Security by Design (COMP7023)

Security Requirements for PATs

Table of Contents

Security Requirements for PATs 1

PATs Assets 5

Key user tasks and security implications 5

PATs Data Flows 6

PATs Threat Models and Risk Analysis 6

Propsed Security Requirements 9

Costs & Benefits 9

1.1 - Personas 10

1.1.1 - Roles 10

1.2 Jessica 10

1.3 Jessica's Factoids 11

1.4 Affinity Diagrams 15

1.5 Lily 16

2.1 - Assets 17

2.1.1 - Software 17

2.1.2 - Hardware 17

2.1.3 - Information 18

2.1.4 - People 22

2.1.5 - Systems - General 23

2.2 Asset Assocations 23

3.1 Tasks 25

3.1.1 Submit tuition session request 25

3.1.2 Uploading Upcoming Events 26

3.1.3 Tracking Instructor's Hours and Student's Sessions Attended 26

3.1.4 Manually Matching Tuition Requests 27

3.1.5 Viewing Upcoming Events 28

3.1.6 Viewing Tuition Sessions 28

4.1 Use Cases 30

4.1.1 Requesting Tuition Sessions 30

4.1.2 Adding Upcoming Events Information 30

4.1.3 Viewing Instructor's and Student's Performance 30

4.1.4 Matching Tuition Requests 31

4.1.5 Viewing the upcoming events 31
4.1.6 Viewing Lily's Tuition Sessions 31

4.2 Data Flow* 32
4.2.1 Requesting Tuition Sessions* 33
4.2.2 Adding Upcoming Events Information 33
4.2.3 Viewing Instructor's and Student's Performance 34
4.2.4 Matching Tuition Requests 35
4.2.5 Viewing the upcoming events 35
4.2.6 Viewing Lily's Tuition Sessions 37

5.1 Attackers 38
5.1.1 Jessica Richardson 38
5.1.2 John Howard 38

5.2 Vulnerabilities 39
5.2.1 Inadequate User Training 39
5.2.2 Unsanitised User Input 39
5.2.3 Insuffient Password Policies 39
5.2.4 Unencrypted Data Transfer Protocols 39
5.2.5 Single Point of Failure 40
5.2.6 Jessica Richardson 40

5.3 Threats 40
5.3.1 Accidential Wrong Use 40
5.3.2 SQL Injection 41
5.3.3 Weak Passwords 41
5.3.4 Man In The Middle (MITM) 42
5.3.5 Denial of Service Attack 42
5.3.6 Ransomware Containing USBs 43

5.4 Risks 43
5.4.1 Confidential Information Disclosure through Human Error 43
5.4.2 Information Disclosure through SQL Injection 44
5.4.3 Privilege Esculation through Dictionary Attack 45
5.4.4 Data theft through MITM attack 46
5.4.5 Availability Attack through DoS or DDoS 47
5.4.6 Ransomware Attack through USB Drop Attack 48

5.5 Risk Model Diagrams 49

6.1 Goals 51
6.2 Requirements 51
6.3 Countermeasures 52
6.4 KAOS Associations 53

User Security and trust expectations

Data was collected regarding the usual activities that students and instructors of dance do from several sources such as blogs and videos to job applications for dance instructors. This data was used to create the personas and then put into factoid form and uploaded to Trello to create an affinity diagram to understand the characticterists of both our personas. This information was then imported into CAIRIS for persona building purposes.

Persona's security and trust expectations.
Jessica Richardson is a dance instructor working with the local PAT team. Jessica teaches several different dance styles and techniques but specialise in ballet. She arrives early at school to set up for the day; where she choreographed routines and selects appropriate music for upcoming recitals and concerts and develops and plans her dance curriculum and lesson plans. She has an extremely busy day where she teaches and leads several different classes and age groups. These classes are dotted around the campus in different classes and studios so Jessica is always on the move. Before her students arrive she first gets changed into appropriate dance clothing. Now that her students have arrived she starts by demonstrating how to warm up, move safely then some dance moves. Jessica's love for dance means that she is a very bubbly person who can easily engage, motivate and communicate with her diverse group of students which has provided a safe and creative place for her students. In her free time she provides feedback and evaluates her students and suggests improvements. Throughout the school year there are several recitals and concerts that happen. It's Jessica's job to select the students who will be selected and to help with costume fittings and makeup calls. Jessica teaches an afterschool club in which she promotes it and markets it throughout the day on campus. After her after school club is where she spends an hour recording her student's performance and progresses, assesses student's exams performance and writes up the plan for the following week.

Jessica is a very organised person and is great at managing her time, every now and then Jessica has to fill in for another dance instructor. She currently holds a bachelor's degree in dance and holds several first aid certificates including first aid. Her years of dance experience means she is very physical and in great health. In addition, she is extremely disciplined and can remain calm in stressful situations. She is considered a great leader with the ability to work with any other dance instructor. She is naturally a brilliant dancer and she is very good at keeping up to date with new dance techniques. She is a quick study and has a passion for the fine arts, this quick study skills means she is brilliant at teaching and designing her dance course. She prefers to use initiative to solve problems and tries to reinforce a degree of dependability for her students.

She isn't very technically savvy and worries that switching to PATs might impact her productivity. The nature of her job requires her to keep private and sensitive data confidential as they relate to young children. The local PAT team understands that this will be a challenge but they expect Jessica to use the system and utilise all services offered by PATs (See 1.2 - Jessica in the Appendix).

In addition to Jessica's persona, we also created a persona for Lily; a dance student studying under the local PATs team. She has several sessions throughout the day and uses the PATs system to check when they've been scheduled. Similar to Jessica, she has a passion and love for dance and she's thrilled and doesn't take for granted the opportunity she's been given to study dance. This has caused a professional friendship like relationship with Jessica as both share a passion. She's a natural when it comes to dance and is an extremely quick study in any other techniques. She's motivated to dance because of her passion and to follow in her mother's footsteps (See 1.5 - Lily in the Appendix). Because of the nature of her persona along with her very limited ability to use the PATs application maliciously and her age, we thought that there was no reason to develop a high level persona for Lily including factoids as we did for Jessica.

PATs Assets

After thoroughly reading how the PAT system would operate and the features that the PAT team wanted to implement, assets were determined and imported into CAIRIS. These assets were then given additional context and information and several security properties were assigned to each asset. (See 2.1 - Assets in the Appendix)

Each asset was assigned a specific type; "Information" included assets that are not physical but rather pieces of data such as ID numbers and confirmation messages, "Software" was the PATs application itself, "Hardware" was the devices used by instructors and students to access the PATs application, "People" were the dance students and instructors themselves and finally "Systems - General" which we assigned to the asset "Unamed Hosting Service" as this could engulf several types like the physical hardware servers and the software running.

Once all the assets for the PAT application were identified the next step would be modelling how each asset interacts with each other to meet the requirements that the PAT team set out. Understanding how assets worked together, it was easy to identify what and how data was flowing through the system (See 2.2 - Asset Associations in the Appendix).

Key user tasks and security implications

To provide and validate our PATs application we have created six theoretical tasks that will test how well our system would work taking into consideration how Jessica and Lily would use the system and what data flows and the assets used (See 3.1 Tasks in the Appendix)

The tasks that were created were:

- 3.1.1 Submit tuition session request
- 3.1.2 Uploading Upcoming Events

- 3.1.3 Tracking Instructor's Hours and Student's Sessions Attended
- 3.1.4 Manually Matching Tuition Requests
- 3.1.5 Viewing Upcoming Events
- 3.1.6 Viewing Tuition Sessions

In 3.1.1 we see Lily use the PATs application to submit a tuition session request. This is then followed up in 3.1.4 where we see Jessica receive this request and matches the request with the related instructor. The next task is 3.1.2 where we see Jessica upload the upcoming events to the PATs application. Again, this is then followed up by task 3.1.5 where we see Lily use the PATs application to view the upcoming events that Jessica uploaded. In 3.1.3 we see Jessica use the PATs application to track and analyse the statistics relating to instructor's hours and student's sessions. 3.1.6 is where we see Lily use the PATs application to view her upcoming and booked tuition sessions.

PATs Data Flows

Now that we have a couple of theoretical tasks for both Jessica and Lily, we can turn those into Use Cases on CAIRIS which shows a more indepth view into how Jessica and Lily will interact with the system which allows us to create a good foundation in modeling the data flown between our assets.

Our six use cases were created based on the tasks above:

- Adding Upcoming Events Information
- Matching Tuition Requests
- Viewing Instructors and students performance
- Viewing Lily's Tuition Sessions
- Viewing the upcoming events

Each use case we created contains steps which helped us fully understand how Jessica and Lily would use the system (See 4.1 Use Cases in the Appendix)

PATs Threat Models and Risk Analysis

Now that we have an idea on how the PATs application will be used by both teacher and student and the type of data that will be flowing through the system, we can now identify the potential attackers, vulnerabilities, threats and risks. In addition, we also considered the security model STRIDE developed by Praerit Garg and Loren Kohnfelder to assign each risk a security threat in one of STRIDEs six categories:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service

- Elevation of Privileges

We modeled our first attacker of our persona Jessica so we can portray the very possible inside attack of accidential and human error. A study by IBM stated that a human error was a major contributing cause in 95% of all breaches (Hacker News, 2021) which is why to provide a reliable scenario involving an attack of PATs we included an vulnerabilty that highlights the need to train the dance instructors on how to use the PATs application, 5.3.1 is a threat that shows how Jessica's lack of training can cause an attack and finally the risk 5.4.1 where we combine Jessica, her lack of training and the fact that her human error could be a threat to create a risk that because of the lack of knowledge with PATs that Jessica has, she is the direct cause of confidential data disclosure through human error (See 5.1.1, 5.2.1, 5.3.1 and 5.4.1 in the Appendix). To emphasise how common sensitive data exposure is, it's now second on OWASPs Top 10 in 2021; A02:2021-Cryptographic Failures previously known as A3:2017-Sensitive Data Exposure (A02 Cryptographic Failures - OWASP Top 10:2021, 2021). This is a clear threat that falls under Information Disclosure of STRIDE. We are also able to assign CWE-201: Insertion of Sensitive Information Into Sent Data from MITRE's CWE list (CWE-201: Insertion of Sensitive Information Into Sent Data (4.6), n.d.).

The next proposed risk introduces a new attacker called John Howard, Lily's older brother who is currently studying at the local university and training to become a penetration tester. This risk explains why it's vital to make sure that any information passing through an application that has a database backend is properly tested to route out any bugs. 5.2.2 is our threat of Unsanitised User Input that allows any threat actor the potential to manuiplate our database by throwing wildcards, characters and scripts to our database in hope they achieve a malicious purpose. 5.3.2 is our SQL Injection threat that is possbile with the use of a database that doesn't sanitise user input, we see John writing a SQL query that grants him access to the default admin account and now he has access to all databases hosted and student's and instructor's information. We see this risk also has a OWASP Top 10; A03:2021 – Injection (A03 Injection - OWASP Top 10:2021, 2021) and several CWEs; CWE-89 (CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (4.6), n.d.). This one comes under Information Disclosure and Elevation of Privileges in the STRIDE model. (See 5.1.2, 5.2.2, 5.3.2 and 5.4.2 in the Appendix).

