FACULTY OF SCIENCE & TECHNOLOGY
Department of Computing & Informatics
Forensic Computing & Security

Security by Design **14th October 2020**
Word Count: 1500

Paul-David Jarvis
s5115232@bournemouth.ac.uk

Security Requirements For N3

Table of Contents

List of Figures

User Security and Trust Expectations

Firstly I read the documentation for Cairis and watched the videos on YouTube. Now that I had an idea about creating personas I created a basic and empty neonatal nurse persona. I then began collecting information by researching what the day of a neonatal nurse was like and reached out to a friend to answer a question as she works in the neonatal department at Brighton Hospital. I then started to build the persona known as Trinity by filling in her environments like the Special Care Baby Unit (SCBU), activities, motivations and other information about her.

Trinity is in the position to break the security triad but we trust her and other nurses to act responsible. Trinity as a neonatal nurse has access to the confidential information stored on N3 such as her patient's medical records and prescription information. Her as a nurse who the parents trust with their children's life trust that she not break the confidentiality policy on any data by showing it to third parties and to maintain the integrity of life or death information such as prescriptions and their medical history. As a nurse she also has an instinctive trust as someone who cares for those less fortunate and especially children.

Figure 1: Persona Picture: Trinity. - (Neonatal nurse, n.d.)

NeoNateNetwork's Assets

I first started mapping out the assets within SCBU by reading the brief over and over again and extracting the information given to us. From the brief I was able to extract the relevant assets needed to perform the next activities.

