

The Cyber Crisis Communications Respond & Recover Package

Being ready to communicate quickly and confidently in the event of a cyber security incident requires careful planning. Done well and you can reduce speculation and position the organisation as being in control and responsive to the needs of its customers and other stakeholders. This helps to manage the impact on those affected and minimise the risk of reputational damage.

Black Vanilla and Resolution IT fuse their specialist expertise to help organisations mitigate the disruption of a cyber security incident.

- Know how to reach your customers, the regulators, intermediaries and other stakeholders
- Have key messages prepared and a media strategy ready
- Anticipate the response from media and on social media
- Keep communication tools in an easy-to-access Cyber Vault separate to your usual IT systems



Regulation now in force

The Guernsey Financial Services Commission Cyber Security Rules 2021 are now in force, and firms must ensure compliance with the Rules by 9th August 2021

Part 5 – Respond

- (1) The licensee must be able to demonstrate that it has a plan in place which aims to mitigate any disruption caused by a cyber security event.

Best practice response plans include communications strategies and these also help organisations to ensure they can also undertake essential communications activities during the recovery phase:

6.1 Recovery from Cyber Security Events

(1) The licensee must be able to demonstrate that it is aware of the appropriate steps that need to be taken in order to restore business capabilities, following a cyber security event, and ensure essential activities are capable of being undertaken in the interim period.



Cyber Crisis Respond & Recover Package from Black Vanilla and Resolution IT

This cost-effective package gives organisations the tools and training they need to create a best practice communications plan and keeps all your communications assets safe in a Cyber Vault.



STEP 1 Tools and Training

A half-day crisis communication training workshop, sharing best practice. You will benefit from the combined expertise of crisis communications and cyber security intelligence with specialists from Black Vanilla and Resolution IT.

During the workshop, we will assess and discuss:

- Cyber risk and communications response
- Crisis communications capabilities and gaps
- Practicalities which impact communications response
- Communication strategies for stakeholders, media and social media
- Key messages and other media/social relations tools

You will be given a set of crisis communications planning templates; following the session, these can be completed by you and your team. A review of your completed plan by Black Vanilla is included in the fee.

What's included?

Half-day workshop for up to four staff with Black Vanilla and Resolution IT

Crisis planning templates / workbook

Review of client's crisis communications plan (one review only)

In the event of a crisis, two hours of crisis consultation time[i]





STEP 2

Secure your assets – Crisis Vault - Resolution IT

All brand assets needed in a crisis would be stored in a Crisis Vault – through Resolution IT.

You, along with Black Vanilla and Resolution IT have 24/7 access to the vault, to enable you to keep the contents up to date.



Additional Services

Black Vanilla offers a number of additional, aligned crisis communication services which include:

- Drafting media statements, Q&As and FAQs
- Preparing graphics for social media

The above materials are helpful to hold ready in the client's Crisis Vault.

- Media training spokespeople



Meet the Experts

Nichole Culverwell, Director, Black Vanilla

Nichole is a CIPR Chartered Public Relations Practitioner and has a CIPR Specialist Diploma in Crisis Communications. She specialises in strategic public relations services and crisis communications and offers a number of different training courses, including media training for corporate spokespeople.

Nick Robilliard, Information Security Consultant, Resolution IT

Nick has worked in security roles in both the public and private sector and particularly enjoys helping people understand that everyone has a role in securing valuable information. He holds the globally recognised ISC2 Systems Security Certified Practitioner (SSCP) qualification.



[i] Must be utilised with a two-year period of completing the workshop. If not utilised, the client will receive a 15% discount on a follow up workshop or training session.