Our third proposed attack is with John being a little more malicious than previous. 5.2.3 is a vulnerability in PATs where they have no policies in place regarding the creation of passwords to ensure that they're complex enough not to be able to crack; sources state different on how long it would take a hacker to brute force your password but the general consensus is that a password should be more than 8 characters long including lower case, upper case, symbols and numbers which would take an hacker more than 40 years to crack. These passwords should also be changed regularly. John takes advantage of the weak passwords in 5.3.3 and is made into a complete risk in 5.4.3 where he uses a penetration testing operating system; Kali, and a cracking tool; John The Ripper, to successfully crack an admin password that was '123456' and gain elevated privileges. This is number 7 on OWASPs Top 10 list; A07:2021 – Identification and Authentication Failure (A07 Identification and Authentication Failures - OWASP

Top 10:2021, 2021) as well as CWE-521 (CWE-521: Weak Password Requirements (4.6), n.d.). This one by definition is Elevation of Privileges Spoofing, Information Disclosure and potentially Tampering and Denial of Service if John were to either change or delete any data. (See 5.1.3, 5.2.3, 5.3.3 and 5.4.3 in the Appendix).

Our fourth potential attack is showing John who is currently connected to the network that PATs is using and is currently running Wireshark in the background intercepting all packets flowing on the network which is a MITM attack shown in 5.3.3. He intercepts a login request sent by a user to PATs to autneticate herself so she can use the application. John takes advantage of the encrypted transfer protocols shown in 5.2.4 as the packets that he intercepted were using plaintext protocols with no encryption so John was able to use the login details that he intercepted to access her account and pretend to be her completing the risk shown in 5.4.4. This one has been assigned the CWE-300: channel accessible by non-endpoint which has alternate terms of “Man-in-the-Middle / MTITM” and “Monkey-in-the-middle” (CWE-300: Channel Accessible by Non-Endpoint (4.6), n.d.). This attack falls under Spoofing in the STIDE framework. (See 5.1.4, 5.2.4, 5.3.4 and 5.4.4 in the Appendix

The fifth proposed attack shows John using a website known as a “booter” that allows users to pay a subscription fee and use their service of launching a DDoS attack at a given IP address taking advantage of the single point of failure vulnerability shown in 5.2.5. He passes on the IP address of the server hosting the PATs application and within a few seconds he notices that PATs no longer is responding. This attack uses the Denial of Service Attack shown in 5.3.5 and the vulnerability of a single point of failure completing the overall risk shown in 5.4.5. This risk has the common weakness enumeration of CWE-400: Uncontrolled Resource Consumption (CWE-400: Uncontrolled Resource Consumption (4.6), n.d.) and by default we have assigned this the Denial of Service category from STRIDE.

Our sixth proposed attack interestingly shows that both John and Jessica are the attackers in this scenario as well as showing that Jessica herself could be a vulnerability to a system. (See 5.2.6 in Appendix). We see John performing a uncommon attack known as a USB drop attack where he loads up several rubber duckies he purchased anonymously from Hak5 with standard ransomware that he can control and drops all the USB devices carrying the ransomware outside the local PAT studio where Jessica works; seen in 5.3.6. She arrives at work and finds the USBs and picks a USB up and puts it in her pocket in which she plugs it into her computer during her lunch break and within a couple seconds the entire PATs network has been locked by John who is now requesting one hundred thousand to be sent to a bitcoin wallet address which completes risk 5.4.6. This attack could fall under several of the STRIDE framework categories; Tampering where John could be tampering with the data that he has locked, Denial of Service in where John has locked out Jessica.

It’s important to note that we could have created an attacker for each scenario but we thought it prudent to focus on the quality of the attackers rather than the quantity of attackers hence why we only have 2 attackers; Jessica and John. CAIRIS has auto generated some interesting

charts and risk diagrams that has given us a good perspective on the security of this system. (See 5.6 in the Apprendix)

Propsed Security Requirements

Now that we have finished modeling the system in its entirety and identified the potential vulnerabilities, threats and risks that could happen, we then identified several security requirements that we could implement to mitigate the aforementioned risks. Our first proposed requirement is to implement and plan mandatory sessions to provide training to the dance instructors to resolve the risk outlined in 5.4.1. The second requirement is making sure that all text boxes sanitise input by not allowing any wildcard character or scripts to help resolve the risk of SQL Injection shown in 5.4.2, In addition we also propose adequate database protection such as passwords and access controls on the databases. Thirdly, we proposed the implementation of a complex password policy that users must have a password longer than 8 characters that include uppercase letters, lowercase letters, symbols and numbers to reduce the risk of bruteforce attacks and dictionary attacks shown in 5.4.3. The fourth requirement will mitigate the risk 5.4.4 which is data theft through a MITM attack by implementing a protocol that encrypts any data being sent over the system. The fifth requirement must be done by the service provider as it will be their job to implement adequate protection like firewalls to block suspicious traffic or attempted DDoS or DoS attacks shown in risk 5.4.5. (See Chapter 6.1, 6.2, 6.3, 6.4 in Appendix)

Costs & Benefits

The majority of our proposed security requirements can be done in house and would require little to no cost for the PAT team. The first requirement would cost the PATs team no money to implement as creating the tutorials would be an easy task to do and would only cost Jessica a couple hours of her time and would benefit the PATs team immensely as previously mentioned that 95% of breaches are from human error. Implementing database protection would also cost the PATs team a low amount as assumingly the database will be hosted on site or from an external provider which means implementing these requirements would be free from any cost other than the cost to host the database. Jessica would not be affected by this requirement as it will most likely be another member of staff who handles the technology. Again, the PATs team would benefit immensely as it reduces the risk of information disclosure and potential GDPR fines. Implementing a complex password policy would be free as this can be implemented in the design and would not cost any users anything. This reduces the chance of bruteforce which again benefits the PATs team. The fourth requirement being implementing encryption should also not cost the PATs team or any users anything as this would be done behind the scenes in the implementation stage. Finally and presuming that this requirement will cost the most is Implementation of serverside protection such as firewalls as some providers must charge additional fees for different levels of buffers to protect against DoS or DDoS attacks.

Appendix

1.1 - Personas

1.1.1 - Roles

Role	Description
Dance Instructor	The dance instructors who currently work with the local PAT team.
Dance Student	The students who attend the local PAT team’s classes.
Attacker	The malicious threat actor is attacking the PATs application.

1.2 Jessica

Activities: Jessica arrives early at work to prepare for her lessons before any of her dance students arrive. She is extremely busy and moves around a lot to meet each of her dance groups. She needs to be flexible in case she ever needs to fill in for another dance instructor. In her free time; in between lessons, she reads up on dance techniques, evaluates students and develops and plans lessons and the curriculum.

Attitudes: Jessica absolutely loves her job. She loves shaping young minds and encouraging the children to take up a passion of theirs and she gets an emotional fulfillment when her students go on to dance in the local events. She's very old school which means she's hesitant to use the new PATs system, however she is willing to learn how to use it if it will help her students.

Aptitudes: Jessica holds a bachelor's degree in dance. She also holds a mandatory qualification for first aid and CPR. She is a quick study and able to change the way she dances to keep modern.

Motivations: Jessica's motivation is the kids. She loves to teach each of her students and loves the feeling of achievement she gets when her students are picked for an upcoming local dance event.

Skills: Jessica is physically fit from all her years of dancing. She is very creative, organised and very dependable. She's great at motivating her students and communicates effectively with all her students.

Contextual Trust: Jessica's Contextual Trust in this system is that she uses the PATs application as it was meant for with no alternative agenda

Intrinsic Trust: Jessica as a teacher who looks after children has an intrinsic trust to prioritise the children's health and safety and not to harm them in any way. As a teacher, she also is expected not to share any information that legally or morally she shouldn't share.

1.3 Jessica’s Factoids

1. Jessica teaches several different dance styles and techniques
2. but specialise in ballet.
3. She arrives early at school to set up for the day
4. where she choreographed routines and selects appropriate music for upcoming recitals and concerts
5. develops and plans her dance curriculum and lesson plans
6. She has an extremely busy day where she teaches and leads several different classes and age groups.
7. These classes are dotted around the campus in different classes and studios so Jessica is always on the move.
8. Before her students arrive she first gets changed into appropriate dance clothing.
9. Now that her students have arrived she starts by demonstrating how to warm up, move safely then some dance moves
10. Jessica’s love for dance means that she is a very bubbly person who can easily engage, motivate and communicate with her diverse group of students.
11. In her free time she provides feedback and evaluates her students and suggests improvements
12. Jessica’s job to select the students who will be selected and to help with costume fittings and makeup calls.
13. Jessica teaches an afterschool club in which she promotes it and markets it throughout the day on campus.
14. Jessica is a very organised person and is great at managing her time,
15. Every now and then Jessica has to fill in for another dance instructor.
16. She currently holds a bachelor's degree in dance and holds several first aid certificates including first aid.
17. Her years of dance experience means she is very physical and in great health.
18. she is extremely disciplined and can remain calm in stressful situations.
19. She is considered a great leader with the ability to work with any other dance instructor.
20. which has provided a safe and creative place for her students
21. She is naturally a brilliant dancer and she is very good at keeping up to date with new dance techniques.
22. She prefers to use initiative to solve problems and tries to reinforce a degree of dependability for her students.

23. After her after school club is where she spends an hour recording her student's performance and progresses, assesses student’s exams performance and writes up the plan for the following week.