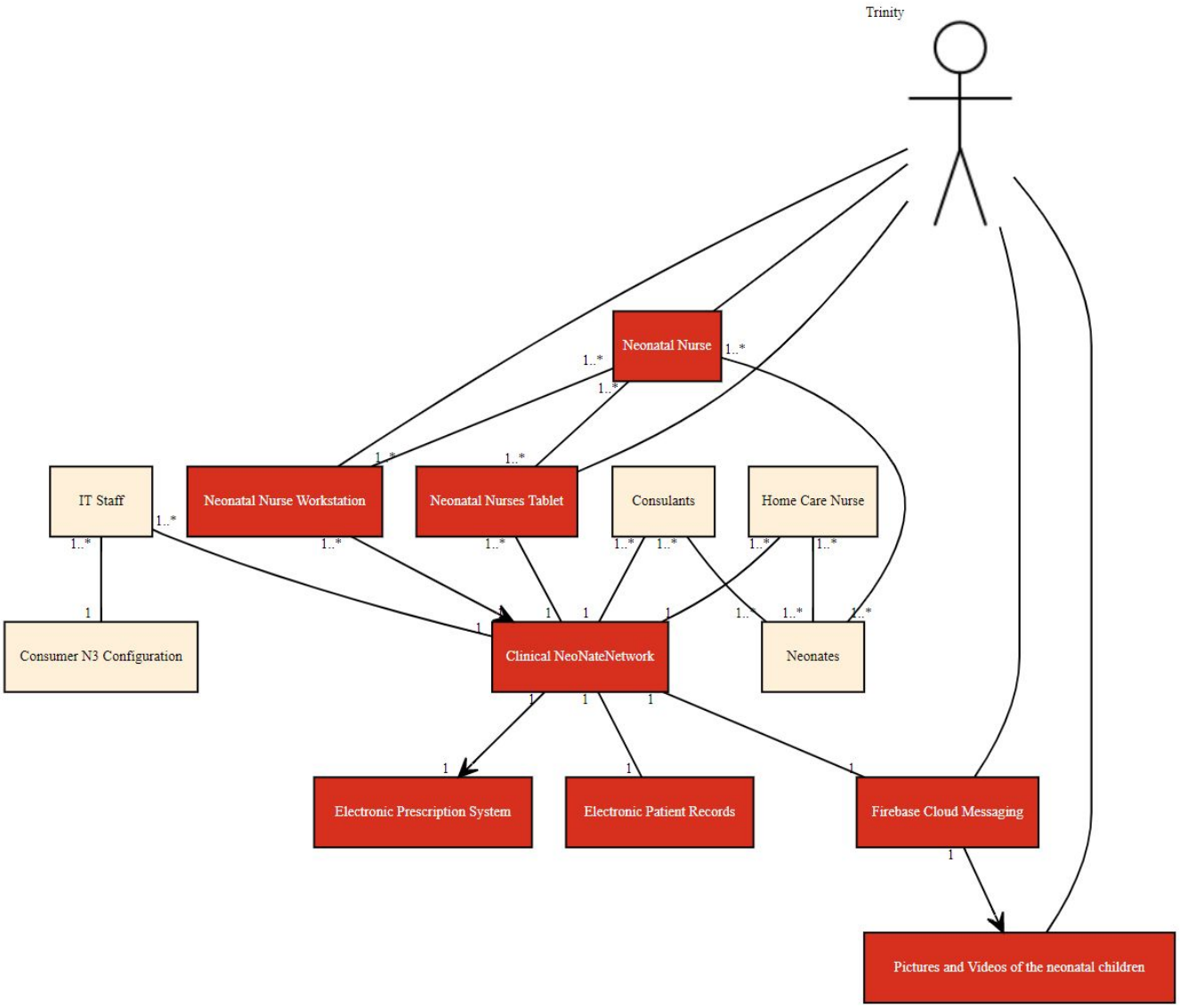

Figure 2: Asset Model: Special Care Baby Unit. - (Cairis)

