# Poster: A Framework for Effective Corporate Communication after Cyber Security Incidents

Jason R.C. Nurse[1*] and Richard Knight[2]
[1]University of Kent, UK,
[2]University of Warwick, UK
[*]J.R.C.Nurse@kent.ac.uk

**Title:** A Framework for Effective Corporate Communication after Cyber Security Incidents

**Authors:** Richard Knight and Jason R.C. Nurse

**Venue:** Computers & Security

**DOI:** 10.1016/j.cose.2020.102036

**Full reference:** Richard Knight and Jason R.C. Nurse, "A framework for effective corporate communication after cyber security incidents", Computers & Security, Volume 99, 2020, Elsevier, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102036.

**Abstract:** A major cyber security incident can represent a cyber crisis for an organisation, in particular because of the associated risk of substantial reputational damage. As the likelihood of falling victim to a cyberattack has increased over time, so too has the need to understand exactly what is effective corporate communication after an attack, and how best to engage the concerns of customers, partners and other stakeholders. This research seeks to tackle this problem through a critical, multi-faceted investigation into the efficacy of crisis communication and public relations following a data breach. It does so by drawing on academic literature, obtained through a systematic literature review, and real-world case studies. Qualitative data analysis is used to interpret and structure the results, allowing for the development of a new, comprehensive framework for corporate communication to support companies in their preparation and response to such events. The validity of this framework is demonstrated by its evaluation through interviews with senior industry professionals, as well as a critical assessment against relevant practice and research. The framework is further refined based on these evaluations, and an updated version defined. This research represents the first grounded, comprehensive and evaluated proposal for characterising effective corporate communication after cyber security incidents.

# A Framework for Effective Corporate Communication after Cyber Security Incidents

Jason R.C. Nurse [1]* and Richard Knight [2]
[1] University of Kent, UK, [2] University of Warwick, UK
* j.r.c.nurse@kent.ac.uk @jasonnurse https://jasonnurse.github.io

## Introduction

- A **cyber security incident** can represent a crisis for an organisation, both because of its impact on operations and the associated risk of reputational damage.
- Security is not only about preventing attacks but also about **responding appropriately having succumbed to an attack**, both in technical and socio-technical incident response.
- This research focuses on **socio-technical incident response**, and engages in a critical, multi-disciplinary investigation into the efficacy of crisis communication and public relations following a data breach.

## Contributions

- A critical investigation into **effective and poor communication after cyber security incidents**, according to **academic literature** and a series of **real-world case studies** (including commentary from well-respected, international security specialists).
- The development, evaluation and refinement of **the first comprehensive framework to enhance best practice regarding corporate communications and announcements in instances of security incidents**.

## Methodology

[redacted] hacking: how not to respond to a cyber attack

[redacted] blamed for [redacted] breach, admits it was hacked

All the Ways [redacted] Epically Bungled Its Breach Response

The [redacted] data breach is way worse than first thought

How could [redacted] have retained customer trust after it was hacked?

Systematic Literature Review

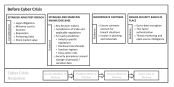
Real-world Case Analysis

Academic best practice

Evaluation of literature review and case analysis findings

Industry best practice

Best practice guidance



Develop initial framework

Initial framework

Evaluate framework (via interviews with CISOs, CIOs, Directors, PR/Comms specialists)

Feedback analysis

Refine and release framework

University of Kent | Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)

**References**

Knight, R., & Nurse, J.R.C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security, 99*. https://doi.org/10.1016/j.cose.2020.102036

Knight, R., & Nurse, J.R.C. (2020). A framework for effective corporate communication after cyber security incidents. Whitepaper. https://jasonnurse.github.io/comms.pdf

## Before Cyber Security Incident (Pre-Event stage)

**Establish/Prioritise Post Event Aims** (Consider)
- Protecting Data Subject
- Managing key Stakeholders
- Minimise damage to reputation
- Protecting sales / ability to trade
- Legal obligations
- Stock market value
- Minimising cost to business

**Determine Security Gaps to inform Communications Response** (Consider)
- Security audits and risks
- Assess key hygiene factors
  - Up-to-date/strong encryption
  - Multi-factor authentication (MFA)
- Utilise threat monitoring and open source intelligence (OSINT)

