

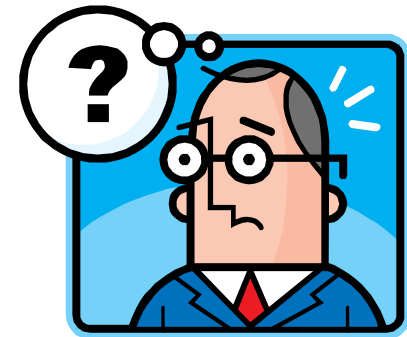


Crisis Communications for Incident Response

Not if but when

As of mid-2020, up to 88% of UK companies have suffered breaches in the last 12 months, [Carbon Black reports](#). That is lower than Germany (92%), France (94%), and Italy (90%)

- Nintendo
- Easy Jet
- Marriott Data Breach
- Antheus Tecnologia Biometric Data Breach
- CAM4 Exposes 10.88 Billion Records

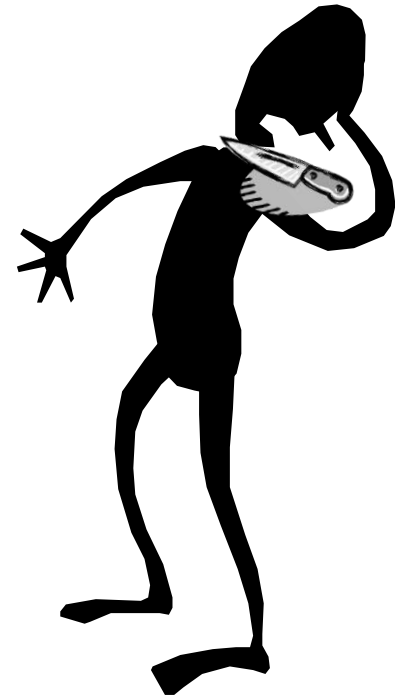


Accept the inevitable and do not get caught
with your pants down



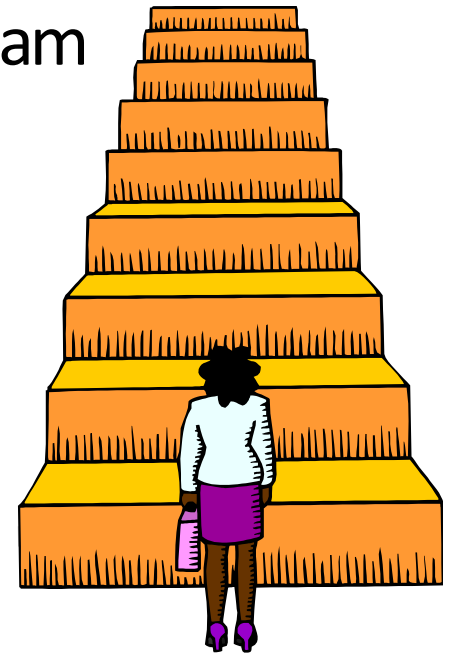
Fail to plan and...

- You will not be able to respond when an incident hits your organisation
- You will appear in the news in a bad light
- Your brand will be damaged
- Your companies value will decrease
- Heads will roll



Key steps

- Establish cross functional crisis management team
- Monitoring strategy – has incident happened
- Develop a crisis plan – checklist
- Prepare for different breach scenarios
- Comms plan know your audiences
- Practice and media training for team
- Remember internal as well as external comms



Crisis management team

- CISO/ IT Security Manager
- CIO / IT Director
- CFO / Financial Director
- CEO / Managing Director
- Comms Director / Marketing Director
- Sales Director / Customer Support
- CRO / Legal Counsel
- External Lawyers
- External Forensics
- External PR specialists



How will you find out?

- IT/CISO
- Staff / manager
- Customer(s)
- Social media
- Criminal (extortion)
- Regulator
- Journalist enquiry
- Website / media / news group



Crisis PR is Different

- First objective stay out of the press
- Second Objective if you can't, need to minimise impact
- Not all publicity is good publicity
- Different skills reduce impact of bad news
- Time sensitive, right message, right now
- You need a specialist approach

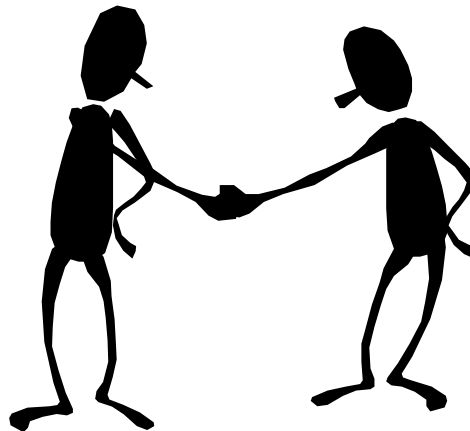


Crisis Comms Plan

- Prepare crisis check list to deal with potential scenarios
- Create a timeline so everyone knows who will do what when
- Team consults with legal and forensics team to determine what incident is and establish who it affects
- Can you keep it under wraps?
- What are your regulatory responsibilities to disclose?
- Which stakeholders are affected?
- Who is responsible for communicating with each group and in what order?