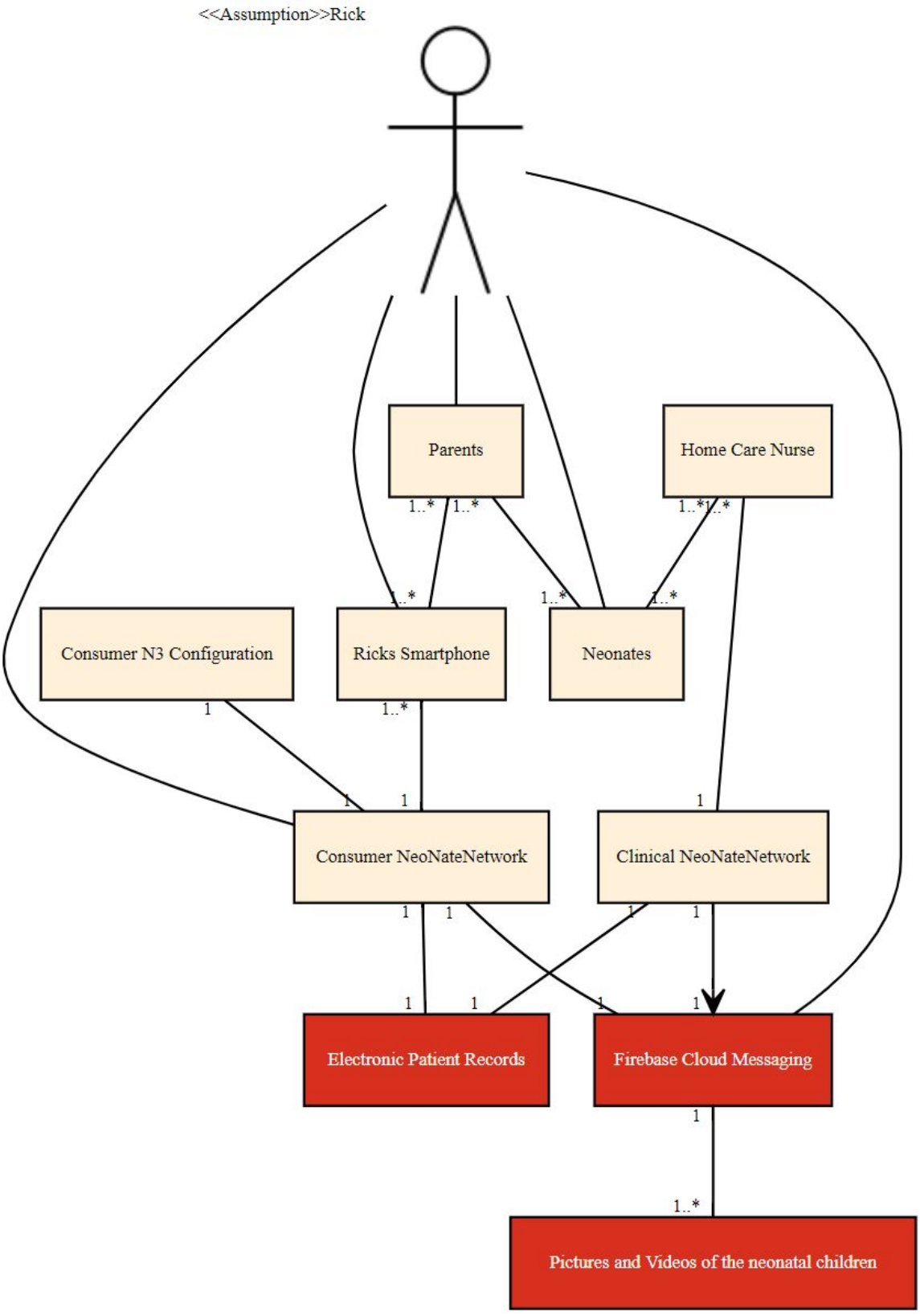

Figure 3: Asset Model: Rick's Home. - (Cairis)

Hardware

The information I extracted from the brief and Figure 1 N3 elements told me that the nurses have workstations and tablets that they use to access N3 and the parents have a smartphone that they can use to download N3 from the appstore.

−	Neonatal Nurse Workstation	Hardware
−	Neonatal Nurses Tablet	Hardware
−	Ricks Smartphone	Hardware

Figure 4: Assets: Hardware. - (Cairis)

Software

I identified from the brief that there were two versions of N3, a clinical version that is used by the staff at the SCBU and a consumer version of N3 that parents can install from the appstore. I also discovered that both N3 versions rely on Firebase Cloud Messanging (FCM) to communicate with each other.

−	Clinical NeoNateNetwork	Software
−	Consumer NeoNateNetwork	Software
−	Firebase Cloud Messaging	System of Systems

Figure 5: Assets: Software and Systems. - (Cairis)

Information

Information assets were the majority of assets discovered when reading the brief. First asset to write down was the child's progress and child’s care plan. I also wrote down all the roles I found such as consultants, neonatal nurses and home care nurses. The next assets were the two interfaces that will assist the roles which are the electronic patient records (EPR) and electronic prescription systems (EPS). N3 also allows for nurses to send pictures and videos of their children to the parents which makes another asset.

−	Consumer N3 Configuration	Information
−	Electronic Patient Records	Information
−	Electronic Prescription System	Information
−	Pictures and Videos of the neonatal children	Information

Figure 6: Assets: Information. - (Cairis)

−	Home Care Nurse	People
−	Consulants	People
−	IT Staff	People
−	Neonatal Nurse	People
−	Neonates	People
−	Parents	People

Figure 7: Assets: People. - (Cairis)

Key User Tasks & Security implications

I first started this by jotting down the assets and objectives that N3 wanted to achieve and linked them together. This gave me a good idea on what assets were being used by which role or persona and how they were being used in the objectives. From this I created 3 tasks that would achieve the objectives and used the assets I discovered in the previous task.

+	Name	Objective
−	Checking Childs Progress	N3 should allow the parents to use the consumer version of N3 to check their neonatal child's progress.
−	Sending Pictures and Videos	To send pictures and videos to the parents of neonates to update them on their progress.
−	Update Clinical Team	Rick will use N3 to communicate with the clinical team that is looking after his child when his child is well enough to come home.

Figure 8: Tasks. - (Cairis)

Checking child's progress

The first task I created was using the consumer version of N3 to communicate through FCM to check how his child is doing. I thought that checking the progress wasn't going to take long so the duration were minutes, I assumed that Rick would want to know the progress regularly so I set the task with a "Daily - Weekly" frequency, This was one of the main objectives and goals for N3 so I set the demands high and the goal conflict to none.

Sending pictures & videos

The second task was for Trinity to send pictures and videos to the parents of her patients. I decided that the duration for this task was minutes as I thought taking pictures and uploading them to the workstation or tablet and sending them through FCM would've been longer than seconds but less than hours. I set the frequency to "Hourly or more" as I can't imagine parent's will wait any longer. The demands and goal conflicts were the same as the previous task.

Updating the clinical team

The third task was keeping the clinical team updated once the child was well enough to go home. Rick will use N3 to keep the clinical team updated when his child is sent home. He uses N3 and

FCM to send the nappy changes, medications and feeding times to the clinical team. This task's duration would be minutes and that the clinical team would want updates daily or weekly. The demands and goal conflict are the same as the previous two tasks.

NeoNateNetwork's Data Flows

I first started this activity by looking at the tasks I created along with the assets and objectives I made. I then wrote down what data would make sense flowing from these assets. Before starting a data flow I first had to create use cases which helped alot in identifying exactly what the assets were and data that was flowing in between them. The several use cases we created ended up linking together.

