Protecting our digital heritage in the age of cyber threats

December 6 2018, by Stanley Shanapinda

Credit: CC0 Public Domain

One of the key functions of the government is to collect and archive national records. This includes everything from property records and registers of births, deaths and taxes, to Parliamentary proceedings, and

even the ABC's digital library of Australian news and entertainment.

A new report released today from the Australian Strategic Policy Institute (ASPI) considers the important role these records play as the collective digital identity of our nation.

The report's author, Anne Lyons, explains how an attack on these records could disrupt the day-to-day functioning of society, and why we need to do more to protect them.

Why are these records important?

Given that we live in the digital era, our digital identity records have been transformed into electronic data and are stored virtually in cloud servers. These servers act as the memory centre of the nation, preserving Australia's unaltered history.

We can trust these records are accurate, confidential and not interfered with. All this digital information may be referred to as "digital identity assets".

These assets are worth protecting, because they are important for the functioning of government, and are a legacy for future generations. Collectively, they embody who and what Australia is as a nation, its journey, and its time and place in history.

What could happen if they were hacked?

The impact of any theft, manipulation, destruction or deletion of digital identity assets could be catastrophic.

The courts would not be able to function without the relevant digital

records. Manipulated property title deeds could create legal challenges. Passports and visas may not be able to be verified and issued. And historic records could be tampered with or forged.

In the worst-case scenario, such an attack could interfere with the proper functioning of government, and shatter public trust and confidence in government institutions.

Lyons paints a picture of what it would look like if property records were hacked: "You wake up in 2022 to discover that the Australian financial system's in crisis. Digital land titles have been altered, and it's impossible for people and companies to prove ownership of their assets. The stock market moves into freefall as confidence in the financial sector evaporates when the essential underpinning of Australia's multitrillion-dollar housing market – ownership – is thrown into question. There's a rush to try to prove ownership, but nowhere to turn. Banks cease all property lending and business lending that has property as collateral. The real estate market, insurance market and ancillary industries come to a halt. The economy begins to lurch."

What are we doing to prevent attacks?

Three pieces of legislation have been passed since 2017 to protect the nation against crimes committed over the internet targeting telecommunications, water, electricity and gas equipment. These are the Security of Critical Infrastructure Act, the National Security Legislation Amendment (Espionage and Foreign Interference) Act and the Telecommunications and Other Legislation Amendment Act.

But cyber attacks are not only targeted at our nation's critical infrastructure. Servers that host digital identity assets are also at risk. Nation states and individual hackers could gain access to databases using our email communications to gain access.

Despite this risk, our lawmakers have failed to exert the same vigour in crafting laws that protect digital identity assets as they have exerted in efforts to decrypt the WhatsApp messages of criminal targets.

There is no clear and specific cybersecurity governance framework in the law books geared towards detecting and preventing attacks against these assets.

How to protect our digital heritage

1. Assess cyber vulnerabilities alongside social ones

Governments need to improve their holistic situational awareness to counter threats. That means assessing cyber vulnerabilities in conjunction with societal ones.

Online disinformation campaigns and malicious cyber activities are all referred to as hybrid threats. Hybrid threats – which could make use of digital identity assets – are challenging to detect and to make sense of due to their dynamic nature. Understanding the complex nature of a hybrid threat is referred to as cyber situational awareness.

Outside of the cyber environment, situational awareness may refer to an awareness of cultural, ethnic and religious tensions in society that could be vulnerable to online exploitation. For example, in the 1980s the Soviet government used the HIV epidemic to sow social division in the United States. Under operation INFEKTION, Russia spread stories that the American government created the virus and spread it among its population.

In cases like this, it's feasible that digital health records could be hacked and altered to serve as fake evidence. In this way, societal vulnerabilities can become one part of a mixed bag of threats.

Our ability to effectively resist and recover from malicious hybrid activities depends on our capacity to detect, analyse and understand the nature of the threat, in near real time. Metadata can be used for this purpose to show who accessed a server and from what location.

To improve cyber situational awareness, access logs should be retained and the computer emergency response team must collect metadata from government departments themselves, and analyse the data in near real time. This is a growing trend in the cybersecurity sector and public bodies must gear up.

2. Store copies of historical records offline

We also need to simulate how digital identity assets can be used against us and be prepared to counter the propaganda. Schools and universities can store multiple offline historic records, which can be used to verify accuracy when conflicting stories arise. Using National Archives as a central repository for digital identity assets is a single point of failure. Redundancy work-arounds must be created.

3. Engage the private sector

This is a job too big and too important to be left to government alone. Historical societies and charitable organisations may need to store hard and soft copies of the same records all over the country. Relevant laws must mandate, cybersecurity situational awareness for telecommunications companies, ISPs, computer emergency response teams, law enforcement and security agencies, but in clear and responsible fashion.

We must take a proactive approach that mandates the roll out of appropriate advance counter measures. A legal mandate that is largely

based on past incidents may not be an effective strategy to prevent dynamic hybrid threats. This is how we will tell hackers to back off our national heritage.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Protecting our digital heritage in the age of cyber threats (2018, December 6) retrieved 25 April 2024 from https://phys.org/news/2018-12-digital-heritage-age-cyber-threats.html