



**Are you ready** to communicate during a cyber security crisis?

It is widely agreed that the nature of cyber security threats is changing so quickly that it is becoming harder for organisations to defend themselves against some kind of attack.

**So rather than 'if', businesses should now think in terms of 'when' an attack might happen and plan accordingly. Add the new General Data Protection Regulation (GDPR) into the mix and the issue becomes even more challenging.**

Under GDPR, organisations will have to report a breach to regulators and those affected within 72 hours of it happening or risk being fined. Put simply, time will be of the essence. Cyber security breaches can cost an organisation in terms of loss of productivity, information, time and data, but the loss

of consumer or shareholder confidence and the long-term impact on your organisation's reputation could be the greatest cost of all.

**However, there are steps that any organisation can take to communicate well during a crisis, reduce the potential reputational fallout and recover more quickly >>**

## Cyber crisis communications planning

Any kind of security breach will put a business on the back foot, but the right preparation in case things do go wrong gives you the best chance of getting back on track quickly and with minimum fuss. It also frees up time to get on with the main job in hand - plugging the breach and getting back to full operations.

### How **Black Vanilla** can help

**Successful crisis and stakeholder management will help to reduce the impact a cyber security attack might have on reputation.**

Black Vanilla can work with your organisation to create your communication plan. Typically this starts with a briefing meeting to discuss the types of threat the organisation has identified and the personnel who will be part of the issues management team.

Black Vanilla will then facilitate a crisis communications planning workshop which typically takes place over a half or a full day. Stakeholder and audience mapping, message development and response plans are devised and we start to work on draft statements. After the workshop, the materials and plans are fine tuned by the Black Vanilla team before being signed off by senior management or the board.

**Black Vanilla recommends a six-monthly review meeting to ensure the plans are up to date.**

**A typical workshop will include:**

- › *Reviewing the possible cyber threats your IT team has identified and the business continuity plans you already have in place;*
- › *Selecting an issues management team (IMT) who will handle communications during an issue, based on the skills and authority required to carry out the work;*
- › *Identifying and mapping stakeholder groups and audiences who might be affected by a cyber security event. This might be local or across multiple jurisdictions;*
- › *Discussing how the news cycle might evolve and identifying critical points for communication;*
- › *Identifying communication priorities and work flows;*
- › *Preparing key messages, fact sheets, a Q&A or FAQs. Drafting copy for notification emails, writing media and website statements; drafting social media posts if relevant.*

**Black Vanilla can complete your preparations with media and social media training if required.**

### Our experts



Cyber security crisis communication workshops are lead by one of Black Vanilla's directors, Nichole Culverwell ACIPR. Nichole has nearly 25 years' experience in public relations in a career which spans London, Sydney and Guernsey. **She is an accredited practitioner with the Chartered Institute of Public Relations and has worked with businesses in the retail, pharmaceutical and financial services sectors.**

**Remember, you can't respond well unless you're prepared and equipped appropriately. If you would like to talk to Black Vanilla about cyber crisis communications planning please contact: [Nichole@black-vanilla.gg](mailto:Nichole@black-vanilla.gg)**



7 & 8 The Grange, St. Peter Port, Guernsey GY1 2PX T: **01481 729229** W: [black-vanilla.gg](http://black-vanilla.gg)