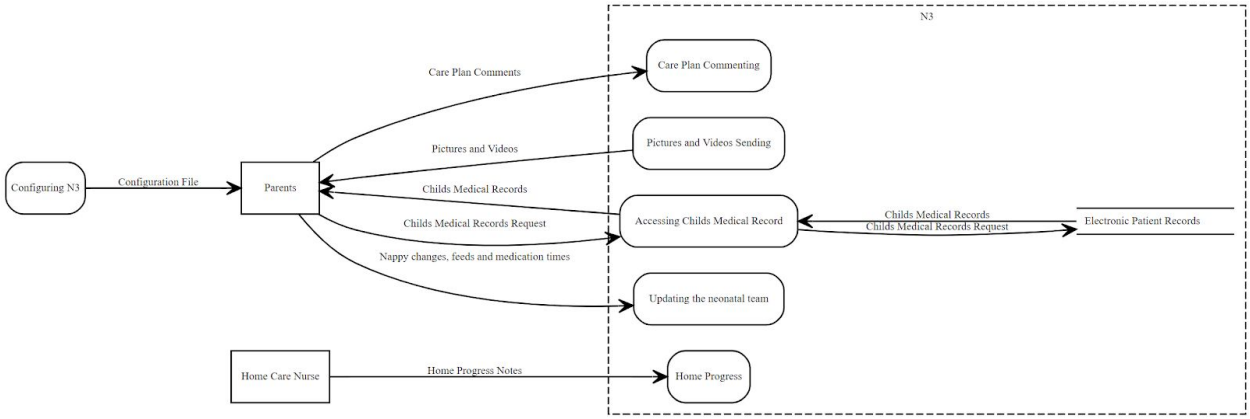

Figure 9: DFD: Parent's Environment. - (Cairis)

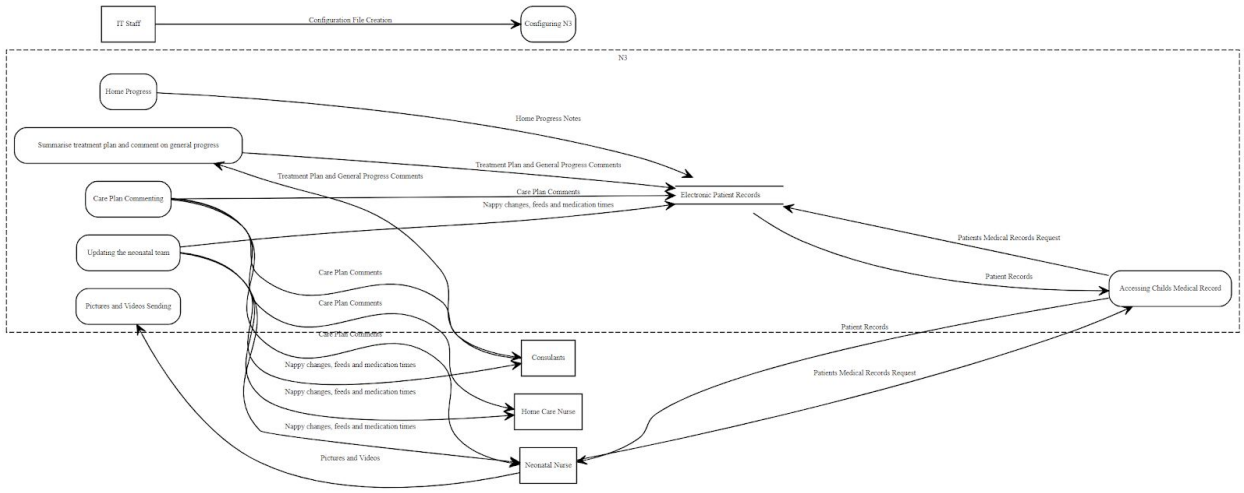

Figure 10: DFD: Special Care Baby Unit. - (Cairis)

NeoNateNetwork's Threat models & Risk Analysis

Attackers

I first started to model the threats that N3 could encounter by creating three potential attackers. One is an emotional threat actor and the other two are insider threats.

Rick Astley

Rick is the father of a patient at the SCBU. I assigned Rick the roles of "Parent" and "Emotional Attacker", his motivation is "Revenge" and his capabilities are high for "Resource/Funding" due to his success, "Technology", "Software" and "Knowledge/Education and Training" due to his intelligence.

