BUSINESS

Reputation Management Framework.

The following document outlines the key steps an organisation should take from a reputation management perspective in the event of a crisis.

Royal Bank of Scotland

Scottish Business Resilience Centre

RBS.CO.UK

Reputation Management Framework.

The following document outlines the key steps an organisation should take from a reputation management perspective in the event of a crisis.

Pre-Event

In advance of an event, there are a series of steps organisations must consider to be fully prepared. By doing these, they may help ease any further reputation management issues that arise in the case of an event occurring. This includes:

Must do

Create a crisis/reputational management process and plan which is secure, but accessible in case if IT disruption

- Agree decision makers and core crisis team, retaining specialists if required
- Agree information/resource flow and crisis team roles and responsibilities (including single point of contact to receive incoming info)
- Establish crisis database featuring:
    - □ Trading jurisdictions (sector and country) and applicable regulations defining how crisis must be addressed
    - □ Data encryption levels
    - □ Any security gaps that could be reputationally harmful
    - □ Contacts sheet with email and emergency phone numbers
    - □ Client library/database with technical experts/focus areas
- Creation of draft responses for likely scenarios aligned to key stakeholders
- Preparation of content for company website to be activated during a crisis (for FAQs, hotline etc.)
- Address challenges with mass comms e.g., bulk emails identified as spam

Incorporate your partners and supply chain

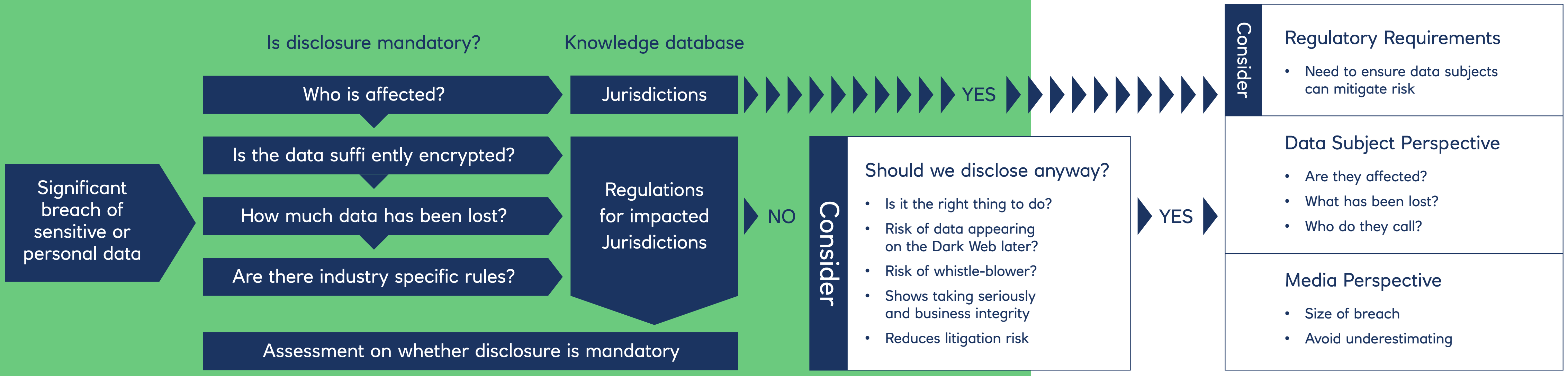
- Ensure contracts account for breaches
- Determine approach if supplier breached
- Involve key partners in planning and rehearsals, as appropriate

Consideration of the following areas (not necessary, but recommended):

Establish what the Post-Event aims are

- Regularly rehearse and test scenarios
- Ensure communications approach is included
- Identify and involve key decision makers (including your comms team)
- Work through realistic scenarios – don't just rely on testing one scenario

DECIDE WHETHER TO DISCLOSE



Significant breach of sensitive or personal data

Is disclosure mandatory?

Who is affected?

Is the data suffi ently encrypted?

How much data has been lost?

Are there industry specific rules?

Knowledge database

Jurisdictions

Regulations for impacted Jurisdictions

Assessment on whether disclosure is mandatory

NO

YES

Consider

Should we disclose anyway?

- Is it the right thing to do?
- Risk of data appearing on the Dark Web later?
- Risk of whistle-blower?
- Shows taking seriously and business integrity
- Reduces litigation risk

YES

Consider

Regulatory Requirements

- Need to ensure data subjects can mitigate risk

Data Subject Perspective

- Are they affected?
- What has been lost?
- Who do they call?