Factoid	Title	Description	Source	Link
1	Choreograph routines	Dance instructors must choreograph routines for their students and select the proper music for recitals and concerts.	1 / 2	4
2	Evaluate Performance	They evaluate the performance of their students.	1	11
3	Suggestion Providement	Provide suggestions and recommendations for improvement.	1	11
4	Specaializes in Ballet	Dance instructors can specialize in one or more dance genres such as ballet, ballroom, or hip-hop.	1	2
5	First Aid	Administer first aid when needed and hold CPR certification.	1	16
6	After School club	Provide a specific hour and fifteen minutes for club time which includes arts and crafts, zumba, rec.	1	13
7	Marketing	Brand, market, and promote the dance team through on campus; alumni; community; and sporting events.	1	13
9	Flexibillity with Teaching schedule	Fill in teaching positions when need (ballet, jazz, lyrical, pointe, and tap)	1	15
9	Organised	Be able to organise and manage time well and organisation of information.	1	14
10	Commitmed	Attend costume fittings, photography sessions, and makeup calls associated with dance performances.	1	12
11	Teach Various Styles and techniques	Teaching students other various styles and techniques of different dance genres.	2	1
12	Leading Classes	Leading dance classes for individuals and groups.	2	6
13	Multiple	Works at the schools, studios and other such	2	7

	Classrooms	dance facilities.		
14	Develop Dance Curriciulms	Develop and plan the current dance curriculums.	2	5
15	Prepare lessons	Prepare and plan lesson plans for students.	2	5
16	Communicatio n	Communicate with a diverse group of individuals.	2	10
17	Engagable	Engage and motivate students.	2	10
18	Safe and creative space	Be able to provide a safe and inclusive and creative place for their students.	2	20
19	Dance Knowledge	Keep up to date in dance techniques and make changes accordingly.	2	21
20	Good Shape	Physically be in good shape and have good cardio	2	17
21	Dependability	Have a degree of dependability for the students.	2	22
22	Discipline	A performing arts teacher will need a strong foundation in the discipline itself	3	18
23	Early	Always be at least fifteen minutes early.	4	3
24	Dress the part	First you must dress the part. Looking well groomed and ready to teach the class in the right way is very important.	4	8
25	Always be prepared	Make a plan each week, and proceed with the plan. Make it flexible so you can change direction if needed, but I recommend that you never go into a class not knowing what you are going to do.	4	23
26	Warmups	show students how to warm up and move safely	5	9
27	Demonstration	demonstrate how to perform dance moves	5	9
28	Dance Design	design dance pieces and performances	5	5
29	Keeping records	keep records of students' performance and progress	5	23
30	Providing Feedback	Provide feedback to students	5	11

31	Dance Exams	Assess students for dance exams	5	23
32	Maintaining Dance Skills	Maintain your own dance skills and techniques	5	21
33	Fine art knowledge	Knowlewdge of the fine arts	5	22
34	Knowledge of Teaching and designing courses	Knowledge of teaching and the ability to design courses	5	22
35	Initiative	The ability to use your initiative	5	22
36	Communicatio n Skills	Excellent verbal communication skills	5	10
37	Teamwork	The ability to work well with others	5	19
38	Leadership	Leadership skills	5	19
49	Patience	Patience and the ability to remain calm in stressful situations	5	18

1.4 Affinity Diagrams

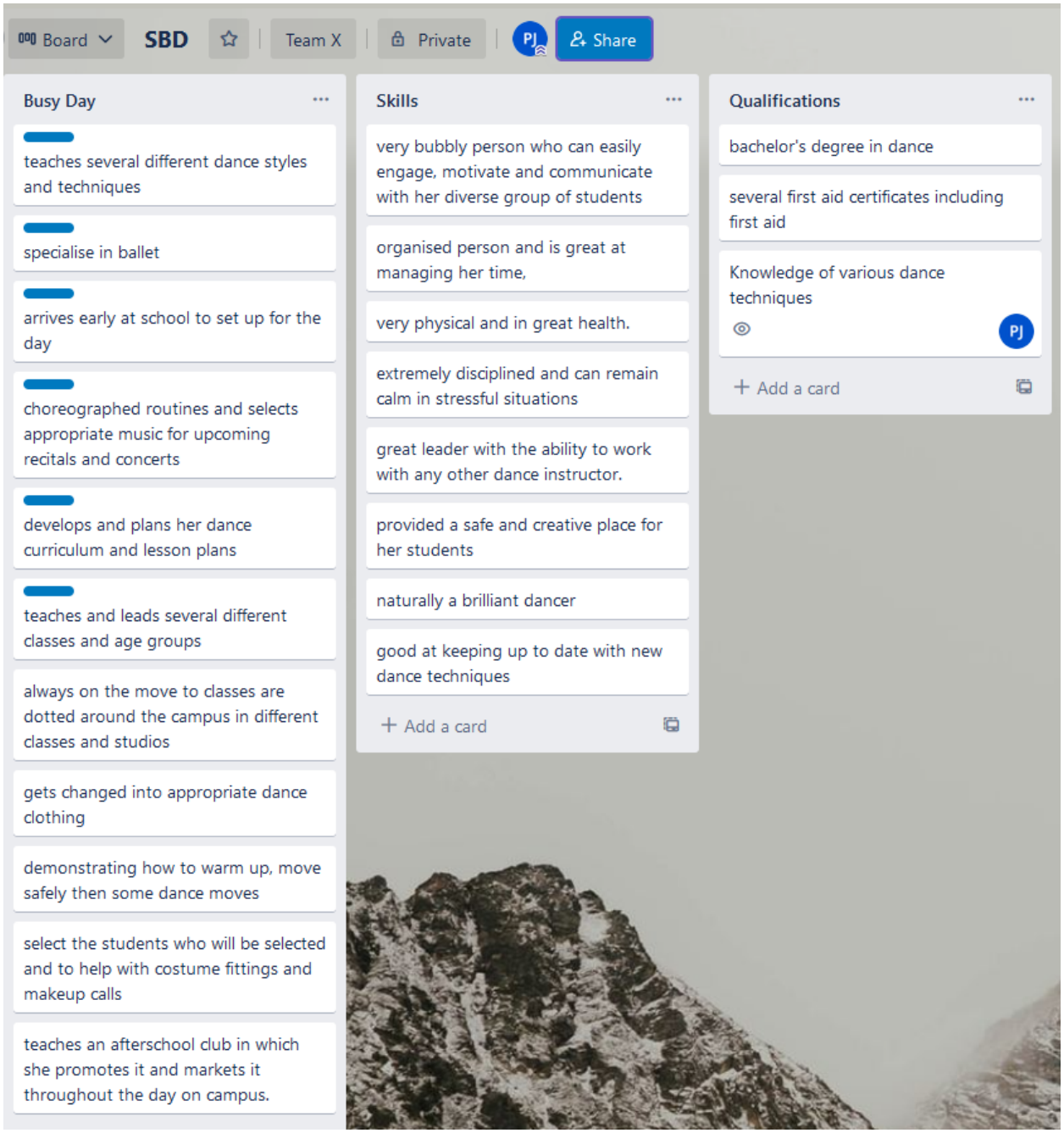

Figure 1: 1.4 Affinity Diagrams. (Trello, n.d.)

1.5 Lily

Activities: Lily wakes up in the morning and gets ready for class, she uses the PATs application to check her sessions then leaves for class. She attends several classes over the day and then leaves to go home at the end of the day.

Attitudes: Lily's love and passion are for dance, she is thrilled that she has the opportunity to attend her local classes and loves when Jessica teaches her as both share a passion for dance.

Aptitudes: Lily is a quick study when it comes to Dance, she's naturally great at dancing and can easily do any other technique after a quick practice session.

Motivations: Lily's motivation for dance is mainly love for the arts but her mother was a professional dancer and she wants to follow in her footsteps.

Skills: Lily is a very motivated person when it comes to dance, she's naturally skilled in all techniques and has brilliant endurance for those long dance periods and shows.

2.1 - Assets

The following appendix describes the assets that we have identified for PATs.

2.1.1 - Software

PATs Application		
Attribute	**Description**	
Type	Software	
Description	The app will be installed on both the instructor's and students' devices.	
Significance	Critical	
Security Properties		
Property	**Value**	**Rationale**
Confidentiality	High	Breaches of confidentiality of this system could impact either instructors or students personal data which could result in potential breach of GDPR compliance.
Integrity	Medium	Tampering of this system could only result in impacting students or instructors schedules of tuition sessions.
Availability	High	This system is the key feature that all instructors and students will be using. The availability impacts the use of this system by not allowing any data subjects or processors access to the system.

2.1.2 - Hardware

Student’s Devices	
Attribute	**Description**
Type	Hardware
Description	The devices used by the students to access and use the PATs app. These could be any smart device able to download or connect to the PATs app; Android, Apple, Windows, Etc.
Significance	High
Security Properties	

Property	Value	Rationale
Availability	High	The device that the student is using must be working for them to be able to access the PATs app.

Instructor’s Device		
Attribute	**Description**	
Type	Hardware	
Description	The devices used by the teachers and instructors to access and use the PATs app. These could be any smart device able to download or connect to the PATs app; Android, Apple, Windows, Etc.	
Significance	High	
Security Properties		
Property	**Value**	**Rationale**
Availability	High	The device that the instructors are using must be working for them to be able to access the PATs app.

2.1.3 - Information

Scheduled Tuition Session		
Attribute	**Description**	
Type	Information	
Description	The tuition session scheduled and assigned by instructors.	
Significance	Critical	
Security Properties		
Property	**Value**	**Rationale**
Confidentiality	Medium	The scheduled tuition session would not contain any data that would be too private. Assuming it would only contain the instructor, students, time and place.
Integrity	Medium	The impact on integrity would only affect student's and instructor's sessions.
Availability	High	The impact of availability would mean that students and instructors would not be aware of when and where they're supposed to be.

Upcoming Events		
Attribute	**Description**	
Type	Infomration	
Description	The Upcoming events and additional resources shared on PATs	
Signifiance	High	
Security Properties		
Property	**Value**	**Rationale**
Integrity	Medium	Tampering of the upcoming events would mean false information to be told to students and instructors.
Availability	High	A breach of availability for the upcoming events would only mean that students and instructors are unable to see what is coming up.
Accountability	Medium	Those that submit any information to upcoming events should be held accountable for any information that shouldn't have been uploaded.

Confirmation Message		
Attribute	**Description**	
Type	Information	
Description	A message confirming a student’s tuition session confirmation.	
Signifiance	Critical	
Security Properties		
Property	**Value**	**Rationale**
Confidentiality	Medium	The confirmation message would not contain any data that would be too private. Assuming it would only contain the session details, instructions and resources
Integrity	Low	The impact on integrity would only affect the details that students receive. May cause them to miss their sessions.
Availability	High	The message needs to be available for the student to know that their session has been confirmed.

Requests		
Attribute	**Description**	
Type	Information	
Description	Tuition requests sent to the related instructor's PATs App on their device.	
Significance	Critical	
Security Properties		
Property	**Value**	**Rationale**
Confidentiality	Low	May only contain data that wouldn't be classified as confidential; Time, Class, Instructor.
Integrity	Low	Breach of integrity of requests would only mean that the time and place of the session and the student would only be tampered with.
Availability	Medium	The request needs to be available for the instructors to see and book the session.

Tracking Information		
Attribute	**Description**	
Type	Information	
Description	Tuition requests sent to the related instructor's PATs App on their device.	
Significance	Critical	
Security Properties		
Property	**Value**	**Rationale**
Confidentiality	Low	The impact of a breach wouldn't leak any important or confidential information.
Integrity	Low	Tampering would only be able to change the hours worked by instructors and sessions attended by students.
Availability	Low	This information would most likely be used during a standard and regular time frame such as monthly or academic season so impact on availability would be low in most periods.

ID Number		
Attribute	**Description**	
Type	Information	
Description	Unique ID numbers used to identify Students and Instructors	
Significance	Critical	
Security Properties		
Property	**Value**	**Rationale**
Accountability	High	These IDs ensure the actions of an entity may be traced uniquely to an entity.

Passwords		
Attribute	**Description**	
Type	Information	
Description	Passwords are used alongside ID numbers to access individual accounts on PATs.	
Significance	Critical	
Security Properties		
Property	**Value**	**Rationale**
Confidentiality	High	These passwords must be kept private so unauthorised threat actors do not gain access.
Integrity	High	Tampering with passwords ensures that users are unable to access their accounts.

User Database	
Attribute	**Description**
Type	Information
Description	The database where IDs for both students and instructors as well as their passwords are stored. In addition, confidential data is stored here regarding students' and instructors' personal details.
Significance	Critical

Security Properties		
Property	**Value**	**Rationale**
Confidentiality	High	Breach of confidentiality could result in unauthorised access of accounts.
Integrity	High	The impact of a breach of integrity could see personal details being changed and altered.

