BC Training LTD

Crisis Communications and Public Relations after a Cyber Security Incident

1 Day

Telephone 01253 542650
(or +441253 542650 outside the UK)
Email info@b-c-training.co.uk

www.b-c-training.com

Head Office Address
Business Continuity Training Ltd, 21 Fairhaven Road, Lytham St Annes, Lancashire, FY8 1NN United Kingdom

Crisis Communications and Public Relations after a Cyber Security Incident

Course Overview

A one day non-technical course, aimed at preparing organisations to manage their crisis communications and Public Relations after a cyber security incident. The course is aimed at both communications and PR professionals, as well as crisis, resilience and business continuity professionals.

The course will teach participants how to understand the requirements of responding to a cyber incident and how to develop appropriate communications under the particular circumstances of a cyber incident. Topics include cyber risk assessments, crisis response hierarchy and working with CIRT teams and learning from other organisation's communications' successes and failures.

This course can be run in-house at your premises or it can be delivered live online.

"Thankfully, we now live in a world where it is accepted that data breaches happen and organisations are more comfortable disclosing that they have been victim to an attack. However, with this welcome move away from victim blaming, organisations are now being judged more on how well they manage a breach." - Brian Honan, Computer Weekly

Programme

Course Overview and Introductions

Module 1 – Introduction to Cyber and the Threat Landscape

- What are the possible types of cyber attacks?
- Double and triple ransomware attacks
- Good & poor communications and PR practice examples in response to cyber incidents

The above points will be illustrated by a number of case studies.

Module 2 – Understanding your organisation's threats, level of preparation and impacts if an attack were to occur

- What are the particular threats to your organisation?
- How to understand the impact of a cyber incident
- Cyber security standards and what you have in place
- Data risk assessment - what you have to lose and the consequences if there is a data breach

Module 3 – Crisis Communications Response Framework

- Roles and responsibilities of Communications and PR during cyber incidents
- Communications role within a CIRT
- Coordination of internal and external communications

Crisis Communications and Public Relations after a Cyber Security Incident

Module 4 – Communications Response Strategies

- Low profile and maximum exposure communications strategies - what has worked and what has not
- The benefits and downsides of each communications channel
- Responding on a full ransomware lockout when channels and information may not be available to responders
- Preparation for a cyber incident, including website preparation and providing information to stakeholders

Module 5 – SEPA Case Study

- Learning from the SEPA cyber incident of Christmas 2020, including a review of external communications

Module 6 – Stakeholder Identification and Regulatory Reporting

- Identifying the stakeholders which need to be communicated with under different scenarios
- Statutory and regulatory reporting
- Requirements and timings for reporting to the ICO
- Development of an effected stakeholder communications plan in response of ICO reporting requirements

Module 7 – Developing Lines to Take and Responding During a Cyber Security Incident

- Developing lines to take in response strategies and writing internal communications statements
- Use of appropriate language and terms
- Framing your response
- Explaining ransomware pay or not to pay decisions
- Identify appropriate support to be offered to those effected
- Exercise to practice skills leaned

Final Quiz and Feedback

- Final quiz to check understanding
- Debrief of the course
- Actions and next steps

Crisis Communications and Public Relations after a Cyber Security Incident

Course Benefits

- Know what actions you can take now to ensure that you are prepared
- Communication with stakeholders will define your organisation's success or failure during a cyber incident
- Avoid making the same communication mistakes other organisations have made responding

Who Should Attend?

- Communications and PR professionals
- Crisis, risk and business continuity practitioners

If you have further questions or would like an official quotation please contact a member of the BC Training Team:

Contact Details

Business Continuity Training Ltd
21 Fairhaven Road
Lytham St Annes
Lancashire FY8 1NN
01253 542650 **www.b-c-training.co.uk**
info@b-c-training.co.uk

Registered in England - No. 6609297