Preface

We wrote this book because we've become concerned about the undermining of public trust from hacked organisations all over the world who seem to have a poor understanding of stakeholder management.

In this age of the 24-hour news cycle and the unprecedented risk of cyberattack, we don't think it's an option to sweep a cyber breach under the carpet and hope it'll go away. It won't. Nor is it possible to spin your way out of such a situation – as in many similar cases, the consequences of a cover-up can be worse than the original problem.

More than ever, customer trust is currency.

One important premise of this book is that you need to work hard to build a store of this currency *before* you get breached so that when the fateful day comes, you will have a reservoir of goodwill to draw upon.

A reservoir of goodwill and a properly resourced, prepared and practised communication plan will insulate you against the worst of public approbation.

We see new norms of disclosure arising in the face of more prevalent and serious attacks. Laws are being drafted under public pressure as people start to realise that every aspect of their online activities and identities is vulnerable.

Legislators hope that by passing mandatory breach disclosure laws, organisations will start to take cybersecurity seriously and make the needed investments in people, processes and technology to better protect organisational, employee, customer and third-party information.

Large companies are coming under the scrutiny of their stock exchanges who see an obligation to defend shareholder value by encouraging greater accountability at the Board level. They too, need to be informed.

This playbook is a guide to action. It gives you a taste of what a breach looks like when it comes and gives you a framework for competent pre- and post-breach action.

Our hope is you'll be better equipped to face the inevitable scrutiny, whether customer, media, regulatory or all three, by having well rehearsed and honest responses so that you'll be seen as a victim of a crime who has taken all reasonable steps but been caught out, rather than negligent, inept or uncaring.

A good reputation is a fragile thing. It is the gift of those who trust you. But it's a conditional gift and you must earn the right to keep it. This book will set you on that path.

Peter Coroneos and Michael Parker
2 August, 2018

Introduction

It's 2.30 am on a Thursday. The phone rings. Your partner rolls over. "What the...." It's your head of IT. "We've been hacked. Big time." 6.30 am. The mobile goes off. It's the producer of the national breakfast radio show. "We hear you've had a slight issue. Can we do a prerecord now for the 7 am news?" A hastily convened Board meeting, utter confusion, switchboard jammed with angry customers, the Regulator making a 'courtesy' call.

Day 1 over. You thought it would never end. This is a day to forget. You feel a dull dread in the pit of your gut as you realise heads are going to roll – maybe yours too.

Rewind.

Phone rings. Still shock, but at least you have a plan. You convene an urgent call with the Breach Coordination Taskforce. Each is prepped. Fact scenario, latest IT report, review the draft releases. How many affected customers?

Any other companies affected? Government comment? Time to get on the front foot.

Fortunately you'd rehearsed this scenario four months ago, and have all the elements in place. Post on website loaded, Twitter updates continue, statement sent to dedicated media list, with an alert flagging a formal press conference at 10 am. Board has been informed. Phone conference scheduled for 2 pm. In the meantime, your Chairman has received her early morning briefing and then status updates on the hour. Priority media monitoring is in place and the first media reports start to roll in. Call centres are jammed, but centre staff have also been drilled so the prepared statement is provided together with assurances. Information Commissioner's office was the first call that morning. 'Thanks for the heads up, anything we can do to help?'

This is what good situational management looks like. By the end of the week, most of the noise has died down. Stock price is recovering. You've managed to reverse negative sentiment so most

commentators regard you as a co-victim with your customers. You've pulled out all stops, and more importantly, been seen to pull out all stops, to get in front of the issue with an ethical and honest message that is going to be seen by competitors and the market as textbook perfect issue management.

But for you, this was a greater victory.

It demonstrated that the investment in preparedness paid off, despite the predictable protests about cost, inconvenience and necessity, you survived a major cyberattack, and even as mopping up operations continued, you receive congratulatory calls from peers impressed by the calm professionalism and mastery.

You tell them it was no fluke. They ask how.
You give some general pointers and suggest that resourcing readiness and rehearsal is the best insurance against condemnation.

Next time, who knows who'll be hit?

To read more, please purchase the book at
https://cyberbreachplaybook.com/store/p1/buythebook