2.1.4 - People

Students	
Attribute	**Description**
Type	People
Description	The students themselves have enrolled and are using the PATs app.
Significance	Low

Security Properties		
Property	**Value**	**Rationale**
Availability	Low / None	Students themselves have to be available for them to use the PATs app.

Instructors	
Attribute	**Description**
Type	People
Description	The Instructors and teachers themselves are using the PATs app.
Significance	Low

Security Properties		
Property	**Value**	**Rationale**
Availability	Low / None	Instructors themselves have to be available for them to use the PATs app.

2.1.5 - Systems - General

Unamed Hosting Service		
Attribute	**Description**	
Type	Systems - General	
Description	The hosting service that will be hosting the application allows for remote connections.	
Signifiance	Critical	
Security Properties		
Property	**Value**	**Rationale**
Availability	High	Breach of availability would impact the usage by not allowing anyone to connect.

2.2 Asset Assocations

Head	**Multiplicity**	**Multiplicity**	**Tail**
Student	*	1	ID Number
Student	*	1	Passwords
ID Number	1	1..*	Students Devices
Passwords	1	1..*	Students Devices
Students Devices	1..*	1	PATs App
Instructors	*	1	ID Number
Instructors	*	1	Passwords
ID Number	1	1..*	Instructors Devices
Passwords	1	1..*	Instructors Devices
User Database	1	*	ID Number
User Database	1	*	Passwords
PATs App	1	*	Request

PATs App	1	1	Scheduled Tuition Session
PATs App	1	1	Tracking Information
PATs App	1	1	Upcoming Events
PATs App	1	1	User Database
Request	*	1	Scheduled Tuition Session
Unamed Hosting Service	1	1	PATs App

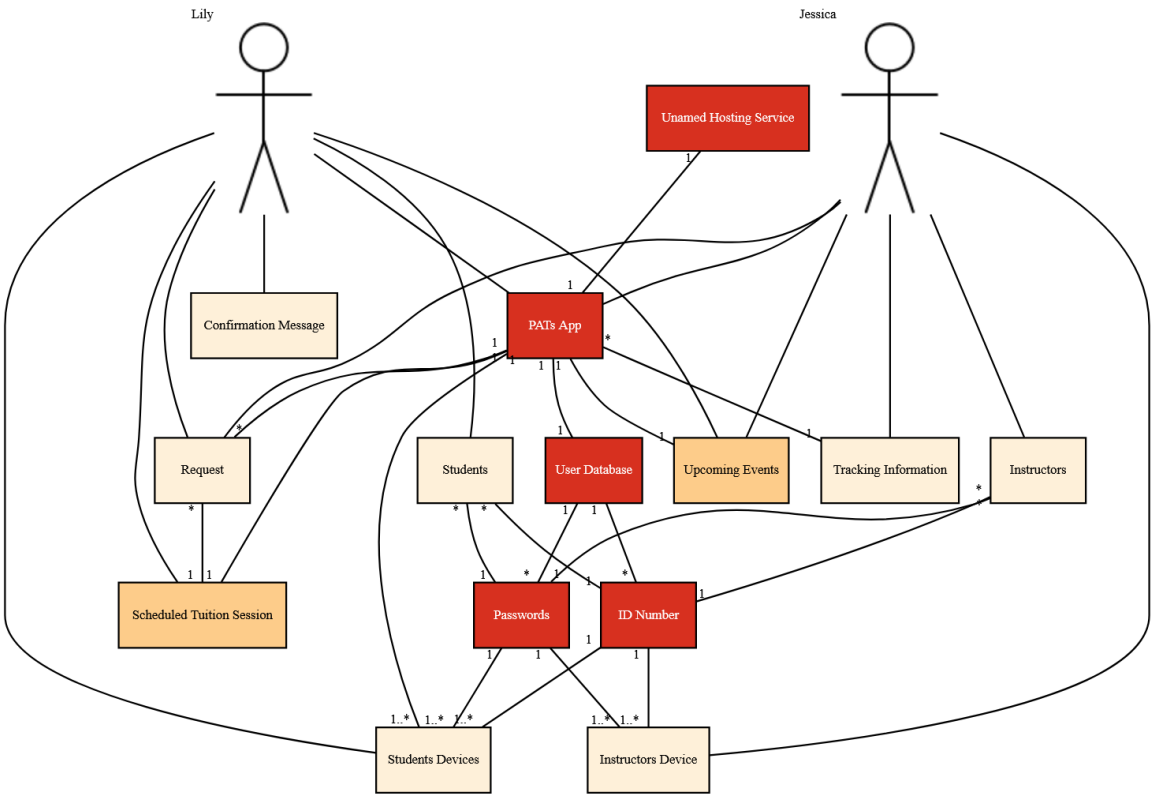

Figure 2: Asset Association. (CAIRIS.)

3.1 Tasks

3.1.1 Submit tuition session request

Lily uses her smart device to connect to the PATs application and fill out a request form to submit to request a session with Jessica.

Task Information	
Title	**Description**
Objective	Submit a tuition session request through the PATs application.
Participants	
Persona	Lily
Duration	Minutes
Frequency	Daily - Weekly
Demands	High
Goal Conflict	None
Assests Concerns	
Students Devices	She uses her smart device to access PATs.
PATs App	Lily uses the PATs Application to submit her request.
Students	Lily herself counts as a people type asset and she is the main author of this task.
Scheduled Tuition Session	Her request once confirmed will be uploaded and her session scheduled.
Confirmation Message	Once Lily’s session is scheduled she will receive a confirmation message.
Request	Lily’s request itself counts as an informational asset and the asset itself is the main feature of this task.

3.1.2 Uploading Upcoming Events

Lily uses her smart device to connect to the PATs application and fill out a request form to submit to request a session with Jessica.

Task Information	
Title	**Description**
Objective	To upload the upcoming events to the PATs application.
Participants	
Persona	Jessica
Duration	Minutes
Frequency	Daily - Weekly
Demands	High
Goal Conflict	None
Assests Concerns	
Instructors Devices	Jessica will use her workstation to access PATs
PATs App	Jessica uses PATs to upload information relating to an upcoming event.
Instructors	Jessica herself counts as a people type asset and is the main author of this task.
Upcoming Events	Jessica uploads relevant information to the upcoming events section.

3.1.3 Tracking Instructor's Hours and Student's Sessions Attended

Jessica uses the PATs software to track and see how many hours each instructor has put it and how many sessions Lily has attended.

Task Information	
Title	**Description**
Objective	To use PATs to track the hours of each instructor and sessions attended by students
Participants	
Persona	Jessica

Duration	Minutes
Frequency	Monthly or less
Demands	High
Goal Conflict	None
Assests Concerns	
Instructors Devices	Jessica will use her workstation to access PATs
PATs App	Jessica uses PATs to view the tracking information stored on it
Instructors	Jessica herself counts as a people type asset and is the main author of this task.
Tracking Information	The tracking information is the data Jessica wants to access to see how many sessions Lily has attended.

3.1.4 Manually Matching Tuition Requests

Jessica uses the PATs application to manually match tuition requests to related insturctors.

Task Information	
Title	**Description**
Objective	To manually match tuition requests to the related instructors.
Participants	
Persona	Jessica
Duration	Minutes
Frequency	Hourly or more
Demands	High
Goal Conflict	None
Assests Concerns	
Instructors Devices	Jessica will use her workstation to access PATs.
PATs App	Jessica uses PATs to view the tuition requests.
Instructors	Jessica herself counts as a people type asset and is the main author of this task.

Request	Jessica reviews the requests and manually matches Lily's request.

3.1.5 Viewing Upcoming Events

Lily uses the PATs application to view the upcoming events posted by Jessica.

Task Information	
Title	**Description**
Objective	To view the upcoming events through the PATs application.
Participants	
Persona	Jessica
Duration	Minutes
Frequency	Hourly or more
Demands	High
Goal Conflict	None
Assests Concerns	
Students Devices	Lily uses her device to access the PATs application.
PATs App	Lily uses PATs to view the upcoming events.
Students	Lily herself counts as a people type asset and she is the main author of this task.
Upcoming Events	The upcoming events are the reason why Lily is doing this task.

3.1.6 Viewing Tuition Sessions

To use the PATs application to view tuition sessions.

Task Information	
Title	**Description**
Objective	To view the upcoming events through the PATs application.
Participants	
Persona	Lily
Duration	Minutes

Frequency	Daily - Weekly
Demands	High
Goal Conflict	None
Assests Concerns	
Students Devices	Lily uses her device to access the PATs application.
PATs App	Lily uses PATs to view the upcoming events.
Students	Lily herself counts as a people type asset and she is the main author of this task.
Scheduled Tuition Session	This task is Lily searching the scheduled tuition sessions for her next session booked with Jessica

4.1 Use Cases

4.1.1 Requesting Tuition Sessions

Actors: Dance Student
Description / Objective: The student will use PATs to request a session from a dance instructor.
Pre-conditions:

1. The PATs application must be working correctly.
2. The student's device must be working.

Steps:

1. Lily uses her device to access PATs
2. She Naviagetes to the requests form and fills it out then submits it

Postconditions:

1. PATs accept the request, schedules and sends a confirmation message to Lily's device.
2. Lily's session is now scheduled and the new information can be found on the scheduled sessions.

4.1.2 Adding Upcoming Events Information

Actors: Dance Instructor
Description / Objective: To use PATs application to upload the upcoming events.
Pre-conditions:

1. The PATs application must be working correctly.
2. The Dance Instructor's device must be working.

Steps:

1. Jessica will use her device to connect to PATs app
2. She now navigates to the upcoming events page where she fills out the needed information and uploads any images needed.

Postconditions:

1. PATs accept the request, schedules and sends a confirmation message to Lily's device.
2. Lily's session is now scheduled and the new information can be found on the scheduled sessions.

4.1.3 Viewing Instructor's and Student's Performance

Actors: Dance Instructor
Description / Objective: To use the PATs application to view the hours that instructors have put in and the sessions attended by students that PATs track.
Pre-conditions:

1. The PATs application must be working correctly.
2. The Dance Instructor's device must be working.

Steps:

1. Jessica will use her device to connect to PATs app
2. She now navigates to the tracking section.

Postconditions:

1. She now has access to and sees the tracking information.
2. The tracking information has been reviewed for their given purpose.

