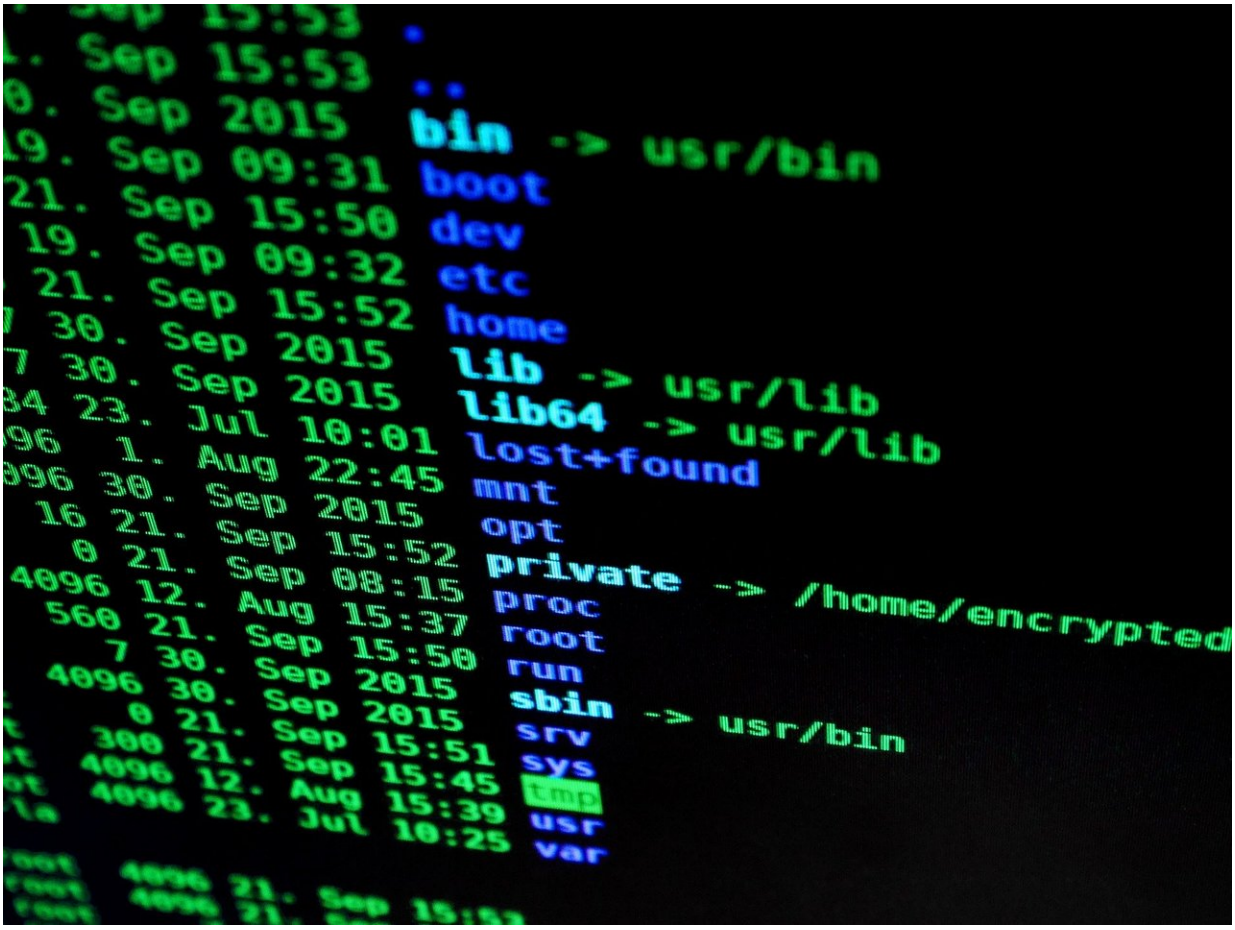
Should cyber officials be required to tell victims of cyber crimes they've been hacked?

January 10 2019, by Greg Austin



Credit: CC0 Public Domain

In Germany this week, the legal limbo that defines cyberspace around

the world was on full display.

