INCIDENT RESPONSE SOLUTIONS

Cyber Incident Simulations and Tabletop Exercises

Incident Response
FORENSIC & CYBER

If your organisation was under cyber-attack, how would you respond?

A cyber incident simulation evaluates your organisation's level of preparedness both from an executive and technical perspective.

The key outcome of a cyber incident simulation, or tabletop exercise as it is often referred, is that your organisation will have greater confidence to prepare, respond and recover in a crisis.

By conducting a simulation, you will:

- establish your current state of readiness
- gain a better understanding of the cyber risks you face
- practice your decision making in a safe environment
- identify areas for improvement.

We combine our experience in responding to actual cyber incidents, along with realistic and engaging tools, to help make your simulation real.

How does it work?

Working with your key sponsors, we expertly design a set of cyber incident scenarios that your organisation is most likely to face. We then create an immersive experience where participants join at varying stages throughout the simulation to apply their subject matter expertise.

A simulation typically consists of four successive scenarios. Our facilitator will introduce each scenario, and depending on progress, add further complicating factors that participants will need to address. Each scenario is timed to ensure the entire simulation is completed. A digital display provides updates and props to ensure it is as realistic as possible.

Simulations and scenarios are designed based on input from the sponsors and our expert knowledge of cyber-attacks, so no two simulations will be the same.

Exercise format

Type

Simulation format, single or multi workplace environment.

Length

Three to four hours.

Participants

Participants typically include executives, general counsels, marketing, strategy, IT management, information security, human resource and risk management professionals.

Structure

- simulation objectives and planning
- meetings with IT and other key stakeholders to ensure realism
- documentation development
- initial briefing
- simulation (four scenarios)
- expert facilitation throughout the simulation
- feedback sessions
- insights discussion, action items and wrap-up.

Logistics

Either in-house, or at a selected location by prior arrangement.

Why Incident Response Solutions?

The core of our business is to provide the confidence you require to prepare for, respond to and recover from incidents, to a forensic standard, i.e. the highest level of proof. We strive to make you look good, even in times of crisis.

We have extensive experience in responding to Cyber Incidents and will ensure your simulation is realistic. We help you uplift your capability, reduce your risk and become better prepared to respond to actual events.

Case Study

WOOLWORTHS NEW ZEALAND

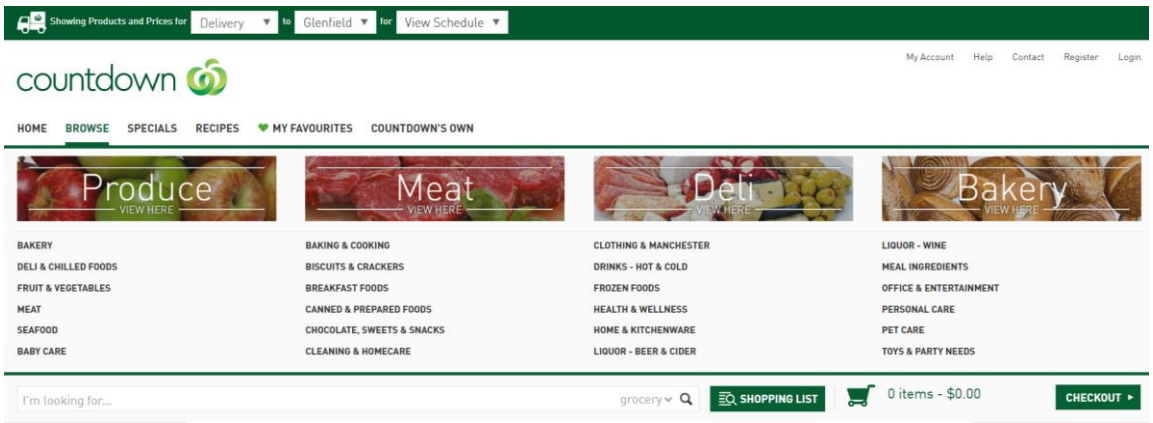
"Countdown regards the security and privacy of its customer data to be critical. We take our obligations seriously, and we wanted to test our cyber incident response procedures to identify any potential areas for further improvement. In order to help us to do this, we sought expert advice from a business offering reputable cyber-crime expertise.

Between February and May 2019, we worked with Incident Response Solutions to develop a simulation to test our cyber incident response maturity.

Incident Response Solutions demonstrated throughout the engagement that they had the expertise and experience to make the simulation not only realistic, but one that provided a number of valuable insights.

As a result of the simulation, we were able to identify a number of areas to build on our existing procedures."

James Radcliffe, General Counsel



Engagement Overview

Incident Response Solutions will lead you through the entire Cyber Incident Simulation process. So you understand what this involves, we've created this handy little guide to help us explain…

PREPARATION

Week 1 – Initial planning

We will provide an overview of the process and help you to compile an initial task list.

Week 2 – Simulation launch

We will draft a welcome letter for you to send to all the participants and other key parties.

Week 3 to 4 – Key stakeholder input

Our forensic and cyber experts will meet with your key stakeholders to ensure we create a cyber incident simulation that is realistic.

SIMULATION

Weeks 5 to 8 – Finalising the situation manual

It takes time to develop an effective cyber incident simulation. We will ensure that the content is clearly articulated into a situation manual which then becomes the primary reference used during the exercise.

Week 9 – Finalise the presentation materials

These materials include the example reports, social media statements, video footage, phone calls etc that will be used during the simulation.

Week 10 – Run the simulation

The Cyber Incident Simulation takes place typically over four hours, involving an expert facilitator from Incident Response Solutions along with all participants and actors.

IMPROVEMENTS

Week 11 – Review feedback and prepare report

We will assemble the feedback from the simulation and where appropriate, suggest improvements to your incident response procedures.

Week 12 - Post-incident review and improvement plan

This is the final session with key stakeholders, where we will step you through the feedback and discuss the recommended improvements.

What next?

Start by asking yourself the following questions … and then get in contact with us.

- What is our current level of maturity within the Incident Response lifecycle?
- Do we have an up to date Incident Response Plan?
- Have we recently tested our Incident Response Plan?
- Have we conducted a post-incident review of any previous incidents, applied lessons learned and made improvements to our plan?

To find out more, please give us a call, send us an email, or visit our website.

Phone 0800 WITNESS (0800 948 637) or
021 779 310 (24 Hour Support)

Email support@incidentresponse.co.nz

Website https://incidentresponse.co.nz

We would be delighted to help.

Incident Response
FORENSIC & CYBER

INCIDENT RESPONSE SOLUTIONS