4.1.4 Matching Tuition Requests

Actors: Dance Instructor
Description / Objective: To use PATs to read student's requests and to manually assign and match them to the related instructor.
Pre-conditions:

1. Lily's device must be working
2. Jessica's device must be working
3. Both must be able to connect to PATs

Steps:

1. Jessica uses her device to connect to PATs app
2. She navigates to the request section
3. Reads and organise the requests
4. Check with the instructor's booked sessions
5. Match the request with a free slot on the instructors time
6. Sends a confirmation to the instructors device

Postconditions:

1. Lily now has a session booked
2. Confirmation message sent to Jessica's device

4.1.5 Viewing the upcoming events

Actors: Dance Student
Description / Objective: To use the PATs application to view the upcoming events posted by the dance instructors.
Pre-conditions:

1. The PATs application must be working correctly.
2. The student's device must be working.

Steps:

1. Lily uses her device to access PATs
2. She navigates to the upcoming events section

Postconditions:

1. Lily has now viewed the upcoming events

4.1.6 Viewing Lily’s Tuition Sessions

Actors: Dance Student

Description / Objective: To use PATs application to view her upcoming tuition session.
Pre-conditions:

1. The PATs application must be working correctly.
2. The student's device must be working.

Steps:

1. Lily uses her device to access the PATs system
2. She navigates to her booked tuition sessions

Postconditions:

1. Lily has now seen her booked tuition sessions

4.2 Data Flow*

Due to poor formatting with data flow diagrams on CAIRIS, it was extremely difficult to read and understand the flow of data so Lucidchart was used to create and upload readable data flow diagrams.

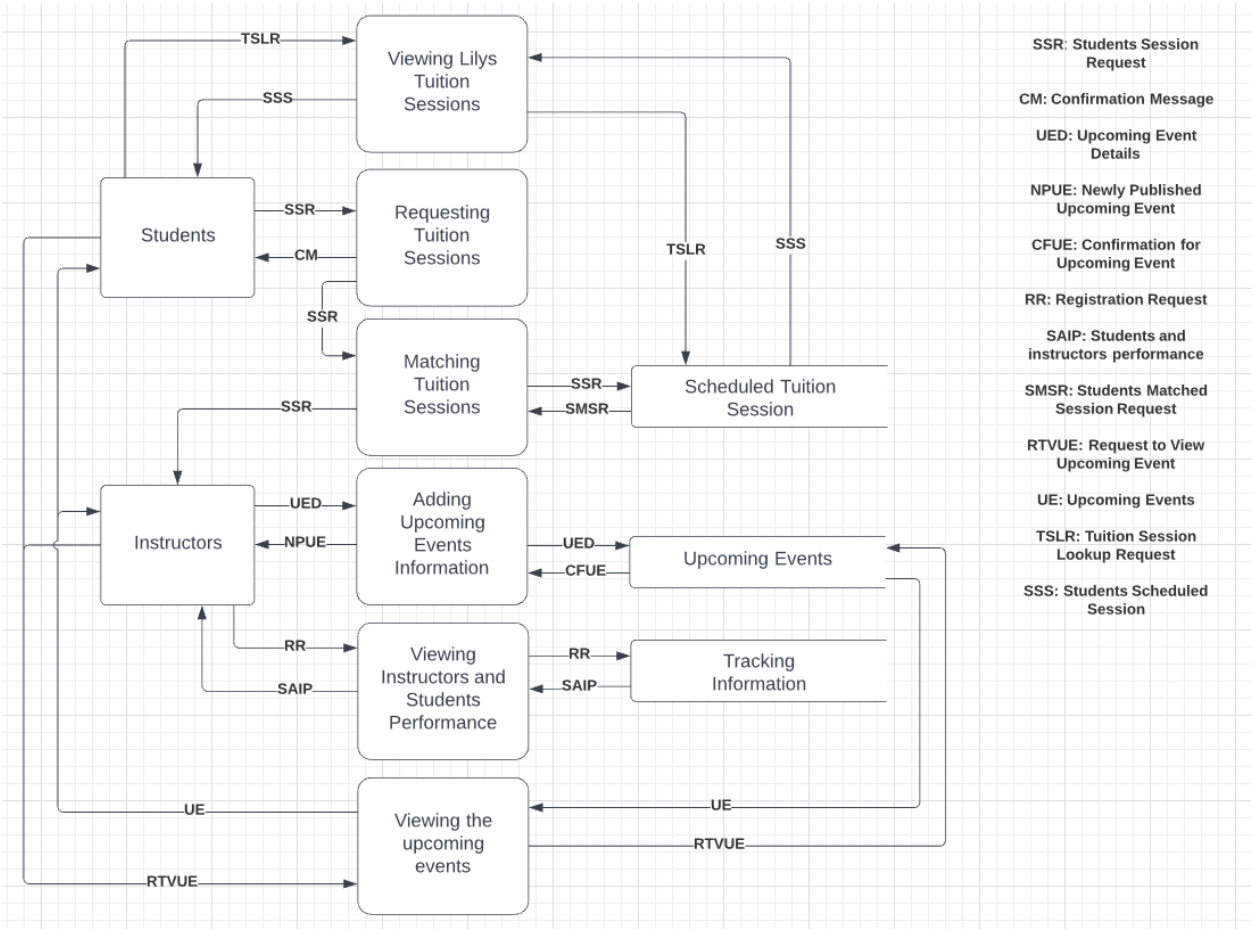

Figure 3: 4.2 PATs Data Flow Diagram. (Intelligent Diagramming | Lucidchart, n.d.)

4.2.1 Requesting Tuition Sessions*

Data	From	From - Type	To	To - Type	Asset
Students Session Request	Students	Entity	Requesting Tuition Sessions	Process	Request
Confirmation Message	Requesting Tuition Sessions	Process	Student's Device	Entity	Confirmation Message

It seems like 4.2.1 doesn't have much of a flow throughout the system as the majority of this task's flow is done behind the curtain with 4.2.4

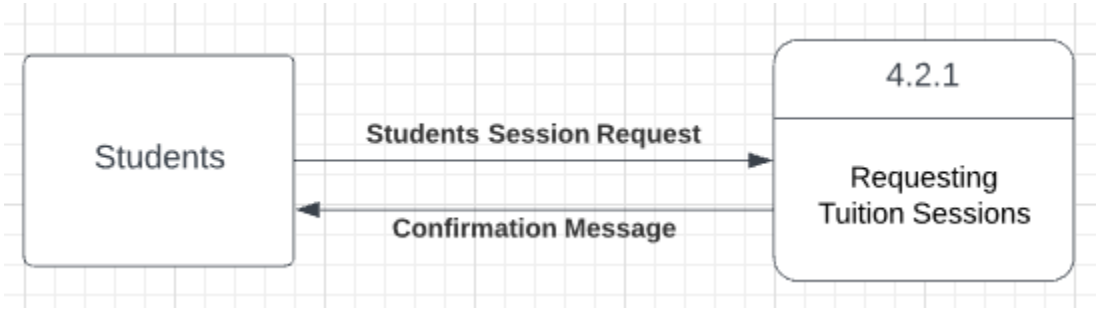

Figure 4: 4.2.1 Data Flow Diagram. (Intelligent Diagramming | Lucidchart, n.d.)

4.2.2 Adding Upcoming Events Information

Data	From	From - Type	To	To - Type	Asset
Upcoming Event Details	Instructors	Entity	Adding Upcoming Events Information	Process	Upcoming Events
Upcoming Event Details	Adding Upcoming Events Information	Process	Upcoming Events	Datastore	Upcoming Events
Confirmation for Upcoming Event	Upcoming Events	Datastore	Adding Upcoming Events Information	Process	Upcoming Events
Newly Published Upcoming Event	Adding Upcoming Events Information	Process	Instructors	Entity	Upcoming Events

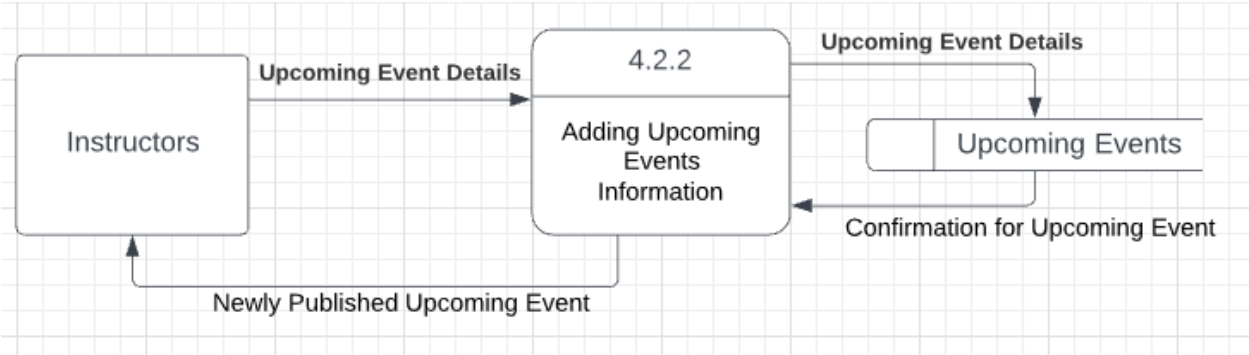

Figure 5: 4.2.2 Data Flow Diagram. (Intelligent Diagramming | Lucidchart, n.d.)

4.2.3 Viewing Instructor's and Student's Performance

Data	From	From - Type	To	To - Type	Asset
Registration Request	Instructors	Entity	Viewing Instructors and students performance	Process	Request
Registration Request	Viewing Instructors and students performance	Process	Tracking Information	Datastore	Request
Students and Instructors Performance	Tracking Information	Datastore	Viewing Instructors and students performance	Process	Tracking Information
Students and Instructors Performance	Viewing Instructors and students performance	Process	Instructors	Entity	Tracking Information

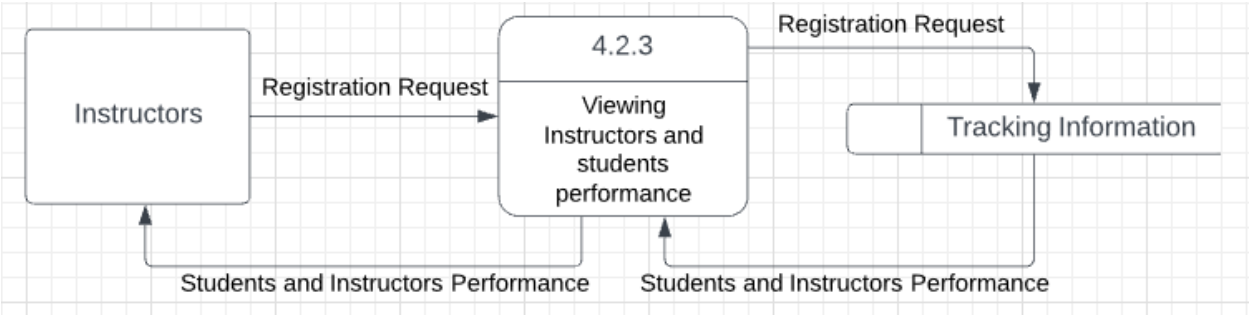

Figure 6: 4.2.3 Data Flow Diagram. (Intelligent Diagramming | Lucidchart, n.d.)