Figure 11: Attacker: Rick. - (Idolwiki, n.d.)

Marcus Hutchins

Marcus is an ex employee of SCBU and was fired due to insubondiation. I assigned him the role of "IT Technican" and "Insider Threat". His motivation is "Revenge" due to his dismissal and his capabilities are the same as Rick's with an additional high "Knowledge/Methods".

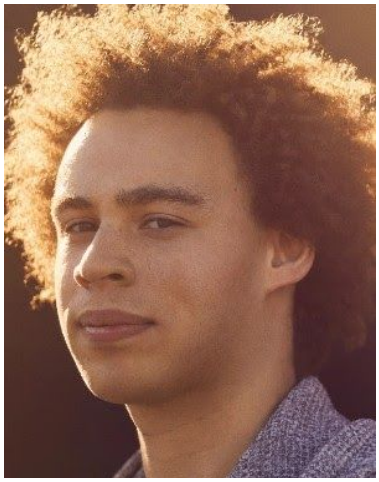

Figure 12: Attacker: Marcus. - (Wired, 2020)

Kate Monroe

Kate is currently working at SCBU and has been for a single year. I assigned her the roles “Nurse (Neonatal)” and “Insider Threat”, her motivation is “Accident” and she has the same capability as Marcus but her “Technology” and “Software" are low.

Figure 13: Attacker: Kate. - (EducationCareerArticles, 2013)

Threats

Now that I had attackers I could come up with potential threats. Rick’s was “Man-In-The-Middle Attack”, Marcus’s was “Inside Theft” and Kate’s was “Accidental Data Entry”

Inside Theft

This is a physical threat and can be succeeded mostly by an insider threat actor and especially those with the knowledge and access such as Marcus. Due to his dismissal and his motivation

and his access to confidential information such as the EPR and EPS and he could steal medical data before leaving the SCBU.

Man-In-The-Middle

This is a remote threat that can mostly be succeeded by threat actors with a good computinog knwoeldge such as Rick. He would access either the FCM service or the SCBU network and use tools like wireshark to intercept traffic. This breaks the confidentiality and integrity principles.

Accidental Data Entry

The last threat is accidentality succeeded by those with little experience with technology such as Kate. Her access to N3 and the EPR and EPS and little idea of how the system works could potentially break the integrity of the data stored on N3 by accidentality committing wrong data.

Vulnerabilties

When looking at vulnerabilities I took my attackers and threats into consideration. From the “Inside Theft” threat I came up with “Inadequate Datastore Protection”, for “Man-In-The-Middle” attack I came up with “Unencrypted Communication” and for “Accidental Data Entry” I thought of “Insufficient User Training”.

Inadequate Datastore Protection

The first vulnerability was not sufficient protection for the datastores and other information. I put the severity as catastrophic as if this confidential data was stolen or leaked because of it not being properly protected then it would break the GDPR.

Unencrypted Communication

The second vulnerability was unsecure traffic. Medical data and other confidential information aswell as pictures and videos of the neonatal children are sent from the clinical version to the consumer version through the FCM.

Insufficient User Training

The third vulnerability was ill-exerience staff members trying to use a new complication system and could potentially make mistakes that causes serious harm or even death if the wrong data was submitted or deleted.

Risks

Now that I know the attackers, threats and vulnerabilities. I came up with “Information Interception”, “Theft of Confidential Data” and “Wrong Data Entry”.

Information Interception

The first risk is “Information Interception” and it is the “Man-In-The-Middle” threat and “Unencrypted Communication” vulnerability with a rating of undesirable and a score of 9 for both pre and post mitigation.

Theft of Confidential Data

The second risk is “Theft of Confidental Data” and it’s the combination of “Inside Theft” threat and “Inadequate Datastore Protection” vulnerability. It has a rating of tolerable and the same as the first migration scores.

Wrong Data Entry

The final risk is “Wrong Data Entry”. It is the mix of the “Accidental Data Entry” threat and the “Insufficient User Training” vulnerability. It has the same rating and mitigation score as the second risk.

Proposed Security Requirements

I was able to propose a few security countermeastures and requirements to combat the main risks and I proposed a few smaller requirements that were specific to one or two assets. Once I added these countermeasures and risks to their correct place on Cairis, I was able to use KAOS to link everything together in relation to the risk analysis.

