

TRIAL OVERVIEW

SPARK SERVICE SUPPORT

Taking care to ensure People, Process and Technology can work well together will help significantly reduce the risk of cybercrime affecting your business.

Many businesses are too small to bother with unwieldy policy documents. However, virtually everyone is connected to the internet through smart mobile devices. If this is you, then there is still some risk to your business.

Writing policies can be very useful, but only if they are 'owned', maintained and most importantly, enforced by people in your business. If security policies sound like something your business can manage, [click here for our FREE Policy template](#). Otherwise, check out handy tips from CERT NZ* to help you navigate through what will likely be a stressful time.

PEOPLE

Training Your Staff.

When you need to send communications out to the public about an incident, talk to your staff. They're your front line for customer questions, concerns and statements.

In a worst-case scenario, your customers may know of an issue before you do. Your staff need to be aware of the incident and know how to react.

The hardest part of an incident will be preparing and sharing communication. Once you have some details about the incident, you may have to disclose this to your customers. Prepare a guide to have ready in the event of a cyber incident and share it with your staff. It's a lot like having a first aid kit ready just in case! The guide should include:

1. Your company's incident plan and key contacts
2. Who to get their incident information from
3. What they can or cannot say during an incident; and
4. Where customers or the public can report their questions and concerns.

PROCESS

Cybersecurity Contact List.

Your contacts should be able to help you make technical, legal and business decisions. They may also be able to help you resolve the situation. Your contact list should include:

1. Your lawyers (especially in cases where customer data has been compromised)
2. Your IT service provider or IT support consultant
3. Any third parties that you share data or systems with, and a public relations (PR) firm

TECHNOLOGY

Continue Operating as Normal.

During an incident, as the business owner you'll need to continue operating as normal. Think about how your business could continue to operate if your IT systems were:

- unavailable, or
- under the control of an attacker

Consider common business critical systems like email or your key operations software.

Have some alternative business processes for staff to follow when your IT systems are down. Your staff should be able to follow these processes (if they're not handling incident-critical tasks). This means your business can continue to operate even in a limited capacity, while you get the incident under control.