4.2.4 Matching Tuition Requests

Data	From	From - Type	To	To - Type	Asset
Students Session Request	Requesting Tuition Sessions	Process	Matching Tuition Requests	Process	Request
Students Matched Session Request	Matching Tuition Requests	Process	Instructors	Entity	Request
Students Matched Session Request	Scheduled Tuition Session	Datastore	Matching Tuition Requests	Process	Request Confirmation Message
Students Session Request	Matching Tuition Requests	Process	Scheduled Tuition Session	Datastore	Request

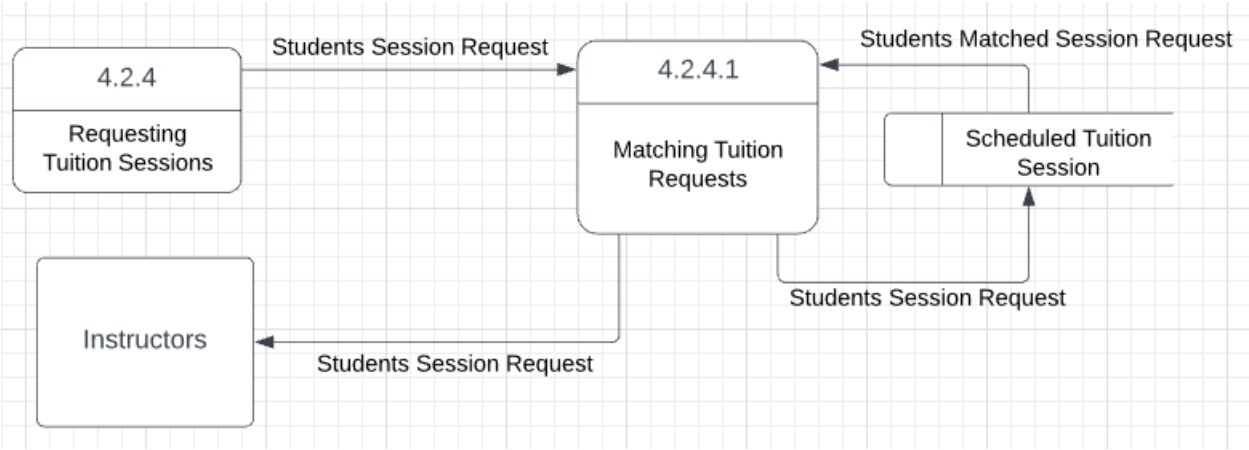

Figure 7: 4.2.4 Data Flow Diagram. (Intelligent Diagramming | Lucidchart, n.d.)

4.2.5 Viewing the upcoming events

Data	From	From - Type	To	To - Type	Asset
Request to View Upcoming Event	Instructors	Entity	Viewing the upcoming events	Process	Request

Request to View Upcoming Event	Students	Entity	Viewing the upcoming events	Process	Request
Request to View Upcoming Event	Viewing the upcoming events	Process	Upcoming Events	Datastore	Request
Upcoming Events	Upcoming Events	Datastore	Viewing the upcoming events	Process	Upcoming Events
Upcoming Events	Viewing the upcoming events	Process	Instructors	Entity	Upcoming Events
Upcoming Events	Viewing the upcoming events	Process	Students	Entity	Upcoming Events

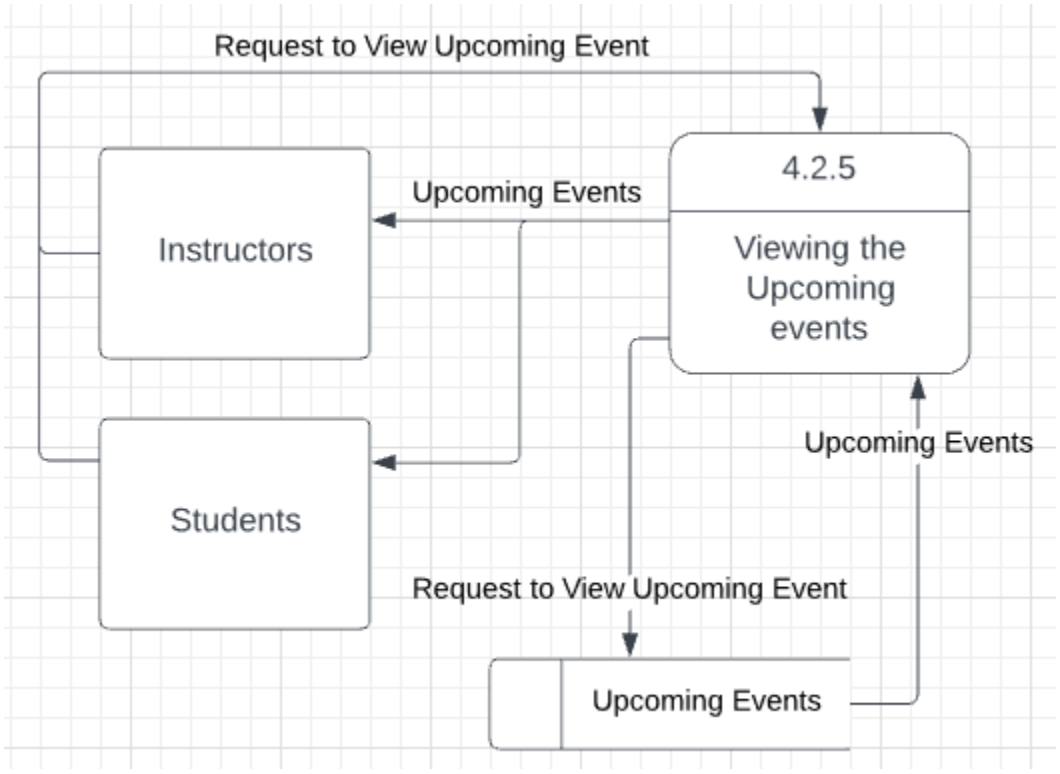

Figure 8: 4.2.5 Data Flow Diagram. (Intelligent Diagramming | Lucidchart, n.d.)

4.2.6 Viewing Lily's Tuition Sessions

Data	From	From - Type	To	To - Type	Asset
Tuition Session Lookup Request	Students	Entity	Viewing Lilys Tuition Sessions	Process	Request
Tuition Session Lookup Request	Viewing Lilys Tuition Sessions	Process	Scheduled Tuition Session	Datastore	Request
Students Scheduled Session	Scheduled Tuition Session	Datastore	Viewing Lilys Tuition Sessions	Process	Scheduled Tuition Session
Students Scheduled Session	Viewing Lilys Tuition Sessions	Process	Students	Entity	Scheduled Tuition Session

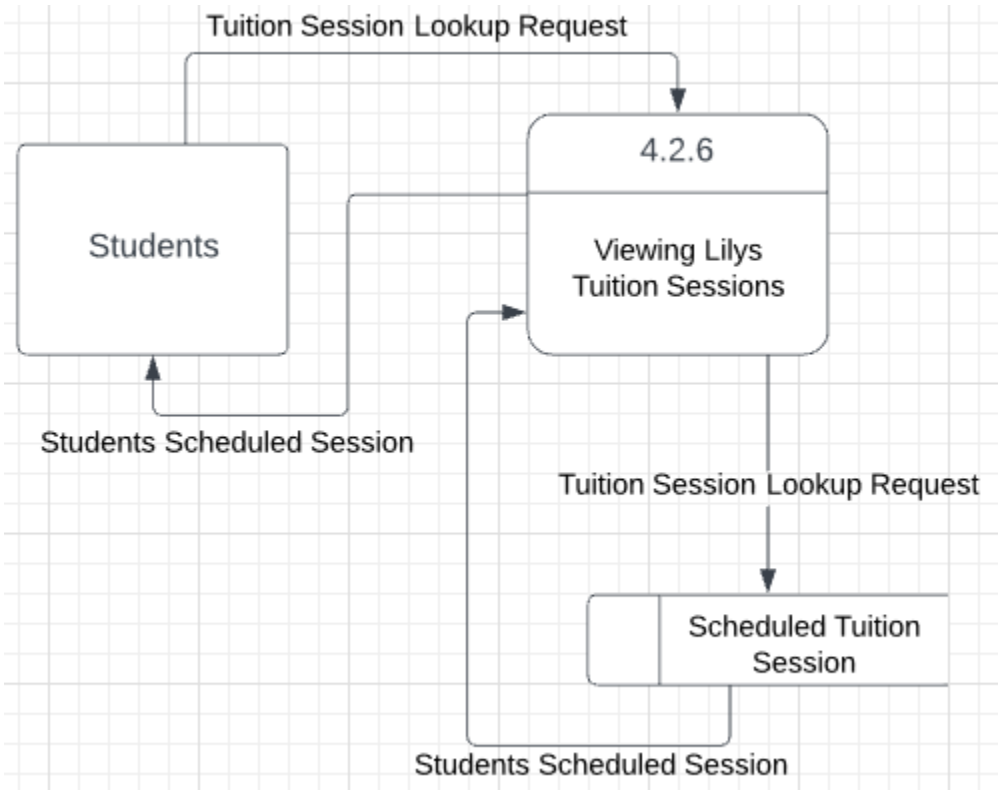

Figure 9: 4.2.6 Data Flow Diagram. (Intelligent Diagramming | Lucidchart, n.d.)

5.1 Attackers

Chapter 5.1 describes the attackers that we create that gives us a good idea on how the system can be exploited with additional context of these attackers. These attackers will also be shown exploiting the vulnerabilities, threats and risks we create in the rest of chapter 5.

5.1.1 Jessica Richardson

Jessica is a dance instructor currently working in her local community Performing Arts Team. She specializes in Ballet and teaches multiple classes at her school and studios. She doesn't have much experience with Technology so is having a little trouble with the PATs application.

Role	**Motivation**	**Capability**	**Value**
Attacker	Accident	Resources/Personnel and Time	Medium
		Knowledge/Education and Training	Medium
		Resources/Facilities	High
		Resources/Funding	Low
		Technology	Low
		Software	Low
		Resources/Equipment	Low
		Knowledge/Methods	Medium

5.1.2 John Howard

John is a student at the local University where the PATs team has a classroom, John's sister Lily attends and dances there. He is an overachiever and tends to go the extra mile by practising his ethical hacking skills on websites like TryHackMe and HackTheBox.

Role	**Motivation**	**Capability**	**Value**
Attacker	Thrill-seeking	Knowledge/Education and Training	High
		Technology	High
		Software	High
		Resources/Equipment	Medium
		Knowledge/Methods	Medium

5.2 Vulnerabilities

5.2.1 Inadequate User Training

Type: Implementation
Description: Inadequate user training for staff and students.
Severity: Marginal
Assets:

- PATs App
- Scheduled Tuition Session
- Upcoming Events

5.2.2 Unsanitised User Input

Type: Configuation
Description: The backend of the database uses SQL queries when presented to search and organise data. The input however has not been properly set up to prevent any wildcard characters that might manipulate the system in a certain way.
Severity: Catastrophic
Assets:

- ID Number
- Passwords
- PATs App
- User Database

5.2.3 Insuffient Password Policies

Type: Implementation
Description: The PATs have no policies when it comes to creating a complex and safe password to use.
Severity: Critical
Assets:

- Passwords

5.2.4 Unencrypted Data Transfer Protocols

Type: Configuration

Description: Login details are sent over to the user database to confirm whether the login details are correct in plaintext.
Severity: Critical
Assets:

- Passwords
- ID Number
- User Database

5.2.5 Single Point of Failure

Type: Design
Description: The PATs application would be hosted on a single location server which is the unnamed server hosting asset. If this goes down then PATs would not be functional.
Severity: Catastrophic
Assets:

- Unnamed Hosting Service
- PATs App

5.2.6 Jessica Richardson

Type: Implementation
Description: Jessica's lack of knowledge of cyber security has meant that she is the main access point and attack vector of a USB drop attack.
Severity: Catastrophic
Assets:

- Instructors Device

5.3 Threats

5.3.1 Accidential Wrong Use

Type: Insider/Sabotage
Method: Jessica with her lack of training accidentally pushes the incorrect data to the upcoming events.
Likelihood: Probable
Attacker: Jessica Richardson
Asset:

- PATs App
- Upcoming Events
- Students

- User Database

Security Property	Value	Rationale
Confidentiality	High	Confidentiality is breached when Jessica pushes information regarding Lily.

