Attachment 1 - Cyber Threat Detection

	Jan-17	Feb-17	Mar-17	Apr-17	May-17	Jun-17	Jul-17	Aug-17	Sep-17	Oct-17	Nov-17	Dec-17	Jan-18	
Email Viruses Detected	421	326	1,541	208	220	406	462	66	56	48	88	61	63	Represents emails blocked at the email gateway , usually for more granular levels of malicious activity such as scripts in emails or content not aligned to TMR's policy
Desktop Viruses Detected	210	118	200	98	202	123	86	65	222	243	319	221	187	Represents files blocked at the endpoint to be suspicious in nature, these may not be delivered via email.
Legitimate	976,031	1,144,416	1,354,881	1,145,860	1,365,428	1,432,812	762,351	995,601	998,272	1,406,674	1,325,850	1,100,556	1,107,524	Emails assessed as legitimate and processed through the permiter technology controls.
Spam/Phishing (Blocked)	1,412,566	3,077,096	2,539,070	2,354,671	1,612,264	1,561,206	1,384,524	1,051,425	1,062,761	1,468,513	1,399,606	888,000	996,266	Emails detected as malicious and unauthorised to enter TMR's network. These emails are blocked at TMR external perimeter based on general Threat intelligence
Total	2,388,597	4,221,512	3,893,951	3,500,531	2,977,692	2,994,018	2,146,875	2,047,026	2,061,033	2,875,187	2,725,456	1,988,556	2,103,790	
Phishing and Spam Emails Reported to phishin	1,562	1,535	2,205	1,623	1,905	1,775	1,574	1,486	1,419	1,307	1,802	1,169	1,382	Emails assessed by the user to be suspicious in nature. Some of these are emails that are not identified by other controls potentially because they are new viruses not previously identified by companies such as virus vendors. Effective user awareness programs support to the overall security posture with defences at several layers.
Security Breach	0	0	0	0	0	0	0	0	0	0	0	**1**	0	Internal Reference: SI2017-062 This breach resulted in unauthorised and malicious use by an entity who successfully obtained two TMR users credentials and used one mailbox for unauthorised activity. No evidence of information leakage was noted but the entity used the account to phish/spam other users using a TMR account. Remediation: Impacted internal users contacted and advised to change passwords. The malicious form was blocked. Emails from the compromised user were blocked internally. AusCert advised Malicious Form is now providing a 404 Error