We could lose $30 billion in weeks from cyberwar. But the real loss is the erosion of public trust

July 16 2020, by Richard Buckland

Credit: AI-generated image (disclaimer)

The Australian Cyber Security Growth Network (AustCyber) on Monday released a report modeling the potential impact of cyberattacks and sustained digital outages on Australia.

The Digital Trust Report's modeling suggests four weeks of partial "digital disruption" could displace up to 163,000 jobs and damage the economy to the tune of A$30 billion.

According to AustCyber's report, that's about 1.5% of our gross domestic product, or three-quarters of our annual defense budget.

The report also emphasizes the devastating impacts digital disruption can have on public trust.

The monetary costs of cyber disruption

The report includes economic modeling by consultants Synergy Group which looked at the general public's digital activity, as well as revenue from some indicative sectors including online retail, digital health, space, solar, and cybersecurity.

The modeling estimates a one-week disruption to digital activity would cost the economy A$1.2 billion directly, and A$5 billion including indirect impact. A four-week disruption could cost A$7.3 billion directly, and A$30 billion in total.

In this context, disruption means a significant drop in digital activity including any resulting loss of public confidence. This could be due to cyberattacks, a natural disaster or other large accident.

The report's modeling is based on current levels of digital activity. As Australia continues to move online, risks and impacts will grow. For example, online sales currently account for 9.6% of Australian retail spending, but on current trends this is expected to grow to 25% within a decade.

The report also notes increasing digital dependency across Australia's

sectors. Some have traveled so far down the digital path, they wouldn't be able to "step back" if faced with serious digital interruption.

This is especially true for the financial sector. Referring to the Reserve Bank of Australia, the report states digital transformation "is occurring to a point that commerce without digital technologies has become nearly impossible".

An attack on trust

That said, it could be argued the risks of cyber failure are much more insidious and far-reaching than impact on revenue alone.

The recent wave of cyberattacks announced by the prime minister, like most cyberattacks, worked by abusing trust. They relied heavily on memory corruption attacks (where programmers trust users) and spear phishing attacks (where users trust other people).

By exploiting trust, attackers also *undermine* trust. The Australian Financial Review reported a survey of 1,600 digital service users and 20 government leaders across Australia and New Zealand. Two-thirds said a poor customer experience damaged their trust and confidence in government.

Trust is needed for societies to work. As social psychologist Robert Cialdini observes, the universal human drive to reciprocate allows us to do good now and trust that we will be repaid in the future.

Moreover, a lack of trust is what leads to banks runs (when large numbers of customers withdraw deposits due to solvency fears), hoarding toilet paper and conspiracy theories.

Foreign influence potential

Modern cyberwar involves information warfare and influence operations that have an effect beyond immediate financial impact. While not known, it's possible the recent cyberattacks on Australia also had a non-financial purpose.

If Australians start believing the country's digital infrastructure can't be trusted, faith in wider institutions may be damaged, too. We could see the emergence of the "fake news" narrative against media and politicians. Or we could see electronic election outcomes come into question.

These are just some examples of how an attack on digital infrastructure can be an attack on society itself. And all this may be in the interests of a foreign nation state wanting to unravel Australian society from within.

The need to prepare and learn from the past

In 2001, US leaders and policy makers ran a simulation exercise called Dark Winter, modeling what might happen if the nation were to suffer a pandemic as an act of bio-terror. The timing was remarkable, coming shortly before 9/11 and the notorious anthrax attacks.

But despite the prophetic modeling, the US neglected to properly prepare for the COVID-19 crisis. In fact, in 2018 the Centre for Disease Control and Prevention's Office of Preparedness and Response canceled (with dreadful timing) a project that could have enabled the US to generate 1.5 million N95 masks per day.

Australia should learn from the US's failures. AustCyber's report says Australia's "cyberattacks are increasing in number and severity over

time". Unfortunately, there's no easy way to flatten this curve, so what matters is how we prepare and respond to future attacks.

We must continue to build our national cyber capability, increase cyber awareness and training at all levels of society, ensure we have sovereign capability (rather than depending on others for critical infrastructure) and have contingency plans for when things do go wrong.

Perhaps even if voting becomes fully electronic one day, just in case of lost WiFi (or a blackout), it would be prudent to keep some good old fashioned pencils and paper ballots in the cupboard.

Provided by The Conversation

Citation: We could lose $30 billion in weeks from cyberwar. But the real loss is the erosion of public trust (2020, July 16) retrieved 19 April 2024 from https://techxplore.com/news/2020-07-billion-weeks-cyberwar-real-loss.html