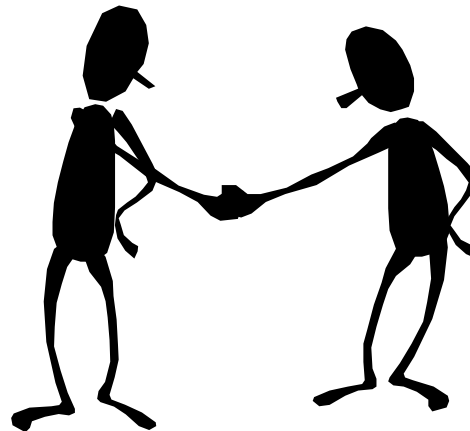
Crisis Comms Plan

- If regulator involved, how to minimise fine by demonstrating appropriate action taken
- If customers involved, what is impact on them and how should they be informed
- If press involved, how to manage the communications
- Social media can exponentially increase if not responded to quickly and appropriately



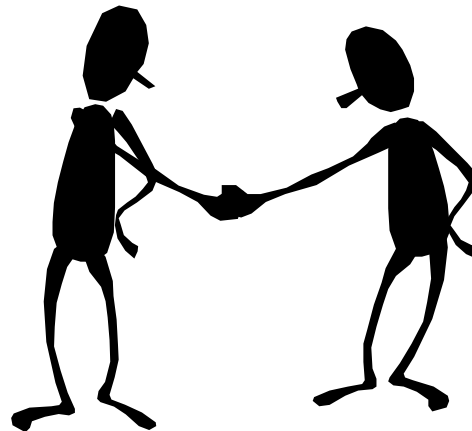
Crisis Comms Plan

- Messages must be consistent so need to brief managers and employees, especially customer facing teams
- FAQ on incident scenarios can be prepared in advance
- Everyone should know who should answer questions or who to refer to
- Spokespeople must be media trained



Crisis Comms Plan

- Prepare Comms Plans in advance with statements on anticipated likely breach scenarios developed by team
- Review plans quarterly with team to see if risk profile has changed
- Do not forget internal comms



How to deal with the media

- Only deal with the press if you have to
- Try to buy time first to investigate claims
- Be as honest as you have to in statements
- Do not drag out bad news in small steps
- Build credibility by being as open as possible
- When to make a public statement
- Press page on your website (FAQ)
- Strategy for dealing with incoming journalist enquiries



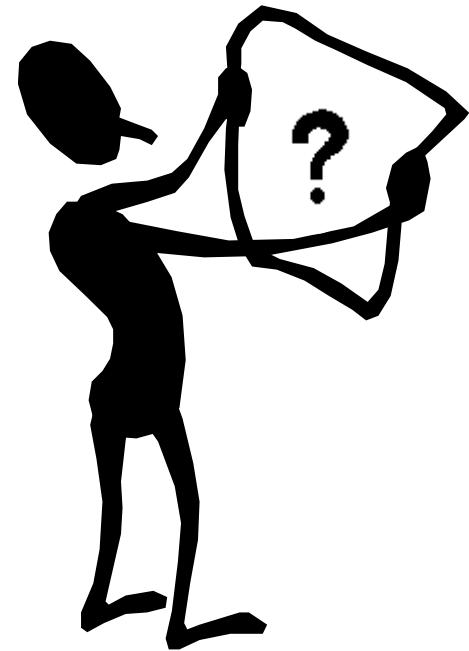
Social Media

- Has changed the comms landscape
- Your stakeholders will all use it
- Highly likely it will be first place news is broken
- Media use it to source stories
- Twitter hacks of PA and Bloomberg show impact
- Social media must be part of comms plan
- Do it wrong and the brand impact can be massive
- Do it right and you can come out unscathed



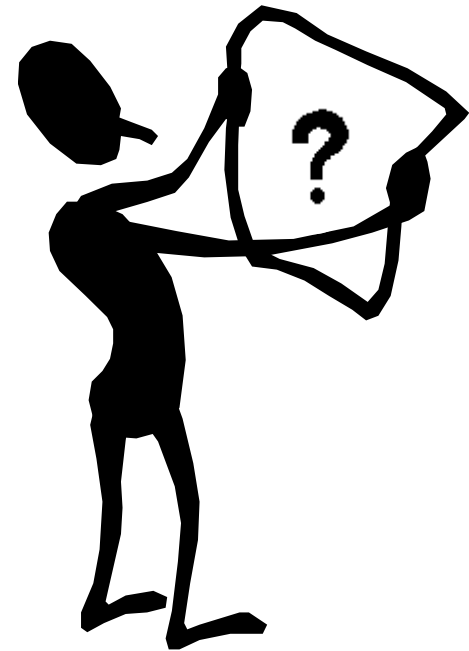
Crisis Plan

- Bring team together in room/conference call
- Brief on incident and likely impact
- Who knows already
- Establish if need to disclose
- Communications timeline
- External communications drafted
- Internal Communications drafted



Crisis Plan

- Brief spokespeople and set up 24 hour cover
- FAQ for website
- Brief customer support on FAQ and dealing with media and customer enquiries
- If necessary inform customers
- Start responsive social media campaign
- Communicate with key media and other press
- Keep Calm and Carry on you will get through it



Thank you

Neil Stinchcombe

Eskenzi PR Ltd.

Tel: +44 2071 832 833

Mobile +44 7947 613 303

Email: neil@eskenzipr.com
www.eskenzipr.com



© Eskenzi PR Limited 2016