GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Speech to the Institute of Directors Breakfast by Ian Fletcher, Director, Government Communications Security Bureau

Tuesday 24 February 2015

Some months ago, at a forum sponsored by the Privacy Commissioner, I started to set out some of the issues which we face as a society migrating onto the internet.

It was necessarily a conceptual presentation, but I made the broad point that privacy and security are complementary values, of growing importance in our society.

We need to have, I argued, a serious debate about how to take those values forward in the age of the internet. I also argued that trust and transparency were not actually complementary values, but opposites.

And I set out the case for a liberal democracy to have the ability to operate covertly on the internet.

It was a case that reflected the fact that the internet is already contested by and between states and others, and it is right to expect government to protect their nation's interests.

Today I want to take those themes further, and look at some of the strategic questions which I believe confront organisations – public or private – dealing on the internet or looking to deliver services over the internet.

I'm assuming that organisations have the basics right.

That means that I'm assuming that any organisation thinking seriously about these issues will have good commercial-grade IT security, clear and compliant privacy policies, and be thinking actively about its IT security, and the way it deals with its customers, consumers and their information.

That said, it's worth remembering the basics: patching systems and applications, ensuring that people don't bring their own software to work (it's called white-listing – only allowing approved software to run), limiting administrator privileges, and strong control of passwords.

GCSB's Australian counterpart, the Australian Signals Directorate, has especially good advice on these and other measures on its website.

This is all basic hygiene, but the evidence is that not everyone does that, and the evidence is also that basic hygiene goes a long way towards providing for good IT security.

It's also worth remembering that security is more than just a matter of IT. It's worth thinking about your organisation's approach to security through the lens of people, places and systems.

On people, risks to your organisation from people can come from the inside (people who you have trusted who take data, or change it), which can be just as damaging as an effective, external cyber-attack or intrusion. And sometimes people facilitate cyber attacks too.

And secure places, whether they are customer facing premises or your data centre, also seem obvious, but can be a point of vulnerability.

How many of us actually know where our IT services provider has their physical data centre and how secure is that data centre against both natural and man-made incidents?

Has that resilience been properly tested? A contractual assurance is cold comfort if an incident shows shortcomings at the expense of your data.

One of the pieces of advice we often provide is that it is important to think of data as a supply chain, which needs to be viewed as being only as secure as its weakest link.

So if your outsourced provider of HR services or finance services, or legal advice, or marketing, or data management is vulnerable then you are too.

The boundary of your organisation is the boundary of its information, not just its premises or its people or its functions.

So much for the basics.

Let us turn to look at the internet itself, and the kind of impact which it's having on the way our society and economy operates.

We all understand how the internet works, right?

The internet protocol structure was designed to provide an ability to move data around a broken network without human intervention.

That's because it was originally intended to provide a means of information transmission which would be capable of at least partially surviving a nuclear attack. It does this by breaking information into small packets which are capable of taking multiple routes to their destination.

It runs over physical telecommunications networks, and is intended to cope with different kinds of network architecture.

The internet has grown and changed enormously since then. Physical networks remain important (and the economics of telecommunications networks remain complicated and difficult).

But the big change which has happened over the last 20 years has been the enormous growth in the scale of the internet, a growth and rate of change which is continuing.

Last year, there were approximately as many internet connected devices on earth as there are people.

By 2017 there will be three times the internet connected devices as there are people.

The number of mobile devices will increase over the same period about 17-fold, and data volumes continue to rise exponentially.

Nearly 2 billion people have “migrated” onto the internet as their preferred means of interacting with the world around them.

The rise of mobile payment systems is likely to provide the biggest single challenge to the banking industry in 500 years.

We are seeing the rapid emergence of what might be called the data economy.

If we think of the agricultural revolution followed by the industrial revolution, followed by the services revolution, we may well now be living through the data revolution.

It’s certainly the case that some of the largest and most successful companies on earth now make their money through the management and monetisation of data.

This has huge implications for the way we think about the role of the state, and about the nature of privacy and security on the internet.

States arose because of their ability to provide internal order (through the Police and Courts in New Zealand) in return for taxes.

Originally, states wanted to be able to raise taxes to prosecute wars, and the benefit of internal order was a kind of by-product of the economics of aggression.

In more recent centuries, democratic pressures have created a new, internal focus for liberal democracies based around welfare, economic growth and the provision of universal health and education.

But the basic bargain has remained valid. It was articulated by Thomas Hobbs in 1651 in “Leviathan”. It is where you and I give up our private right to violence to the state in return for a framework of order.

The historian Ian Morris described this development over the last 7,000 years or so in the pithy phrase “war made the state, and the state made peace”.

The data economy looks very similar: companies like Google and Facebook are able to make their money by organising data, so that the individual benefits from organisation of data to make it easier to use, but the data is then able to be sold.

The expression that sums this up is “if it’s free on the internet, then you are the product”.

So what does all of this mean? In the world of the data economy, privacy and security really are central questions.

But there are no global rules for these issues in the internet, and the sheer scale of the internet means that it is bigger than any given country.

I don't yet detect any broad global consensus in favour of whole-of-internet rule making, and I think that countries like New Zealand need to plan and act accordingly.

It's not that the internet is entirely ungoverned; existing commercial and contract law, competition law, telecommunications regulation and specific rules around subjects like child exploitation provide something of a framework.

But there are a lot of gaps, and we need to think through what any organisation's strategy needs to be in an environment which is at least partly unregulated, and changing rapidly.

Research shows that people in our society are increasingly willing to share their data online, but mistrustful of the organisations, public and private, with which they share their information.

