|  |
| --- |
| Compromised!  A lessons learnt story of a TEO |

A tertiary education organisation (TEO) experienced a ransomware attack just before its April Single Data Return (SDR) submission. The attack prevented the organisation from accessing the systems and data it needed for the SDR.

The attackers contacted the TEO and demanded payment via cryptocurrency in exchange for returning the data.

While the TEO correctly decided not to pay, rebuilding its data set was a major exercise, because it did not have effective data backup measures to quickly retrieve the “lost” data.

The rebuild took more than a week, and the TEO missed the SDR submission deadline, which meant a lot of stress and anxiety for staff. Additional cost was involved due to having to involve IT and cyber security partners.

While the TEO rebuilt the data and made the submission (after getting permission to submit late), it could have avoided the extra work with backed-up data, which requires a relatively small investment and effort. There are several reliable BaaS (Backup as a Service) providers that can do this. See the [Backup as a Service Overview resource](https://www.tec.govt.nz/assets/Forms-templates-and-guides/CSTS/Controls/R22_Backup-as-a-Service-Overview.docx).