Asset Identification:

* Account password
* (Numeracy and literacy) Test results
* Personal details (email, D.O.B., phone number, etc.)

Threat Evaluation:

* Unauthorised access – This type of vulnerability leaves the attacker with full access to the user’s account. This can happen through obtaining a password, leaving an account logged in, etc.
* Malicious Insiders – This is where employees of the company use their own inside access/knowledge to harm the company, such as leaking information.
* Lost/Stolen Devices – If work is done on a portable device (laptop, tablet, etc.) these can easily be lost or stolen, putting all the work and data left on that device at risk.
* Injection Flaws
* Denial of Service
* Poor IT Management
* Sensitive Data Exposure

Vulnerability Appraisal:

* Unauthorised access – All users are encouraged to have strong passwords using combinations of numbers, letters, and special characters. For improved security, we give permissions so only certain users can access certain work.
* Malicious Insiders – User permissions are set so users can only access the work for their own team, so if any data is leaked, we’ll know which team it came from.
* Lost/Stolen Devices – Users are encouraged to keep backups of all work they do, so if a device is lost, they will still have access to their work. They are also encouraged to keep a strong password on all of their devices, so if it is stolen, their work will not be able to be accessed.

Risk Assessment:

* Unauthorised access – Medium risk. This would give them full access to the work of the team, but at least they don’t have access to all teams work. Also it’s possible the unauthorised user will not know where/what they’re looking for.
* Malicious Insiders – Strong risk. We would possibly not know if there was a malicious inside attack as the attacker would have access to the systems without suspicion. If an insider, for example sold data, it is possible we would never find out about this.
* Lost/Stolen Devices – Low risk. The lost/stolen device should have a password on, so no data should be accessible. Even if the device is unlocked, there will only be work from the 1 team on there, and possibly only part of the work.