5.3.2 SQL Injection

Type: Insider/Manipulation
Method: John accesses his sister's device and launches the PATs application. John wrote an SQL query that would allow him access to the admin's account.
Likelihood: Improbable
Attacker: John Howard
Asset:

- ID Number
- Password
- PATs App
- Students
- Instructors
- User Database

Security Property	Value	Rationale
Confidentiality	High	Breach of this data will involve confidential data disclosed to this attacker.
Integrity	High	This data contains highly personal data and an impact of tampering would mean that data would be altered such as phone numbers and addresses.
Availability	High	The impact of availability is that the system would not be able to request and decide whether the correct ID number and password were entered.

5.3.3 Weak Passwords

Type: Electronic/Hacking
Method: Using Kali and John the Ripper, John was able to crack and gain access to an admin account.
Likelihood: Incredible
Attacker: John
Asset:

- PATs App
- User Database

Security Property	Value	Rationale
Confidentiality	High	The data John now has access to should have been confidential
Integrity	High	The account John now has access to has the ability to change all data.
Availability	High	The account John now has access to has the ability to delete all the data.

5.3.4 Man In The Middle (MITM)

Type: Electronic/Phising and Spoofing
Method: Using Kali and Wireshark, John intercepts the login request of another student.
Likelihood: Improbable
Attacker:
Asset:

- Passwords
- User Database
- ID Number

Security Property	Value	Rationale
Confidentiality	High	ID numbers and passwords need to be kept confidential.

5.3.5 Denial of Service Attack

Type: Electronic/DoS and DDoS
Method: Using Kali and Wireshark, John intercepts the login request of another student.
Likelihood: Improbable
Attacker: John Howard
Asset:

- Unnamed Hosting Service
- PATs App

Security Property	Value	Rationale

Availability	High	A DoS or DDoS attack would result in a server crash causing an availability impact.

5.3.6 Ransomware Containing USBs

Type: Electronic/Hacking
Method: Jessica finds a USB on the floor and puts it into her computer.
Likelihood: Improbable
Attacker: John Howard, Jessica Richardson
Asset:

- Instructors Device

Security Property	Value	Rationale
Confidentiality	High	Data is breached and confidentiality is broken once John has access to all files.
Availability	High	Device availability has now been broken due to ransomware lock.

5.4 Risks

5.4.1 Confidential Information Disclosure through Human Error

Threat: Accidental Wrong Use
Vulnerability: Inadequate User Training
OWASP Top 10: A02:2021-Cryptographic Failures
Common Weakness Enumeration: CWE-201: Insertion of Sensitive Information Into Sent Data

Impact	
Title	**Value**
Rating	Undesirable
Name	None
Score (Pre Mitigation)	9
Score (Post Mitigation)	9

Misue Case	
Attackers	Jessica Richardson
Assets	Upcoming Events, PATs App, Scheduled Tuition Session
Objective	Exploit Vulnerabilities in PATs App, Scheduled Tuition Session, Upcoming Events
Likelihood	Probable
Severity	Marginal
Narrative	Jessica arrives at work at 7:00 pm and she logs onto her workstation and accesses the PATs application. She receives an email from her boss telling her to upload an upcoming event so her students can see it. While uploading the needed information, she accidentally drags some text from a student's file onto the end of the description of the event and saves it. Now Lily's home address has been posted for everyone to see.
Response	
Mitigate	Prevent Confidential Information Disclosure

5.4.2 Information Disclosure through SQL Injection

Threat: SQL Injection
Vulnerability: Unsanitised User Input
OWASP Top 10: A03:2021 – Injection
Common Weakness Enumeration: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Impact	
Title	**Value**
Rating	Tolerable
Name	None
Score (Pre Mitigation)	9
Score (Post Mitigation)	9
Misue Case	

Attackers	John Howard
Assets	Students, Instructors, User Database, PATs App, Passwords, ID Number
Objective	Exploit vulnerabilities in PATs App, ID Number, Passwords, User Database
Likelihood	Improbable
Severity	Catastrophic
Narrative	John uses his sister's device to gain access to the PATs app. His curiosity to test his new knowledge of SQL Injections gets the better of him and he crafts a query that will already return as true "SELECT * FROM users WHERE username = or 1=1 - -' AND password ='[password]';" Upon posting this as the username on Lily's app he is granted access to the standard admin's account.
Response	
Mitigate	Prevent Information Disclosure through SQL Injection

5.4.3 Privilege Esculation through Dictionary Attack

Threat: Weak Passwords
Vulnerability: Insuffient Password Policies
OWASP Top 10: A07 - Identification and Authentication Failures
Common Weakness Enumeration: CWE-287: Improper Authentication and CWE-521: Weak Password Requirements

Impact	
Title	**Value**
Rating	Negligible
Name	None
Score (Pre Mitigation)	1
Score (Post Mitigation)	1
Misue Case	
Attackers	John Howard
Assets	PATs App, User Database, Passwords

Objective	Exploit vulnerabilities in Passwords to threaten PATs App, User Database.
Likelihood	Incredible
Severity	Critical
Narrative	John gains access to Lily's device and hooks it up to his PC. He starts a Virtual Machine running Kali Linux and connects the phone and launches the PATs application. Upon a little more configuring he has set up John The Ripper to use a dictionary attack on an account with the admin user ID, it takes John a couple of seconds to crack the password; "123456".
Response	
Mitigate	Prevent Privilege Esculation through Dictionary Attack

5.4.4 Data theft through MITM attack

Threat: Man in the middle (MITM)
Vulnerability: Unencrypted Data Transfer Protocols
Common Weakness Enumeration: CWE-300: Channel Accessible by Non-Endpoint

Impact	
Title	**Value**
Rating	Tolerable
Name	None
Score (Pre Mitigation)	9
Score (Post Mitigation)	9
Misue Case	
Attackers	John Howard
Assets	ID Number, Passwords, User Database
Objective	Exploit vulnerabilities to threat ID Number, Passwords, User Database
Likelihood	Improbable

Severity	Critical
Narrative	John while connected to the PATs wifi intercepts a login request sent from a student to PATs that gets authenticated with the user of their user database. This request is sent over plaintext protocols so John while using Wireshark can see the student's user ID and her password. He then exploits this and logs onto her account using her phished details.
Response	
Mitigate	Prevent Data theft through MITM attack

5.4.5 Availability Attack through DoS or DDoS

Threat: Denial of Service Attack
Vulnerability: Single Point of Failure
OWASP Top 10:
Common Weakness Enumeration: CWE-400: Uncontrolled Resource Consumption

Impact	
Title	**Value**
Rating	Tolerable
Name	None
Score (Pre Mitigation)	9
Score (Post Mitigation)	9
Misue Case	
Attackers	John Howard
Assets	Unamed Hosting Service, PATs App
Objective	Exploit vulnerabilities in PATs App, Unamed Hosting Service
Likelihood	Improbable
Severity	Catastrophic
Narrative	John registers and signs up to a website known as a booter which he can pay to launch a DDoS attack against a given IP address. He gives this booter the IP address that is hosting the PATs application and within a few seconds, he notices that he can no longer log in

	using stolen login details. This has caused the PATs Application to no longer work due to the hosting service being flooded and crashing.
Response	
Mitigate	Prevent Availability Attack through DoS or DDoS

5.4.6 Ransomware Attack through USB Drop Attack

Threat: Ransomware Containing USBs
Vulnerability: Jessica Richardson

Impact	
Title	**Value**
Rating	Tolerable
Name	None
Score (Pre Mitigation)	9
Score (Post Mitigation)	9
Misue Case	
Attackers	John Howard, Jessica Richardson
Assets	Instructors Device
Objective	Exploit vulnerabilities in Instructors Device to threaten Instructors Device.
Likelihood	Improbable
Severity	Catastrophic
Narrative	John loads up a bunch of Rubber Duckies with standard ransomware that he drops outside of the local PATs studio where Jessica works. When Jessica arrives at work she notices a USB which she picks up and pockets. During her lunch break she plugs in the USB and within seconds the entire network has been locked by John who is now requesting one hundred thousand to be paid to a bitcoin wallet.
Response	
Mitigate	Prevent Ransomware Attack through USB Drop Attack.

5.5 Risk Model Diagrams

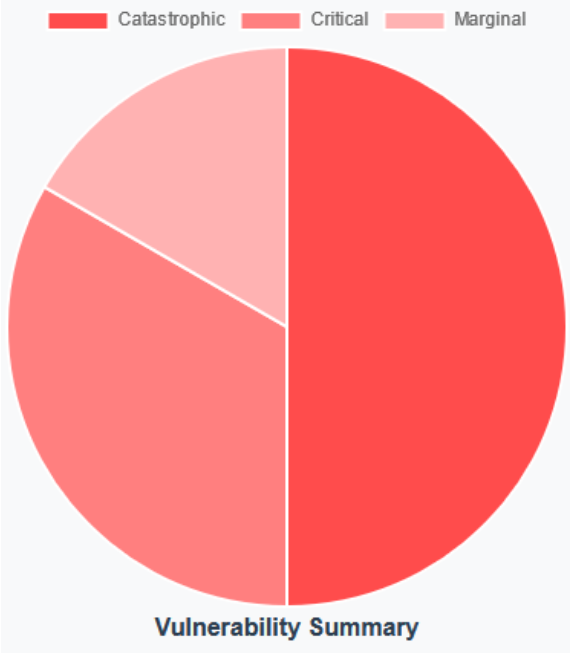

Figure 10: Vulnerability Summary. (CAIRIS.)

Figure 11: Threat Summary. (CAIRIS.)

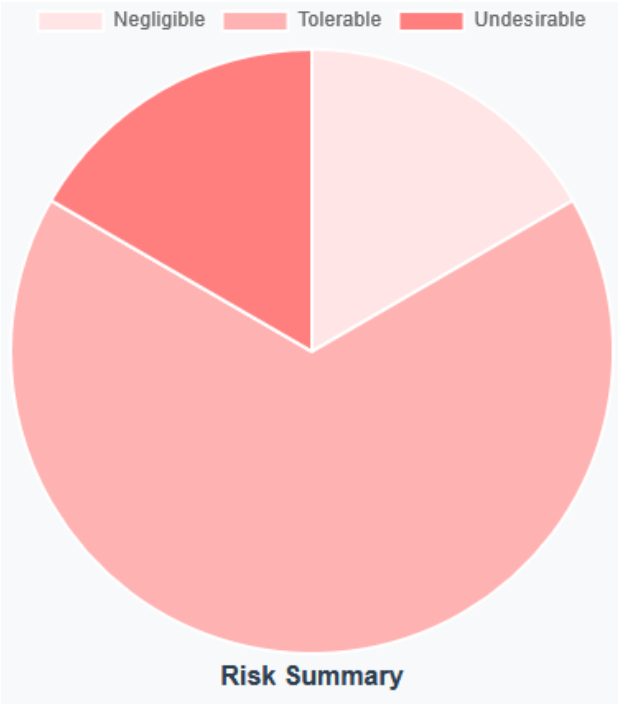

Figure 12: Risk Summary. (CAIRIS.)

