Video transcript
Cyber Security for Business Owners

[Nigel Phair:]

So one of the things I want you to start thinking about as I'm talking is 'What is your technology strategy?'

For let's call it, the next three years and in technology terms, it's a bit like dog years with the internet, you know. Three years is an awful long time away when you look at what's coming.

So that's a headline to think about is what is your strategy going to be?

How are you going to use information and how are you going to use - mobile devices?

Are you going to go and use cloud enabled technologies?

Are you going to use social media?

Where are you going to store data? How are you going to optimise that data, that you've stored and collected.

Should you be collecting and storing data? If it's personally identifying information? How are you going to control that versus other information?

Lots to think about, what does technology mean to you as a business?

And at the end of the day all this discussion is about risk management and you're probably pretty good at your jobs and you're probably very good at risk management, in every aspect of your organisation, until I put the word 'cyber' in front of it.

And what you're essentially doing as you think about your technology strategy and how you're going to protect your business. Is working out what is the return on investment that I have to come up with when I make certain decisions on investing in controls.

So the first thing you need to think about in your strategy and how you're going to win with technology and how you're going to protect it is 'What is the data assets I hold?'

Now because I said before you don't have enough money to spend on everything. You're going to have to really be very pointed with your investments and your thinking.

And so that comes down to identifying, what are the data assets that you have and ranking them in importance down to not very important.

So some controls to think about as we start thinking about because the criminals are moving ahead so rapidly. You really need to start thinking about what are the controls that I put around that really serious and important data.

So you might be thinking about encrypting it for example, and it's easy to encrypt data.

You've still got to think about your key sets and who has them and where they're held and a whole lot of other stuff. But it's getting easier to encrypt data and hold it.

You might think about moving it to a cloud environment and there's many commercial cloud environments. You've got your big players Microsoft Azure and Amazon Web Services, Google etc. There's lots of smaller players.

You might want to think, is that data being hosted here in Australia or overseas. And a part of your risk management thinking you need to think, is this data so sensitive it's got to reside in Australia.

You might have a government contract and your particular piece of intellectual property. Part of the contract even might be that the data resides in Australia, doesn't go overseas.

People are our key asset when it comes to the business. They're key information users.

We all love our employees, but the reality is all the statistics will tell us and all the surveys tell us 1 in 5 cyber attacks is an insider. And it's either a malicious insider or a stupid insider.

So we really need to think of how do we train our staff in the process of good information security.

What's the tools and techniques that we can give them? What is it that we demand of them? A part of our contract, negotiations and our contract with them as an employee, that they're going to do the right thing with corporate data.

The two other things, the best thing you can do, is A: is what we call reducing administrator access.

So think about your IT network, you're going to have someone with administrator controls that can do everything, can change everything, can update everything. That should probably be one maybe two people.

All the other users on your network should not have any ability of what we call an administrator or root access.

Because if you don't have that and that person get phished, and the criminal tries to use their credentials to download some software which encrypts everything because they don't have that administrator access they can't perform that function.

Incident response is really the number one game town at the very end of it.

So yes, we have a whole lot of people out there trying to do harm to us as users and harm to our organisations. They are really good at what they do, some of them. Some of them trying to make money out of you, some of them just trying to take you down, some of them just want to use your computer power.

How are you going to be ready for it? How are you going to respond? Is the key.

[-END-]