CYBER CRISIS PLAN

HOW TO PROTECT YOUR REPUTATION FROM CYBERCRIME: A TEN STEP GUIDE TO CRISIS COMMUNICATION PLANNING

Insignia's crisis management experts give leaders, managers and officials the tools, skills and confidence to do and say the right thing when the heat is on. As a result, they can sleep peacefully, knowing they are prepared to respond effectively should the worst happen.

For assistance in ensuring your reputation is well protected in the event of a cyber attack, please contact:

E: info@insigniacomms.com
T: 0121 382 5304
M: 07868 329102
W: www.insigniacomms.com

INSIGNIA
Crisis management training, planning & consultancy

01

CONFIRM LEGAL AND REGULATORY REQUIREMENTS

Knowing how much to say and when is one of the trickiest decisions to make in the event of a data breach. But the starting point should always be the regulatory and legal requirements for disclosure. Make sure that you know what is required of your business.

02

CONDUCT A CYBER REPUTATIONAL RISK ANALYSIS

'Cybercrime' covers a multitude of sins and different kinds of attack will affect the reputations of businesses in different ways. Take time to assess what kinds of cyber attack are most likely to affect your organisation and, crucially, which kind of attack would do most reputational damage.

03

CONDUCT SCENARIO PLANNING

A quick and effective response to cyber attack is impossible without thought beforehand. Assemble key people in advance of an incident to consider how an attack could play out and your response to it. Identify information, capability, resource, knowledge and training gaps to be addressed.

04

CREATE AN INCIDENT RESPONSE PLAN

Based on your reputational risk analysis and scenario planning, build a cyber incident response plan (either as a standalone or as an adjunct to your overall crisis management plan).

05

PREPARE TO COMMUNICATE

Agree message themes to be used in response to a data breach, identify key stakeholders, determine the best communication channels to reach them and ensure you have their contact details to hand. Pre-prepare core communication materials such as your initial media statement and internal briefing.

06

BUILD YOUR CYBER INCIDENT RESPONSE TEAM

Identify the people who would be critical to responding to a data breach and include them in your response plan. Make sure that you include their out of hours contact details – hackers don't work from 9 to 5.

07

DISCUSS RESPONSE PROTOCOLS AHEAD OF TIME

Have key members of your incident response team (IT, legal, communications and HR) meet beforehand and agree principles for cyber incident response. Don't wait until a crisis breaks to find that your communication and legal teams have very different perspectives on what to say and when.

08

TRAIN YOUR SPOKESPERSON

Communicating about a data breach is challenging and sensitive: admitting that you don't know exactly what has happened is uncomfortable, but saying nothing can be the most damaging thing of all. Give your cyber spokespeople media training to ensure they are able to communicate clearly and credibly under pressure.

09

RUN CYBER EXERCISES

When your planning and training is complete, run a simulation exercise to rehearse your team, test the plan and identify where further improvements can be made. Never wait for a real incident to find out whether your plan works and your team has the skills to succeed.

10

REVIEW AND LEARN

Most organisations will be subjected to a cyber attack at some point. If it happens to your organisation, never resume business as usual without a full review of what happened and actions to be taken as a result. Most reputations can withstand a single incident; multiple failures are harder to defend.