It's time to make cyber security compulsory

May 28 2021, by Richard Oloruntoba and Nik Thompson

Credit: CC0 Public Domain

On May 7, a pipeline system carrying almost half the fuel used on the east coast of the United States was crippled by a major cyber attack. The five-day shutdown of the Colonial Pipeline resulted in widespread fuel shortages and panic-buying as Virginia, North Carolina and Florida declared a state of emergency.

The attack highlights how vulnerable critical infrastructure such as fuel pipelines are in an era of growing cyber security threats. In Australia, we believe the time has come to make it compulsory for critical infrastructure companies to implement serious cyber security measures.

Collateral damage

The risk of cyber attacks on critical infrastructure is not new. In the wake of the events of September 11, 2001, research demonstrated the need to address global security risks as we analyzed issues of vulnerability and critical infrastructure protection. We also proposed systems to ensure security in critical supply chain infrastructure such as seaports and practices including container shipping management.

The rise of "ransomware" attacks, in which attackers seize important data from an organization's systems and demand a ransom for its return, has heightened the risk. These attacks may have unintended consequences.

Evidence suggests the Colonial shutdown was the result of such an attack, targeting its data. It appears the company shut down the pipeline network and some other operations to prevent the malicious software from spreading. This resulted in a cascade of unintended society-wide effects and collateral damage.

Indeed, the attackers may have been surprised by the extent of the damage they caused, and now appear to have shut down their own operations.

We have seen how critical supply chain infrastructure can be severely disrupted as collateral damage. We must consider how severe the fallout might be from a direct attack.

The events in the US also raise another important question: how vulnerable is our critical supply chain infrastructure in Australia?

Critical infrastructure is an attractive target

Australian society is dependent on many international and domestic supply chains. These are underpinned by critical supply chain infrastructure that is often managed by advanced and interlinked information and communication systems. This makes them attractive targets for cyber attackers.

Cyber risk frameworks are often derived from traditional risk management approaches, addressing issues of a potential cyber attack as routine conventional risk. These risk management approaches weigh up the costs of preventing a cyber attack against the costs and probability of a breach.

In some industries, this assessment will factor in the cost of a lost customer base who may never return. However, providers of critical services such as transportation, medical care, electricity, water, and food see little risk of losing customers.

After the Colonial incident, customers trooped back to petrol stations as soon as they could and went on buying fuel. Thus, critical industries may perceive less cost from a breach than companies in other industries because their customers will return.

Time for compliance

Australia's national efforts in cyber security are coordinated by the Australian Cyber Security Center (ACSC) under the auspices of the Australian Signals Directorate. The ACSC works with public and private

sector organizations to share information about threats and guidance on best practices for security.

ACSC documents such as the Essential Eight provide guidance for organizations on baseline security measures. These are supplemented by more comprehensive resources including the Australian Government Information Security Manual.

However, our research has shown the best practices are not universally followed, even by the Australian government's own websites.

Lack of knowledge is not the problem. Security best practices are generally well understood and documented by the ACSC. The ACSC also provides specific guidance for critical sectors and industries, such as a security framework developed for the energy sector.

The challenge here is that these are guidelines only. Companies can choose whether to follow them or not.

What Australia needs is a cyber security compliance program. This would mean making it compulsory for companies that manage critical infrastructure such as ports or pipelines to follow some kind of rules.

A first step might be to demand these companies comply with the existing guidelines, and require certification of a baseline of cyber security.

Lessons from the United States

The U.S. government responded to the Colonial cyber attack with an executive order to improve cyber security and federal government networks. The order proposes a raft of measures to modernize standards and improve information sharing and reporting requirements. These are

valuable measures, many of which are already within the scope of the existing duties of Australia's ACSC.

Another measure in the US order is the establishment of an independent Cyber Safety Review Board. Australia could likewise establish a partnership between government and industry to oversee cyber security. A similar body already regulates aviation: the Civil Aviation Safety Authority.

Such an organization would provide robust analysis and reporting of cyber incidents. It would also share information with information technology managers, software and hardware developers, public administrators, crisis managers, and others.

Cyber security threats create high levels of uncertainty for the public and private sector. Attacks that disrupt critical supply chain infrastructure have widespread impacts on society and trade.

A cyber security compliance program may be financially costly, but would be a worthwhile investment given the societal impact of a successful cyber attack.

Provided by The Conversation