**RISKS IDENTIFIED**

**Potential for unauthorised access to student data or course content**

If a student's Discord account was compromised and the account was registered with a valid oAuth token, the actor in control of that Discord account could access anything from MyLO that the student could.

More accurately, the actor would only be able to access (via Discord) anything that the Discord bot could access from MyLO on behalf of the student (this would be a well-defined and limited subset of information that the student could normally access through a logged in browser on MyLO). This is an important distinction to make, as this access would not enable the actor to do things like submit assignments on behalf of the student, or view arbitrary content from MyLO – these things still require a valid login via a browser.

Additionally, this is generally not the vector of attack of compromised Discord accounts. Unless the attack was with the purpose of gaining access to the student’s MyLO/UTAS information, a Discord attack generally consists of sending spam messages via DMs or as public posts on Discord with the purpose of monetary gain and gaining access to more Discord accounts. This is usually an automated approach that doesn’t consider the personal circumstances of the student having access to a bespoke Discord bot. In fact, since DMs are a target of this kind of attack, it is possible to implement detection of a compromised account, and part of the attack would likely DM the Discord Bot itself, which could be monitored for spam messages as a red flag.

If a student identifies themselves as having a compromised account, they will have available to them the ability to revoke any Discord OAuth tokens via MyLO itself. If a student is unable to do that in a timely manner, contacts a Unit Coordinator instead, or the Unit Coordinator detects that themselves (by witnessing a spam DM/post or otherwise), the Unit coordinator would have the ability to revoke the Discord OAuth tokens manually. Since a log of Discord Bot commands is kept, staff would be able to identify any malicious activity conducted by the account with regards to MyLO while the account was compromised—as unlikely as that may be.

Additionally, if a unit coordinator's Discord account was compromised, and the account had a valid oAuth token registered, the actor in control of that Discord account could access anything the unit coordinator could – including all course content and data of students in the unit.

As above, the actor would only be able access (via Discord) anything that the Discord bot could access from MyLO on behalf of the unit coordinator, not everything that the unit coordinator can see. Again, this would be a well-defined set of information.

For University user accounts, the Cyber Security team has certain tools available to monitor for and disable compromised user accounts, however there would be no means for us to proactively monitor for compromised Discord accounts. Phishing and hijacking of Discord accounts is a common occurrence and the only protection we would have against this sort of vulnerability is the short term nature of the oAuth token (24 hours) - this is more than enough time to extract significant amounts of data.

As mentioned above, it is an unlikely attack vector for a traditional Discord attack to focus on the specific capabilities of this bot, and as mentioned above, there would be at least one method for detecting a comprised accounts via the Discord Bot itself.

In addition, students are recommended to implement as many security features as possible, including 2FA. Discord implements email-based verification of logins from new or unrecognised IP addresses as well.

Importantly, during the Discord+MyLO OAuth flow, **it is possible to determine if the user has 2FA enabled on their Discord account** (via the mfa\_enabled field). It could be implemented such that a MyLO connection would only be allowed to be made if 2FA was enabled for the account. Since all the MyLO integration functionality is intended to supplement student learning and is not required for assessment, students who chose not to implement 2fa would not be disadvantaged by not being allowed to create a MyLO connection.

**Leakage of University IP**

If course content is transmitted to open Discord channels this could easily be logged by third parties. There is potential for it to be plagiarised and used elsewhere, or to be shared among potential future students.

This could potentially reduce the value of the content, and could also have ramifications for academic integrity, depending on how the content was used.

Content would be **linked**, rather than transmitted itself, revealing at most the title of the content page. If there were any features which were to extract mylo content and transmit it to Discord, there are the following mitigations:

* The Discord channels are not “open”, the Discord channels are by invitation given to students directly via MyLO and students must identify themselves with their utas username. If a member of the server appears to be not a student, they are removed from the server. This has never been an issue in the past
* Transmitted content would be in an “ephemeral” message, visible only to a requesting user, and not permanently stored in any chat logs. A rate-limit on commands that retrieve information from mylo could be implemented in the code to prevent “scraping” by a malicious party.

**Potential Code Vulnerabilities**

The code for the Discord bot is open source (we recognise that some data such as oAuth tokens is not published). This allows anyone to inspect the code and attempt to find vulnerabilities – which is a double edged sword. On one hand, communities of altruistic developers usually find and fix vulnerabilities quickly – on the other, particularly with a reasonably small user base, it would be quite easy for a malicious user to quietly find a previously undiscovered vulnerability and exploit it.  
  
If this happened and a third party was to gain access to the bot’s infrastructure or database, this could potentially give them access to any data the bot has access to.

Doesn’t need to be open sourced. This issue is also predicated on third-party access to the infrastructure being compromised. If that were to happen, they would already have the source code available to them via the infrastructure itself, and not need any open-sourced repository.

I reiterate that the bot stores minimal MyLO/personal data in its database and obtains its information via API calls that require an authenticated student account and a non-revoked oauth secret, so access to the infrastructure would not mean ongoing access to MyLO or student data.

**Support, Maintenance and Security Updates**

The application (Discord Bot) has been developed as a project within the school of ICT without funding. A support and maintenance agreement has not been provided for hosting of the application, Operating system management and application support. A maintenance schedule for testing of the API and integration with MyLO and/or Discord has not been documented. Roles and responsibilities for application support have not been defined.

In the event of Lindsay’s departure from the university there is a real risk that the code could end up orphaned and UTAS could lose the ability to perform security updates or adjust to API changes from systems such as MyLO that the bot interacts with.

While these are valid concerns for a full-scale roll-out of the system beyond more than a handful of units, these concerns are not relevant to the current scope of the project (proof of concept).

Currently the Discord bot serves to supplement the learning and teaching activities of staff in selected units within the School of ICT. The removal of the bot even mid-semester would not have a detrimental effect on either staff or students, and resumption of the project could be continued by colleagues in the School of ICT; Dr Ian Lewis and Lake Hopkins.

The server hosting the bot itself already requires some attention. A vulnerability scan on that server identified one critical and two severe vulnerabilities which could be exploited by a malicious actor. There is a genuine need to ensure that the server itself as well as the bot are regularly updated to patch vulnerabilities as they are identified.

I am open to working with security to ensure that the server itself has any security vulnerabilities addressed.

We acknowledge that Lindsay has somewhat addressed this in his proposal, however past experience shows that often circumstances change, motivations wane and the risk of losing support in future still exists.

**US Privacy Laws**

The bot application is hosted in the NeCTAR Research Cloud Service, but the database for the bot is stored in Google Firebase and hosted in the US. This means it is potentially subject to US privacy laws and any security implications from hosting on that platform would apply.

The current database location for the Firebase Database is hosted in a US data center. However, if the security team is able to determine if US privacy laws apply and would have a negative impact on this project, it is possible to migrate either a) a Firebase datacenter hosted in Sydney or b) switch to a different database solution hosted directly on NeCTAR Research Cloud.

**The Discord Platform Itself**

We have not performed a security assessment on the Discord platform itself. However even ignoring the risks of extracting potentially sensitive data from MyLO for use in other systems, Discord itself appears to have a reputation for being less than security focussed.

In the event of a data breach we could not guarantee that any and all necessary assistance would be provided.

Short of enterprise solutions by Microsoft or the existing D2L platform itself, the same could be said of most communication platforms where the weakest link in security is the user’s susceptibility to scams etc.

From the perspective of having used Discord for teaching in various forms over the last 6 years, it is clear from the outcomes we have observed and documented (via student surveys, direct feedback, and evaluates responses), that the benefits largely outweigh the risks of the Discord platform.