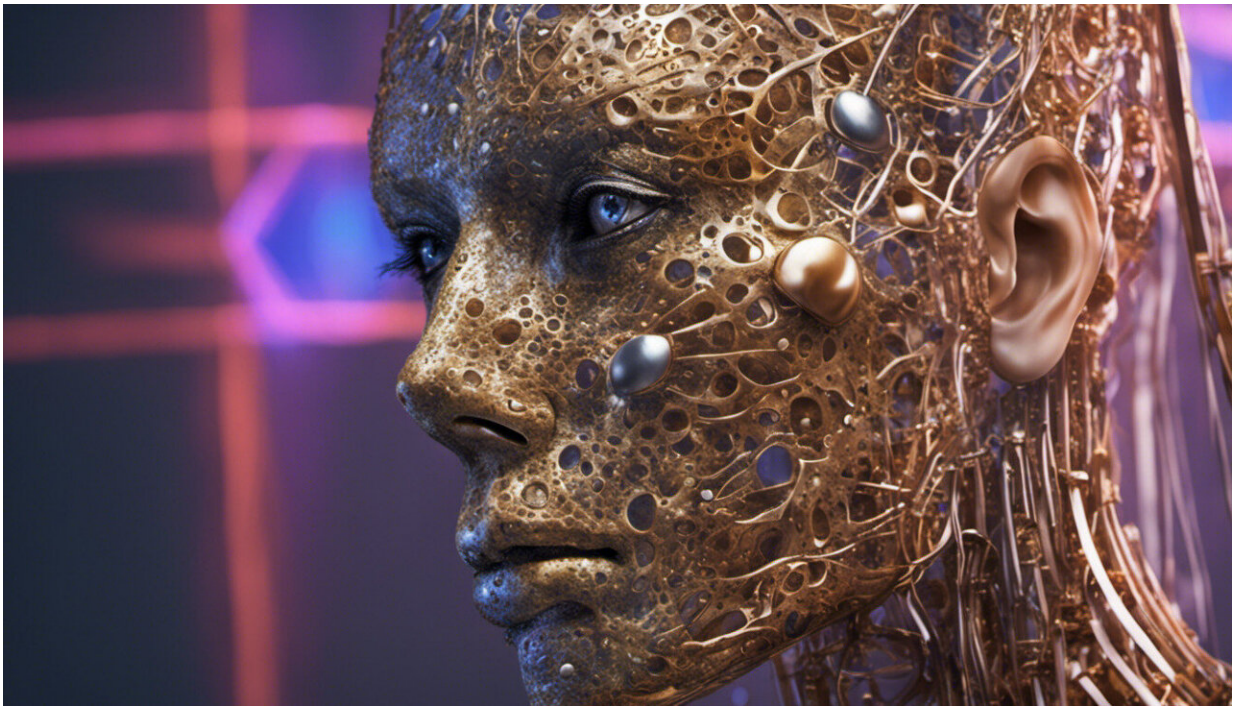
The first 72 hours are critical for hacking victims

March 12 2015, by David Lacey



Credit: AI-generated image (disclaimer)

US President Barack Obama is seeking US$14 billion to tackle it. The UK wants to build a start-up industry around it. And Australia is in the middle of what could be a year-long review into getting better at it. The issue is cyber security, and at risk is the entire digital economy and consumer confidence in it. In this Cyber insecurity series we investigate

the size and nature of the cyber crime threat, the industry growing with it, and the solutions emerging to get in front of it.

More than at any other point in time, your personal information is worth a lot of money to a lot of people. There's a whole industry created around it that's typically referred to as direct marketing. There's a similar industry also booming in the trade; that's called hacking or data breaching.

Let me explain a slight nuance between the two. The direct marketing industry will typically know more about you than you do. In fact, it knows so much about you, it's willing to sell your details to others so they can better predict your purchasing behaviour before you even get that itch to buy.