**Establish and Maintain Crisis Communication Capability** (Guidance)
- Agree decision makers and cross functional crisis team
- Educate, consult and support decision-makers / board
- Establish crisis information knowledge database
  - Jurisdictions trading in and applicable regulations
  - For each jurisdiction:
    - Industry specific regulations
    - Disclosure benchmarks
    - Sanction regimes
    - Class action risks
  - How is personal / sensitive data encrypted
  - Security gaps identified that could be reputationally harmful
  - Ensure information secured but accessible in event of IT disruption
- Review internal capability and retain specialists if required
- Establish draft responses for likely scenarios aligned to key stakeholders
- Consider website to be activated during a crisis (for FAQs, hotline etc.)
- Address challenges with mass comms e.g. bulk emails identified as spam

**Incorporate Partners and Supply Chain** (Guidance)
- Ensure contracts account for breach situations
- Determine approach if supplier breached
- Involve key partners in planning and rehearsals

**Perform Regular Rehearsals and Testing** (Consider)
- Incorporate communications response within Business Continuity Plans (BCP) and Major Incident Rehearsals
- Involve key decision makers
- Work through realistic scenarios
- Include scenarios for breaches within supply chain

## Cyber Security Incident Response (Cyber Crisis Response stage)

**Significant breach of sensitive or personal data**

**Decide Whether to Disclose**

**Is disclosure mandatory?**
- Who is affected?
- Is the data sufficiently encrypted?
- How much data has been lost?
- Are there industry specific rules?
- Assessment on whether disclosure is mandatory

Knowledge Database: Jurisdictions; Regulations for Impacted Jurisdictions

Yes / No

**Should we disclose anyway?** (Consider)
- Is it the right thing to do?
- Risk of data appearing on Dark Web later?
- Risk of whistle-blower?
- Shows taking seriously and business integrity
- Reduces litigation risk

Yes

**Establish What to Disclose** (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

**Frame the Message**

Guidance
- Accept responsibility
  - You are custodians of their data – apologise
  - Even when stakeholder (including customer) is at fault (e.g., password reuse) you will be expected to have mitigated through multifactor authentication (MFA) and monitoring
- Avoid downplaying – may be seen as not taking breach seriously
- Address feelings of vulnerability for data subjects
  - Identify ways data subjects can protect themselves
  - Consider providing credit monitoring – ensure free to customer or this may be seen as profiteering
- Avoid blaming others
  - Blaming hacking groups – gives them the limelight
  - Blaming service partners – can lead to public disagreements

Consider
- Review aggravating factors to avoid message damaging credibility
  - Previous data breaches – "Are you really taking security seriously?"
  - Exposure of organisational limitations – "Is your comprehensive security plan that good?"
  - Breach being discovered by third party – "Is the security of customer data really at the heart of what you do?"
- Take into account age, gender and cultural differences
  - Ethical Stance – Gender and age differences
  - Younger generation may be less impressed with credit monitoring as a mitigation
- Other considerations
  - How are you working with law enforcement to bring the culprits to justice?
  - Can you share lessons learnt in due course to help others avoid repeating your mistakes?

**Choose When to Disclose** (Consider)
- Better to notify public as quickly as possible
  - Helps address feelings of vulnerability for those affected
  - Important data subjects hear it directly from you first to avoid a loss of trust
  - May be easier to frame public opinion at an early stage in a crisis
  - 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

**Select How to Disclose**
- If possible, it is important data subjects hear it directly from you first, otherwise it may result in loss of trust
- It may be appropriate to use all available channels for communication to increase reach

**Direct**

**Email**
- Requires email address
- May enhance perception of harm and generate negative emotions
- Can be tailored to target those most impacted
- Challenges include server throughput and spam filters

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

**Surface Mail**
- More direct and personal
- Avoids risk of phishing
- 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

**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, e.g. "twitter storm"

**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** (Guidance)
- Brief staff
- Ensure sufficient social media / call centre resources
- Scale up response website and telephony capacity
- Anticipate move of transactions to non-breached channels
- Ensure capability in place for dealing with media enquiries
- Anticipate drop in share price for first few days
- Put measures in place to disrupt phishing/scam attempts

**Deliver the Message** (Guidance)
- Keep the message clear and easy to understand
  - Avoid jargon
  - Keep it simple
- Ensure CEO / Chair delivers message
  - To establish organisation is taking things seriously
  - Reconfirm breach represents crisis to prevent unnecessary escalation
  - In choosing spokesperson consider their capability in front of media