GOVERNMENT INFORMATION AND COMMUNICATIONS TECHNOLOGY SYSTEMS — CYBERSECURITY

231. Mr Y. MUBARAKAI to the Minister for Innovation and ICT:

I refer to the ongoing ransomware attacks that have struck computer systems across the world in the past 24 hours. Have any information and communications technology systems of the Western Australian government been impacted by the attacks; and what is this government doing to address cybersecurity issues?

Mr D.J. KELLY replied:

I thank the member for Jandakot for his question. Most members would be aware that we are currently, around the world, dealing with another ransomware attack—the Petya attack. I am advised that, to date, no Western Australian government agencies have been penetrated by this ransomware. There is evidence in at least one agency that that bit of malware, or ransomware, has been detected, but the security protocols in place have prevented that bit of ransomware from entering the system. We are fortunate that the current cyberattack is based upon the same vulnerability that the earlier WannaCry ransomware attack used a few months ago, and our systems successfully repelled that attack. I might say that we were very fortunate that on that occasion the ransomware attack occurred on a Friday night, so our systems were down. I am advised that we would have been much more vulnerable had that ransomware attacked our systems during the day on an ordinary business day.

Since becoming minister, I have looked at our preparedness for these types of attacks and digital security in general, and I am disturbed that the Auditor General has released not one, but eight annual reports under the previous government that have all indicated that, as a public sector entity, we are not well prepared in the areas of digital security. In information protection, one of the criteria that the Auditor General checks, only 40 per cent of our agencies meet the required standard. Over the eight years that the Auditor General has done those reports, there has been virtually no improvement in that area. Information that the government holds is not protected to the satisfaction of the Auditor General, and for eight years the previous government did nothing. The Auditor General also released a specific malware report in December 2016. That report painted a very poor picture of the previous government's performance—a lack of training, a lack of coordination and, importantly, a lack of a cross-government approach to digital security.

One of the first issues I raised with the Government Chief Information Officer was how we were to address, in particular, the most recent Auditor General's report. As it would happen, we released today an updated digital security policy that improves significantly upon what was done under the previous government. It begins the implementation of the recommendations made by the Auditor General in this area. Further, the Premier has written to each minister urging them to ensure that the agencies they are responsible for take this issue seriously. The one thing that the previous government did was to create the Office of the Government Chief Information Officer, but—surprise, surprise—it funded it for only three years, as though the question of cybersecurity was going to be dealt with within three years. Members opposite may be surprised to realise that the issue of digital security is not getting any easier. It is getting more complicated, and as a government we have an obligation to deal with it. Under this government, in its first 100 days, we are getting on with that job.