like an threat to itself in order to protect the company.

The Cyber Kill Chain

* + 1. **Scenario**

Aberdeen based robotics manufactures AMR have recently become the market leader in their respected industry. The company is spilt between two sites, the head site in Aberdeen with another site located approximately 20 kilometres away. The head office contains a web server, email server and a file server, because of its relatively small size and it securing two major contracts last year AMR is a top target for attackers and a review of their security must be done.

The company possess many important assets

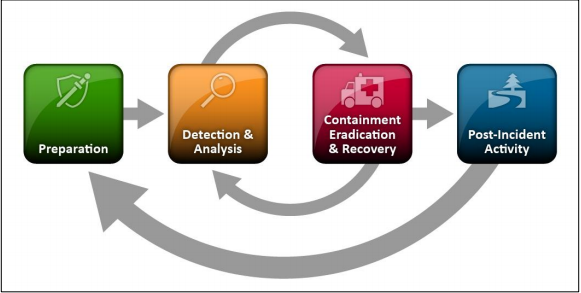
* + 1. **Threats**

Information Assets in Agri-Marine Robotics

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Vulnerabilities | C, I or A? | Reason |
| Designs/ Patents of Robotics |  | Availability |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**3. Incident Handling and Ransomware**

Ransomware is a term used for malware that is used to hold a system *“hostage”* until some kind of payment has been made. The simplest form of this usually locks a user out of their system until the ransom has been paid. A notable example being the “*WannaCry worm*” that was used to attack the NHS in 2017 and demanded Bitcoin in payments to let the user back into the system. The figure below shows the steps that will be used in this ransomware scenario.

 **Incident Handling Process**

The most important stage in my mind is he preparation phase this is because a company with large amounts of security will not have to deal with the other stages as much as a company that is not prepared. Preparation includes having every workstation secure with anti-virus and anti-malware software, firewalls and Intrusion Prevention Software(IPS). There are also extra steps that companies can take to be prepared. These can include: Having a dedicated war room for communication and co-ordination, Network diagrams and a list of critical assets and current baselines of expected network and system activity. All of these precautions would be adequate preparation.

The detection and analysis phase is the hardest phase to properly manage as an incident could occur in countless ways form countless sources. Making it nearly impossible to be fully prepared however organisations can be prepared to handle the most common form of attacks and their most likely targets. Such as theft or loss of equipment with sensitive data on it, Impersonation which includes spoofing and man in the middle attacks, and attrition attacks which involve DDos attacks, These usually employ an brute force attack to destroy a system. Another issues that arises in this stage is noticing signs of an attack while having anti-virus and anti-malware will help with this the are other ways organizations can be vigilant to notice an attack. These can include web server log ins showing usage of a vulnerability scanner or filenames with unusual characters. These steps will hopefully allow administrators to analyse the ransomware attacks and discover the point of origin.

The first step of this stage is to deciding how to contain the ransomware. This strategy should be determined beforehand and a company should have a different containment strategies for each major type of attack. If only a single part of the network has been affected by the ransomware it can be separated easily to stop the spread, if this is not the case then the entire network will have to be wiped clean. To eradicate the ransomware the easiest way is to pay the fee demanded but this might not be the possible for smaller companies . In that case it may be cheaper to wipe the system assume backups are available.

The most important part of Post-Incident Activity is learning and improving from the attack. This should include a discussion on; Exactly what happened and when? How well did staff react to the incident? And what would be done differently next time if a similar attack occurs. It is also important to collect data on the ransomware that was used, this can be used if the company wishes to prosecute the attackers or can just be used to prepare for an attack of the same type of ransomware in the future.

The reason the process described above is used in a ransomware attack is it covers all the necessary steps needed while not over-complicating the process for non-technical staff. Overall I belive that this process first evidenced by NIST handles the scenario well and is robust enough to hadle other threats not just this scenario.

**4.Evaluation**

During this coursework I have learnt about the many uses of attack defence modelling. At its worst modelling will allow a company to prepare for cyber-attacks by training them to think in a certain way which can be very useful. While modelling might not be a without its flaws it is useful start for companies with limited or no knowledge about cyber-attacks.

My scenario being based around the robotic industries in Aberdeen was very suitable for me, as I am from Aberdeen and knowing many people from this industry I am aware how competitive it is and how desperate companies are to get ahead of each other meaning they must have the most up to date security systems to protect themselves. While the model that was used was simplified and not as robust as a complex model , it does allow for staff with no experience in security to communicate easily with those who do. It also highlights the need for a multi-layer defence which is important as some may think that prevention or detection are the most important and forget to think about the other stages.

The model is not without its issues however with its closer focus to malware other attacks maybe not be prepared for causing a massive issue if a spear-phishing or dos attack occurs. While the model maybe a much cheaper to implement then alternative models, the cost greatly increase the more stages fail and the further the attacker gets causing a snowball effect. An issue also arises when a non-technical staff member is asked to complete any stage as understanding the cyber kill chain is very different from being able to implement it. It is also important to note that while this cyber kill chain is a great starting point in terms of security. It should not be the only form of defence that a company make use of and be used in conjunction with other forms of defence.

In conclusion , the simplified Cyber Kill chain is a great starting point for companies who are not technically gifted, although it might not be perfect and should not be a company’s only form of defence. The positives far outweigh the negatives. It is definitely more beneficial to a company such as Equifax that in my mind would have benefited from using the model. While it might not have prevented the massive data breach it would have certainly minimised the damage that the breach caused.

**References**

Jon Fingas(2018) Equifax breach may have exposed more data than first thought Retrieved 11 February 2018 <https://www.engadget.com/2018/02/10/equifax-breach-may-have-exposed-more-data/>

# James R. Rutherford and Gregory B. White (2018) Cyber Kill Chain Model Needs A Makeover

Retrieved 11 February 2018 <https://www.afcea.org/content/cyber-kill-chain-model-needs-makeover>

Paul Cichonski Tom Millar TimGrance Karen Scarfone Computer Security Incident Handling Guide Retrieved 11 February 2018 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

# [Warwick Ashford](http://www.techtarget.com/contributor/Warwick-Ashford) (2017) WannaCry a signal moment, says NCA Retrieved 11 February 2018 <http://www.computerweekly.com/news/450421936/WannaCry-a-signal-moment-says-NCA>

# [CASSIMIR MEDFORD](https://boundless.aerohive.com/authors/Cassimir-Medford.html)(2016) HOW CAN YOU ERADICATE RANSOMWARE? Retrieved 11 February 2018 <https://boundless.aerohive.com/experts/How-Can-You-Eradicate-Ransomware.html>