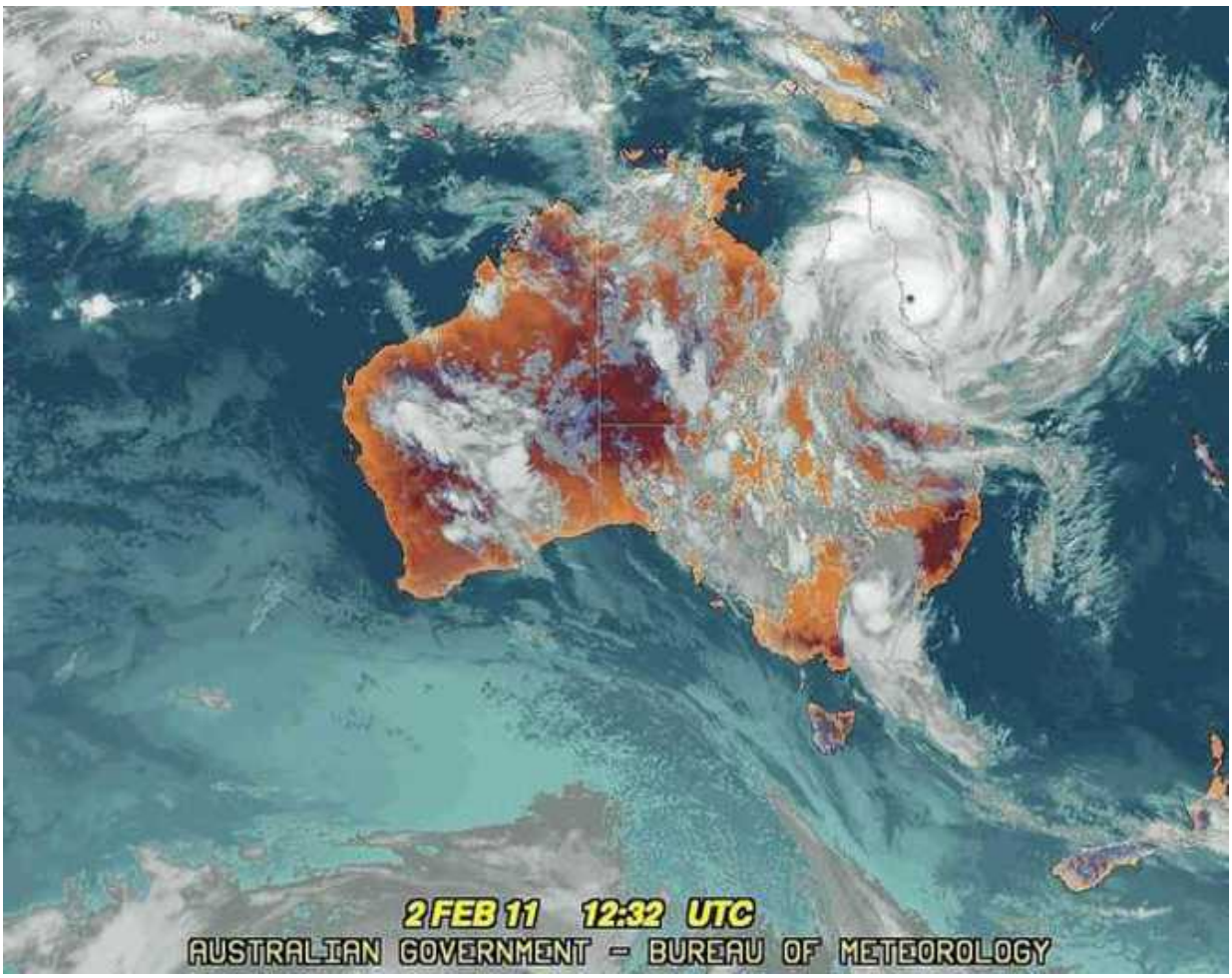
Cyber breach at the Bureau of Meteorology—the who, what and how, of the hack

December 2 2015, by David Glance



Trouble at the BOM. Credit: flickr Tatters, CC BY-SA

The ABC is reporting that there has been a "massive" breach of computer systems at the Australian Bureau of Meteorology (BOM). The hack of computer systems at the BOM is believed to have originated from China and the ABC has quoted an expert as saying: "It could take years and cost hundreds of millions of dollars to fix".

The BOM has not denied the breach but has stated that:

The Bureau's systems are fully operational and the Bureau continues to provide reliable, ongoing access to high quality weather, climate, water and oceans information to its stakeholders.

Unfortunately, little is known about what computers were hacked, nor what was actually done by the hackers. This in turn makes it hard to say definitively what will need to be done to clean up after the hack and more importantly, stop it happening again.

What could realistically have been hacked?

The Bureau of Meteorology, like any government agency, will have a network of desktop computers and servers that are used for their day-to-day business. These systems are the easiest targets because access can be obtained by "phishing" for user names and passwords directly from employees. This hacking approach was used by Chinese hackers in their infiltration of the New York Times in 2013.

It is possible, but less likely, that the hackers were also able to access the BOM's latest supercomputer, a A$77 million Cray computer that is handling the agency's ever growing processing power needs. The reason that supercomputers are safer is that access to the computer is rarely direct and interactive. Programs are usually run on the computer by way of another computer that schedules them. This makes direct access harder.

The storage sites attached to the supercomputer that contains the massive amounts of data collected by the BOM could have been targeted but this data alone would not necessarily have been very interesting and much harder to move out of these locations without detection.

Finally, the BOM is connected through to other government agencies, including those involved in defence and security and so hackers could have got access to systems or networks that would allow them access beyond the Bureau's systems.

What would the hackers been after?

If the hackers were state-sponsored Chinese hackers such as the People's Liberation Army Unit 61398, then the target of the hack would have been wide-ranging but possibly focused on information related to Australian defence and security services and capabilities. The Bureau of Meteorology provides environmental monitoring services to these agencies in addition to its role of providing weather information to the public.

The hackers could also have been after other intellectual property including software source code for the systems that the Bureau uses to model weather and make predictions. This would potentially be something of the greatest value to the Chinese because they could use this information to greatly improve their own capabilities.

If the hackers had been simply been cyber criminals, they would have been more interested in getting information about individuals or anything that could be potentially leveraged into a financial gain at some later stage.

What would the damage have been?

The main damage relating to a cyber attack is not usually as a result of any specific damage done by the hackers during their forays through the systems. The damage is actually the cost of work that is needed to investigate and record what has happened, to then make sure that the hackers have not left behind any software that is continuing to spy or providing hackers with renewed access, and finally to plug whatever holes the hackers used to gain access in the first place.

For most systems, this means either re-installing all of the software from scratch or restoring from a backup that is known to be safe. For the supercomputer, this is slightly harder because the system is in continuous use and can't be taken offline for extended periods of time.

The costs of doing all of this come from the cost of people's time, especially consultants. Whether this amounts to "hundreds of millions of dollars" as reported by the ABC is doubtful.

If the hack was done by the Chinese PLA, then it is unlikely that whatever security mechanisms are put in place will be completely effective in stopping a recurrence of this attack. Even less likely to have an effect is the recent agreement between US and Chinese leaders to not engage in corporate espionage of each other's countries.

As reported by The Register, President Obama and President Xi Jinping managed to announce the deal without betraying the scepticism they both must have harboured that it would actually stop any hacking.

Source: The Conversation