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


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

Contributions

- 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.

Methodology

- Systematic Literature Review
- Academic best practice
- Real-world Case Analysis
- Develop Initial Framework
- Evaluate Framework (via interviews with CISOs, CIOs, Directors, PR/Comms specialists)

Before Cyber Security Incident (Pre-event stage)

Establish Priorities: Post Event Aims
- Protecting Data Subject
- Managing Key Stakeholders
- Minimising damage to business
- Minimising cost to business
- Minimising cost to reputation
- Minimising legal obligation
- Stock market value

Determine Security Gaps to inform Communications Response
- Security public and press
- Assess key hygiene factors
- Review incident response
- Multi-factor authentication (MFA)
- Utter threat monitoring and open source intelligence (OSINT)

References


University of Kent Interdisciplinary Research Centre in Cyber Security (KIRC)