Corporate Hierarchy and Levels of Access

I proposed implementing a corporate hierarchy and assigning access levels to the staff at the SCBU. This was to combat staff members potentially accessing confidential information that they were not supposed to. Reserving the confidentiality and integrity of the information aswell as combating potential inside information theft.

Data Modification Double Confirmation

This countermeasure was to combat the accidental deletion and entry of data that would breach information integrity and availability policy. This countermeasture and the double confirmation requirement will also help staff members with little to no training of the N3 software.

Using Secure Traffic Measurements

The third countermeasrure uses the secure traffic requirement and helps to combat and prevent the man-in-the-middle attack, the unencrypted communication risk and the breach of confidential information policy. Using AES instead of a plaintext protocol.

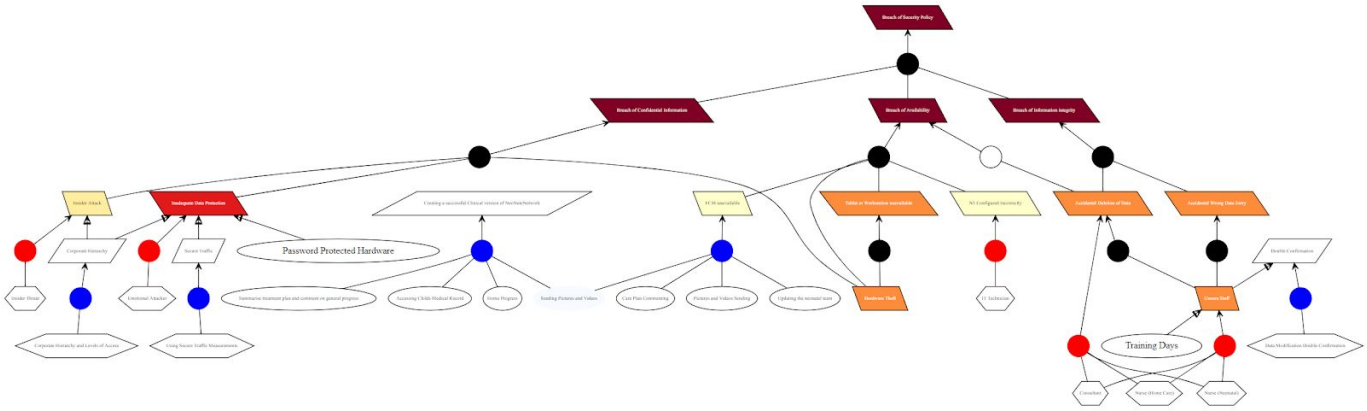

Figure 14: Goal Model: SCBU Environment. - (Cairis)