The country's Federal Office for IT Safety (BSI for its German initials) had been tracking a cyber attack targeting some of the country's parliamentarians since early December. It ultimately led to the public release of mobile phone numbers, credit card information and ID card details of hundreds of members of parliament, and other public figures.

Only some MPs were informed by BSI about the attacks, while others learned about them only after the details were published in the media. MPs were outraged that BSI had failed to notify them that their personal data was being targeted, despite knowing about elements of the attack for up to four weeks.

A deeper concern, raised by some MPs, was that over the same period, BSI (which is not a law enforcement agency) did not inform the German police that a political crime of this seriousness had possibly been committed. Once engaged, the police quickly found a suspect who reportedly confessed.

Hacking, whether or not data is publicly compromised, is a crime in most countries. The crime is constituted simply by the unlawful accessing of data or machines. But few countries have laws that require their cyber agencies that monitor hacking to report the criminal acts – either to third party victims or to the police.

This legal vacuum needs to be addressed urgently.

Is hacking a 'serious crime'?

The challenge for cyber agencies or private sector firms which detect a hack is that these events are very common. Millions take place every day, and complex forensic information needs to be assembled in order to

judge which incidents are serious enough to require notification. This sets up a defacto, but ill-defined, distinction between "petty crime" (most hacks) and "serious crime".

What this means in reality can be illustrated by the practice in the Australian state of New South Wales. In NSW, there is an obligation under the Crimes Act to report serious crimes. These are defined as those attracting legal penalties of five years or more of imprisonment. But when it comes to cyber hacking, it's often not immediately clear whether the extent of a hack would trigger such a penalty threshold.

This uncertainty was at play in the German hack, with BSI justifying its failure to notify with the claim it was still trying to analyse it, and did not know the full scale of it.

Even after arresting the suspect and knowing the scale of the attack, the head of cyber security at the Federal Police Office (BKA) said it was still unclear whether the hack was a serious crime inspired by political motives. The suspicion that it may have been politically motivated arises from the fact that the only political party whose MPs were not targeted was the extreme right party, AfD.

What 'mandatory reporting' means in Australia

In 2018, after a long public debate, Australia introduced the Notifiable Data Breaches (NDB) scheme as an amendment to the Privacy Act. The NDB requires companies to notify the Office of the Information Commissioner (not the police), as well as any victims, if personal data they hold is compromised in a way that constitutes a serious breach of privacy.

This civil code provision is very weak due, in part, to the fact that it allows the firm or agency involved to self-assess the seriousness of the

breach over a 30-day period before the obligation to notify kicks in.

It is also weak because there is a blanket exemption for law enforcement activities, and for the secrecy needs of the government. Australian cyber agencies, such as the Australian Signals Directorate and the Australian Centre for Cyber Security, appear to have zero obligation to tell either the police or victims that there has been been a hack or a data breach.

That means, if Australian cyber agencies learned that a foreign government had hacked an Australian citizen, the victim may never be told. Or if family photos of an unclothed child were hacked from a family computer by a paedophile, the victim's family might never know.

A right to know?

In many countries, cyber agencies do notify large corporations of certain hack attacks, regardless of the kind or scale. There are several motivations for this mostly voluntary practice. One is to help corporations realise the seriousness of state-sponsored espionage against them. Another is to help the cyber agency itself coordinate an investigation of the hack, and figure out what might have been lost.

That is not the same as the police investigating the crime.

In most countries, only police agencies are authorised to investigate crimes for the purposes of court prosecution. Few jurisdictions, if any, have formally clarified the ways in which police and courts may rely on information on cyber hacks collected by cyber agencies or security companies.

Australia is yet to have a serious debate about cyber crime reporting, and its forensic complexities: who is responsible for what, and where the priorities should lie. It's at least a decade overdue.

While recognising that some distinction will need to be made between petty and serious cyber crimes, such a debate should recognise the right of citizens to be informed by our cyber agencies when they have been assaulted in cyber space and, if possible, by whom.