It's not confined to those wanting to make a dollar. Government agencies are also on the bandwagon. Agencies want to know where to deliver their services more effectively and where wastage can be cut. The central player in all of this is you. It's just that you are a passive participant. Our data and the identity footprints our personal information creates is what drives these markets.

So what about the criminals? This other market called hacking? Well, they love us too, more specifically our personal information. They too like to make money from selling personal information. But increasingly, those who access personal information illicitly are doing so for ideological reasons.

Hacking in vogue

CNet and many other technology commentators described 2014 as "the year of the hack". Leading industry sources such as the United States Identity Theft Resource Center, Gemalto, and Risk Based Security

report that between 700 million and 1.1 billion records containing personal information were compromised last year.

A fundamental issue with the volume relates to the grapple with ideology. Hacktivism is not a new concept - Denning wrote about it in 2001 when commenting on the Kosovo crisis of 1998/99.

But hackers don't need Kosovo. All they need is a lack of appropriate controls and a platform to tell the world what they've found to further their political platform.

In October last year the Commonwealth government announced the creation of iDcare. I've a personal and professional interest in such a body, as I'm on its board and see how its operations impact the lives of many each day. It's a joint public and private sector national initiative that operates a toll-free hotline for individuals concerned about their personal information.

In a little over 12 weeks iDcare provided direct assistance to more than 4,000 clients. A fair chunk of these clients were victims of hacking events. What have we learnt in this short amount of time? Hacking of individuals can have dramatic impacts on how they attribute blame, the likelihood of repeat business, and the overall confidence they have in participating online.

Hacking for the most part has little to do with what you or I have done, but what organisations have not done to protect what's ours in their custody. A common way hackers make their point today is by publicly releasing the spoils of their victory - the personal information and communications they have acquired. Some prefer the big bang approach and release their spoils en masse.

Others prefer the more painful drip-fed approach. The recent Aussie

Travel Cover hacker went the extra mile to share with the world how they did it – why not educate while inspiring others?

The protectors

So where does all this leave those of us who represent the information, and those organisations that are the compromised custodians? Like a classical complex system, hacking events, their prevention and response is not a unitary problem for one group or organisation. It's a systems problem, and a complex one at that.

While I'm a proponent of some form of mandatory data breach notification framework, this system is fraught with danger and requires a much deeper consideration of the impacts, their antecedents, associated control failures, and best effort responses.

The first three months of iDcare tells us that the 72 hours following the initial compromise of personal information really counts. In that 72 hours an individual can do things that makes their personal information more resilient to further misuse – you can make your personal information complex and unattractive for the criminal.

Putting credit bans or freezes on your credit file and alerting the right government and business channels that your personal information is at risk are important considerations. These measures can make a misuse more difficult for the hacker and the criminals that purchase such information.

iDcare's data tells us that if nothing is done in the first 72 hours, the chances of a further misuse increases four and a half fold. What does this mean for hacking? It's simple, organisations must prioritise engagement throughout the identity eco-system immediately after a hacking event, least of which is to communicate with impacted

individuals, so that they can build resilience to identity theft. The only way to truly understand and effectively respond is to take a systems approach, not solely an organisational one.

A systems approach means organisations examining both the causal nature of hacking, as well the implications of their response across the human, technological and process domains (to name a few).

A response that promotes greater resilience for those individuals that have had their details compromised, has different implications to one that preferences an "ignore it, and it will go away" solution.

There's so much that can go wrong in a response to a hacking event. The Sony Pictures example of 2014-2015 is a great case in point: to release a movie or not; to pay a ransom; to inform current and former employees; to provide assistance to these individuals in order to build their resilience to any further misuse of their identity information; to assist the next of kin of staff who may have also had their details put at risk; to work with law enforcement and national security agencies; to respond to calls from many stakeholders, including even the president of the United States; to respond in a specific way.

How could hacking events be anything but a complex system problem? No wonder the first 72 hours counts. For those organisations that collect and store personal information, better start planning on what your first 72 hours will look like.

Source: The Conversation