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 the Cyber Kill Chain, this was created to help company’s like AMR to think like an threat to the itself in order to protect the organisation.

* + 1. **Scenario**
    2. **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.

**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 Retrived 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

Retrived 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 Retrived 11 February 2018 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

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