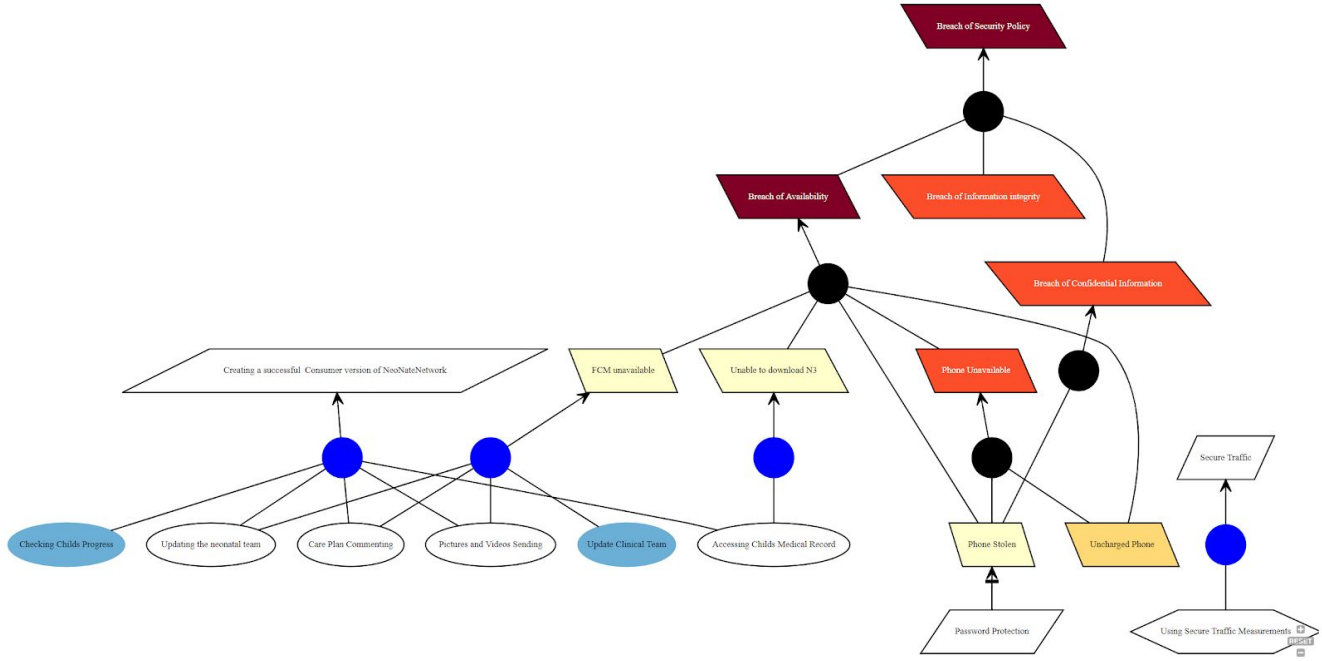

Figure 15: Goal Model: Rick's Environment. - (Cairis)

References

Nbt.nhs.uk. 2020. *A Day In The Life Of A Neonatal Nurse | North Bristol NHS Trust*. [online] Available at: <https://www.nbt.nhs.uk/our-services/a-z-services/neonatal-intensive-care-unit/a-day-life-a-neonatal-nurse> [Accessed 1 October 2020].

Interview Question.txt [Accessed 1 October 2020]

Jillings, B., n.d. *5 Must-Have Neonatal Nurse Skills | Nursechoice*. [online] Nursechoice.com. Available at: <https://www.nursechoice.com/traveler-resources/5-must-have-nursing-skills-for-neonatal-nurses/> [Accessed 1 October 2020].

Idolwiki, n.d. *Rick Astley*. [image] Available at: <https://idolwiki.com/1600-rick-astley.html> [Accessed 19 October 2020].

Wired, 2020. *The Confessions Of Marcus Hutchins, The Hacker Who Saved The Internet*. [image] Available at: <https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/> [Accessed 19 October 2020].

EducationCareerArticles, 2013. *Information On Degrees And Requirements Needed To Become A Neonatal Nurse*. [image] Available at: <http://educationcareerarticles.com/education-articles/higher-education-articles/information-on-degrees-and-requirements-needed-to-become-a-neonatal-nurse/> [Accessed 19 October 2020].

Appendices

Appendix A: Personas

Trinity

Trinity is a nurse persona that I created while modeling this system using Cairis. She is a neonatal nurse that looks after the children at the Special Care Baby Unit. Her day starts with her shift at 7:30am where she and her colleagues where she will be informed for the day. She then goes about her day completing her tasks such as checking medication, managing fluids and recording her observations. (A Day in the Life of a Neonatal Nurse | North Bristol NHS Trust, 2020) She has worked as a neonatal nurse for over 10 years and has always enjoyed her work even when she needs to make a terrible decision such as getting the parents consent to withdraw care and a do-not-resuscitate order if they get worse. She is a little worried about a new system as she has always done a certain way and has relied on an established set of protocols. Trinity's friend's consider her OCD due to her attention to detail but she knows that it helps in understanding the stages that these children go through. She has developed the skills and ability to make quick decisions due to her 10 years of experience in a fast paced environment. (Jillings, n.d.)

Rick

Rick is a largely assumption based persona that I created to take the role of a parent of a patient currently being looked after by Trinity and other SCBU professionals. He runs his own software company and spends his time at home managing his company and waiting to hear from the SCBU with any information on his child.

Appendix B: Interview Transcript

1 Oct 2020, 9:21

Paul: "Hi D! hope you and everyone else is doing good!! I was wondering if I could ask a weird question? my course is surrounding neonates and I was wondering about the procedure when it comes to looking after the babies?"

D: "Hi Paul, I'm good I hope your ok!!! If it's medical intervention we have to act in the babies best interest and we go on protocols to preserve life, but if a baby is very sick and not likely to survive then we will advise and get parents consent to withdraw care or to not resuscitate their

baby if they collapse or get worse, I hope that makes sense! But we always inform parents of descions we make and it is always good when they give us consent x”

Paul: “Yes this helps so much D!!! thank you so much xx”