Media Perspective

- Size of breach
- Avoid underestimating

Crisis Response

Framing the message

Must do

Gather information

- **Prepare and agree a fact sheet if necessary**
- **Ascertain if a wider issue at play (i.e. other organisations also impacted)**

Accept responsibility

- **You are custodians of the data – apologise**
- **Even when a stakeholder (including customer) is at fault you will be expected to have mitigated through multifactor authentication and monitoring**

Avoid downplaying

- **Address feelings of vulnerability for those impacted**
- **Identify steps those impacted can protect themselves**

Avoid blaming others

- **Hacking groups – gives them the limelight**
- **Service partners – can lead to public disagreements**

Consideration of the following areas (not necessary, but recommended):

Ensure factors to avoid message damaging credibility addressed

- **Previous data breaches**
- **Exposure of organisational limitations**
- **Breach being discovered by third party**

Take into account age, gender and cultural differences – will everyone understand?

Other considerations

- **Involvement of Police and ICO**
- **Whether you will be open about failings to avoid future breaches**

When to disclose

Notify those impacted as quickly as possible

- **Addresses feelings of vulnerability for those affected**
- **Important data subjects hear the news early to avoid a loss of trust**
- **Obligations around insider trading**

Balance between accuracy and timing

- **Sometimes difficult to ever establish true scale of breach**
- **Avoid underestimating**

Based on regulations for applicable jurisdictions and advice from Law Enforcement

Ways to share the message

- **Utilise owned channels to share news with appropriate audiences**
- **It may be appropriate to use all available channels for communication to increase reach**

Direct

Email

- **Requires email contact details**
- **May have been compromised from attack**
- **Can be tailored to target those most impacted**
- **Challenges include server throughput and spam filters**

Physical Mail

- More direct and personal
- Avoids risk of phishing, but not immediate form of communication
- May not have correct (up-to-date) address
- Expensive and may also be seen as damaging to the environment

Telephone

- More personal / caring
- Resource intensive
- May not have current number

Website

- Less direct – data subjects need to visit site
- Can contain FAQs, hotline nos.

Indirect

Social Media

- Opportunity to set the initial tone of social media posts
- Interactive so able to set straight negative rumours
- Risk of negative reinforcement spiral

Traditional Media

- Often main source of information for customers
- Have own agenda and may not focus on the things you want
- Consider list of trusted journalists to help disseminate

Prepare for reaction

- Brief staff
    - □ Ensure sufficient social media / call centre resources available
    - □ Scale up response website and phone capacity as appropriate
- Ensure capability in place for dealing with media enquiries
    - □ Anticipate drop in share price or sales for first few days
    - □ Put measures in place to disrupt future phishing/scam attempts

Deliver the message

- Keep the message clear and easy to understand
- Avoid jargon
- Keep it simple
- Ensure CEO / Chair delivers message to establish organisation is taking crisis seriously
- Reconfirm breach represents crisis to prevent unnecessary escalation
- In choosing spokesperson consider their capability in front of media
- Honed policy for media management e.g. no call backs

Post-event

After an event (or an exercise), it is as important to review the aspects that went well and those that did not to inform the future plan. In doing this post-mortem, it is vital that the key stakeholders clearly address these successes and failures in a pragmatic fashion. Should the organisation have failed in some areas, consider bringing in a third-party organisation to support the organisation in the future (and have them appointed and on stand-by should a crisis arise in the future) or by ensuring training is arranged for those who require it.

As part of this post-mortem, the following should be addressed and adapted as necessary

- Timing – how quickly did you respond? Were all internal and stakeholders addressed?
- Content – was this accurate? Was the tone of content right?
- Spokesperson – is this the right person? Do you need more spokespeople?
- General process/plan review – did the plan cover all eventualities? What were the gaps, and could they be reclarified for the future?
- Right the culture – restore trust internally and externally
- Build a drumbeat of good news, while focusing on mitigating risk

This document references guidance from Richard Knight and Jason R.C. Nurse, "Effective Communications and Public Relations after a Cyber Security Incident" available from https://doi.org/10.1016/j.cose.2020.102036 and https://jasonnurse.github.io/comms.pdf

Royal Bank of Scotland

RBS.CO.UK

Scottish Business Resilience Centre