The paradox of privacy and security and of trust remains unresolved at the level of the individual as well as the level of the community.

And there are good reasons to be mistrustful: the internet changes everything, except human nature, which it industrialises.

While that has meant that we have been able to derive great benefit from the internet, it's also provide a super highway for criminals, as well as those engaged in espionage and, increasingly, in conflict.

The key point about crime, espionage and conflict on the internet is that, compared to previous methods, it's easy, cheap and much less risky.

A black economy has grown up providing people with the hacking tools they might want to intrude into systems and steal data, and my key observation here is that barriers to cyber-crime and espionage are falling rapidly.

Sophisticated malware is now increasingly easy to get, at reliably low prices, with a good deal of technical support.

What used to be the preserve of the state is increasingly within reach of criminal groups and even individuals with enough determination to go and seek it out.

The other trend which I think we will see over the next five years is a move from simply stealing data to altering it, or destroying it.

There are already signs of this. The recent incident involving Sony is a good example, but it's not the only one.

And organisations need to plan accordingly.

You can imagine how disturbing it would be to find not only that one's personal data had been copied, but to find key details had been modified along the way.

Before I go on and look at what that might mean for any one of us running organisations in the mid-21st century, it's worth standing back just to capture the wider context: a huge amount of our social and economic life takes place on the internet, which is both less well ordered than we think, and more actively contested than we realise.

Indeed, it's possible to see conflict in the 21st century as being carried out in seven domains (land, sea, air, space, cyber, money and information).

Conflicts in the Middle East, and elsewhere, often involve cyber and information conflict, for example.

What's intriguing about the internet is that it enables both the cyber domain (and to some extent the information domain) to be contested by non-state actors as effectively as by state actors.

A private Navy is beyond most of our reach, but non-state conflict on the internet is entirely feasible.

We've seen for decades the way terrorist groups combine an information narrative with acts of violence.

The internet, the rise of social media and the collapse of the distinction between fact and opinion means that information conflict is also easier, and its barriers to entry are also falling.

This matters at the organisational, as well as international level.

In a post-trust society, where not only the distinction between fact and opinion is contested, but where conventional news media is under enormous economic pressure from the internet, we need to think through the consequences of a fragmentation of news and opinion for the organisations we manage.

This is important for us today because anything which affects the reputation of our organisation (like a major privacy breach) challenges how we manage in the information and media world, as well as our formal cyber security or data privacy policies and responses.

Image and reputation are part of the intangible capital of any organisation just as much as other attributes.

So what does this mean in practical terms?

Firstly, identity. Philosophers have long seen the identity question as a central one in human experience.

The internet puts it on steroids. Loss of identity, identity theft and identity validation will be central challenges for any transaction-based organisation in future.

Society will expect that we know who we are dealing with.

Secondly, the reality of cyber intrusions and theft: it will happen, people will try to take our stuff, and as it gets easier for them to do so, they will succeed at least a proportion of the time.

The public, both in general and as customers, won't be either understanding, or forgiving.

A response plan is not optional; it's going to be essential for any organisation that is to survive with its reputation (and its management) intact.

Get help with this: it's too important to be done on a self-help basis.

And it's urgent.

We will all do everything we can to keep the bad guys out, but we all need to be ready for when things go wrong.

That includes what we actually do, as well as how we handle the reputational fall out, in public.

Thirdly, rules will lag behaviour, at least for our lifetime.

There may one day be a strong international consensus around internet governance and rule-making to constrain bad behaviour and put some sort of self-denying framework around the steps which states might be taking to advance their own interests or use the internet for destructive purposes.

But we're not there yet, and we can't expect to be there any time soon.

If rules lag behaviour, then we need to manage organisations accordingly.

It means that in the commercial world there will continue to be a real (but very uncertain) premium on new ideas, new business models, and new practices.

A genuinely Darwinian process of trial and error, with a very high failure rate.

But it will be a struggle, and there will be many more failures than there will be successes.

If we are running a public sector organisation, we need to watch closely what's happening globally and in the private sector so that we understand what's going on.

But we also need to be very careful about adopting models too quickly and without thinking through what could go wrong.

Fourthly, opinion and reputation will continue to matter even more. In addition to learning how to manage setbacks, I also think that there will be a real struggle for talent in the labour market, and reputation will be really significant in attracting the right people to our organisations in future.

In world where the distinction between fact and opinion has begun to collapse, opinion wins in the short term.

Finally, the real strategic value is likely to come from the ability to learn from others' experience. Paul Ormerod wrote a book some years ago called "Why Most Things Fail".

In it he argued that organisations were surprisingly poor at learning from their experience, but that those that did learn had even more surprising benefits from a limited ability to do so.

In the rapidly evolving world of the internet, and in the swirl of fact, opinion, new business models, trending ideas, and all of the rest then the ability to learn from others' experiences may well turn out to be just as valuable as the ability to learn from our own.

After all, even if our organisations survive a major cyber or privacy incident, the management of the day is not likely to survive. Whatever management has learned may well be lost in a welter of blame.

How much better to cultivate the ability to really learn from others' Darwinian challenges rather than learn it ourselves the hard way.

Let me end by saying again that I think the privacy and security question is one of the central issues of the internet age.

It deserves serious thought, which it doesn't always get.

The internet is hugely convenient, quick and a source of immense productivity as well as pleasure.

It's a lot like 17th century seafaring, with immense fortunes to be made, but with a lot of nameless wrecks along the way.

The internet has many of the features of an ocean of data. Learning to navigate that ocean is a great but risky enterprise which we have all embarked on, perhaps without necessarily realising it.