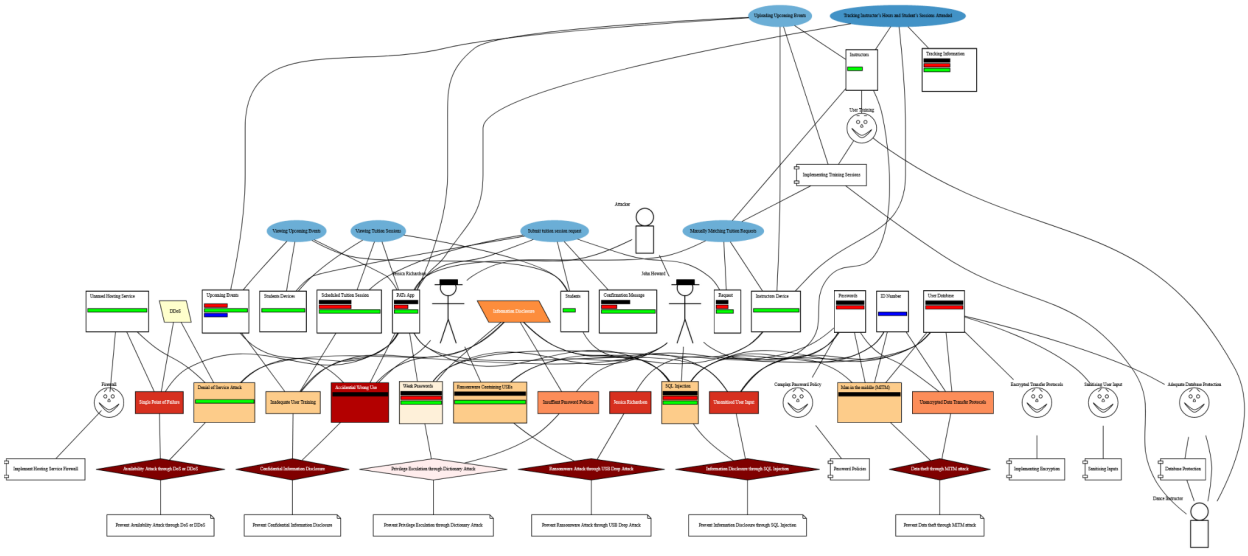

Figure 13: Risk Diagram. (CAIRIS.)

6.1 Goals

We will be discussing the overall goals in this chapter which are achieved by taking countermeasures and responses to our proposed attacks, obstacles that may arise and requirements of the PATs application.

6.2 Requirements

Name: Complex Password Policy
Type: Security
Asset: Passwords
Specification: A complex password policy.
Fit Criterion: More than 8 characters long and must include lower case, upper case, numbers and symbols.
Priority: 1
Rationale: Implementing a complex password policy that would stop any attackers from easily guessing or crack a user's password.
Originator: PATs

Name: Adequate Database Protection
Type: Security
Asset: User Database
Specification: Implementing a high level of security for PATs backend databases.
Fit Criterion: Password protection and access controls on the databases. Sanitising user input to block and wildcard characters.
Priority: 1
Rationale: Implementing passwords and access controls alongside sanitising user input will help us mitigate any potential SQL injection attacks.
Originator: PATs

Name: User Training
Type: Functional
Asset: Instructors
Specification: Organise resources on how to use the new PATs application.
Fit Criterion: Organise sessions for training along with tests to ensure users are learning.
Priority: 1
Rationale: Training the instructors to use PATs would reduce any inside attacks cause by human error.
Originator: PATs

Name: Encrypted Transfer Protocols
Type: Security
Asset: User Database
Specification: Data sent over the app is encrypted.

Fit Criterion: Login details and other data is sent over the PATs application using an encrypted protocol and not plaintext.
Priority: 1
Rationale: Having an encrypted protocol to transfer data will mitigate and prevent hackers from using a man in the middle attack to intercept any confidential information
Originator: PATs

Name: Firewall
Type: Security
Asset: Unnamed Hosting Service
Specification: A firewall is in place.
Fit Criterion: A physical firewall that blocks any suspicious traffic.
Priority: 1
Rationale: A firewall would help mitigate the risk of a DDoS attack.
Originator: Unamed Hostsing Service

Name: Sanitising User Input
Type: Security
Asset: User Database
Specification: To sanitise any and all user input.
Fit Criterion: Users are not able to pass wildcard characters through to the database.
Priority: 1
Rationale: Sanitising User input will mitigate SQL Injection.
Originator: PATs

6.3 Countermeasures

Countermeasure: Implement Hosting Service Firewall
Type: Hardware
Description: Implement a firewall with the hosting service provider to block any suspicious network traffic that may be malicious.
Cost: Medium
Requirement: Firewall

Countermeasure: Implementing Training Sessions
Type: Information
Description: To implement sessions where the dance instructors can attend and learn the basics on how to use the system.
Cost: Low
Requirement: User Training

Countermeasure: Database Protection
Type: Information

Description: Implementing security measures such as passwords and access controls.
Cost: Low
Requirement: Adequate Database Protection

Countermeasure: Password Policies
Type: Information
Description: Implement password policies that are 8 characters long, and contain upper case, lower case, numbers and symbols.
Cost: Low
Requirement: Complex Password Policy

Countermeasure: Implementing Encryption
Type: Information
Description: Implementing encryption when data is being transferred over the PATs system.
Cost: Low
Requirement: Encrypted Transfer Protocols

Countermeasure: Sanitising Inputs
Type: Software
Description: Sanitise user inputs.
Cost: Low
Requirement: Sanitising User Input

6.4 KAOS Associations

Head	**Type**	**Tail**	**Type**
Information Disclosure	Obstacle	Unsanitised User Input	Vulnerability
Information Disclosure	Obstacle	Inadequate User Training	Vulnerability
Information Disclosure	Obstacle	SQL Injection	Threat
Information Disclosure	Obstacle	Accidential Wrong Use	Threat
Information Disclosure	Obstacle	Attacker	Role
Information Disclosure	Obstacle	Exploit Confidential Information Disclosure	Misuse Case

Information Disclosure	Obstacle	User Training	Requirement
DDoS	Obstacle	Exploit Availability Attack through DoS or DDoS	Misuse Case
DDoS	Obstacle	Firewall	Requirement
DDoS	Obstacle	Attacker	Role
DDoS	Obstacle	Denial of Service Attack	Threat
DDoS	Obstacle	Single Point of Failure	Vulnerability
SQLi	Obstacle	Exploit Information Disclosure through SQL Injection	Misuse Case
SQLi	Obstacle	Sanitising User Input	Requirement
SQLi	Obstacle	Attacker	Role
PreventAccidential Wrong Use	Goal	Information Disclosure	Obstacle
Implementing Training Sessions	Countermeasure	Uploading Upcoming Events	Task
Implementing Training Sessions	Countermeasure	Manually Matching Tuition Requests	Task

Persona Factoids Sources

Source Reference	Source ID
What does a Dance Instructor do?	1
Dance Teacher Resumes	2
Performing Arts Teacher Requirements	3
DanceTeacherWeb	4
National Careers	5

References

Cwe.mitre.org. n.d. *CWE-201: Insertion of Sensitive Information Into Sent Data (4.6)*. [online] Available at: <https://cwe.mitre.org/data/definitions/201.html> [Accessed 6 April 2022].

Cwe.mitre.org. n.d. *CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (4.6)*. [online] Available at: <https://cwe.mitre.org/data/definitions/89.html> [Accessed 6 April 2022].

Cwe.mitre.org. n.d. *CWE-521: Weak Password Requirements (4.6)*. [online] Available at: <https://cwe.mitre.org/data/definitions/521.html> [Accessed 6 April 2022].

Cwe.mitre.org. n.d. *CWE-300: Channel Accessible by Non-Endpoint (4.6)*. [online] Available at: <https://cwe.mitre.org/data/definitions/300.html> [Accessed 7 April 2022].

Cwe.mitre.org. n.d. *CWE-400: Uncontrolled Resource Consumption (4.6)*. [online] Available at: <https://cwe.mitre.org/data/definitions/400.html> [Accessed 8 April 2022].

Danceteacherweb.com. n.d. *The Dance Teacher Success Formula: Follow the 3B Rule!*. [online] Available at: <https://www.danceteacherweb.com/en/articles/teacher_article/2022/1/31/The-Dance-Teacher-Success-Formula-Follow-the-3-B-Rule/> [Accessed 6 April 2022].

Hacker News, T., 2021. *Why Human Error is #1 Cyber Security Threat to Businesses in 2021*. [online] The Hacker News. Available at: <https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html> [Accessed 6 April 2022].

Lucidchart. n.d. *Intelligent Diagramming | Lucidchart*. [online] Available at: <https://www.lucidchart.com/pages/> [Accessed 6 April 2022].

Nationalcareers.service.gov.uk. n.d. Dance teacher | Explore careers | National Careers Service. [online] Available at: <https://nationalcareers.service.gov.uk/job-profiles/dance-teacher> [Accessed 10 April 2022].

Owasp.org. 2021. *A02 Cryptographic Failures - OWASP Top 10:2021*. [online] Available at: <https://owasp.org/Top10/A02_2021-Cryptographic_Failures/> [Accessed 6 April 2022].

Owasp.org. 2021. *A03 Injection - OWASP Top 10:2021*. [online] Available at: <https://owasp.org/Top10/A03_2021-Injection/> [Accessed 6 April 2022].

Owasp.org. 2021. *A07 Identification and Authentication Failures - OWASP Top 10:2021*. [online] Available at: <https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/> [Accessed 6 April 2022].

Trello.com. n.d. *Trello*. [online] Available at: <https://trello.com/> [Accessed 6 April 2022].

Teachingproject.org. n.d. *Performing Arts Teacher Requirements | Become a Performing Arts Teacher*. [online] Available at: <https://www.teachingproject.org/articles/performing-arts-teacher.html> [Accessed 6 April 2022].

Zippia.com. n.d. *What Does A Dance Instructor Do*. [online] Available at: <https://www.zippia.com/dance-instructor-jobs/what-does-a-dance-instructor-do/> [Accessed 6 April 2022].

Zippia.com. n.d. *How to Become A Dance Teacher in 2022: Step by Step Guide And Career Paths*. [online] Available at: <https://www.zippia.com/dance-teacher-jobs/#resumes> [Accessed 6 April 2022].