Effective Communications and Public Relations after a Cyber Security Incident

Richard Knight and Jason R.C. Nurse

Cyber security incidents and attacks are a harsh reality faced by every business today. While one of the primarily goals of security measures is to prevent incidents from occurring, your company also needs to be prepared to respond if it becomes a victim of an attack.

Effective communication following a cyber security incident forms a critical element of the activities needed to protect your company's customers, stakeholders, and reputation more generally. This communication goes hand-in-hand with the more technical incident response strategies, to create a broad business continuity approach. These activities are essential for all types of organisations, from small/SMEs to large enterprises.

This document aims to support you in the event of a cyber security incident, by providing new and extensive guidance on how to communicate and engage effectively in such situations. This can inform and complement your existing practices and help to increase the resilience of your organisation if breached.

Specifically, a guidance framework for communication and public relations is introduced below, which provides advice on what organisations should do before a breach occurs (to prepare themselves) and after a breach (to respond in such a way that it reassures customers and stakeholders).

This guidance, it addresses questions such as: What mechanisms should be in place to best prepare for if a security breach occurs? How should a security breach be communicated to stakeholders? When should it be communicated and by whom? Answering these questions in the right way can make a substantial difference to how stakeholders respond to the news of a breach.

This framework is grounded in industry and academic best practice, and has been evaluated refined through interviews with senior security professionals and crisis response specialists within industry.

This framework was produced by Richard Knight & Jason R.C. Nurse, and published in the Computers & Security Journal. For more information, see: Knight R. & Nurse, J.R.C. (2020), "A Framework for Effective Corporate Communication after Cyber Security Incidents", Computers & Security (99). Elsevier.
Full article link: https://doi.org/10.1016/j.cose.2020.102036 and https://arxiv.org/abs/2009.09210

A FRAMEWORK FOR EFFECTIVE CORPORATE COMMUNICATION AFTER CYBER SECURITY INCIDENTS

Pre Event

Consider

Establish/Prioritise Post Event Aims

- Protecting Data Subject
- Managing key Stakeholders
- Minimise damage to reputation
- Protecting sales / ability to trade
- Legal obligations
- Stock market value
- Minimising cost to business

Consider

Determine Security Gaps to inform Communications Response

- 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)

Guidance

Establish and Maintain Crisis Communication Capability

- 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

Guidance

Incorporate Partners and Supply Chain

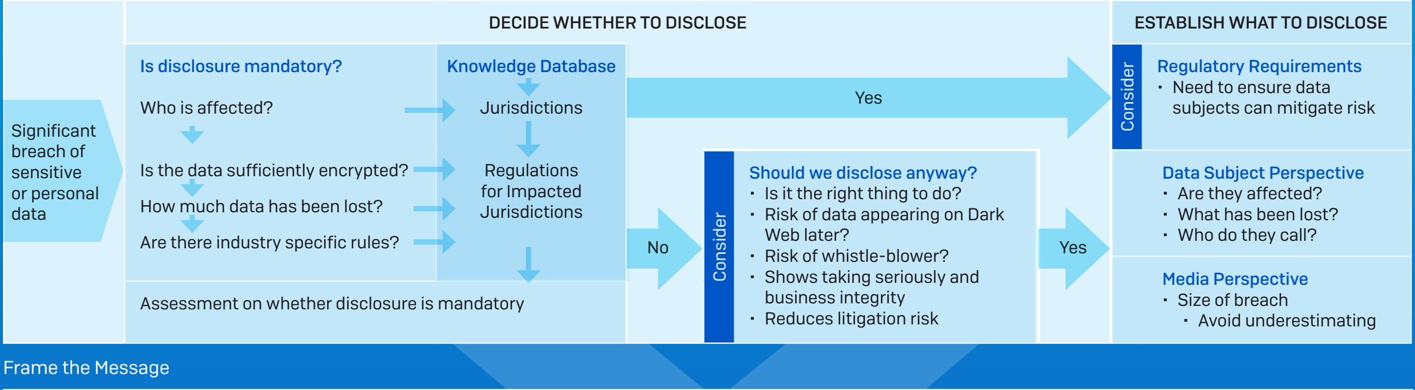
- Ensure contracts account for breach situations
- Determine approach if supplier breached
- Involve key partners in planning and rehearsals

Consider

Perform Regular Rehearsals and Testing

- 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 Crisis Response



DECIDE WHETHER TO DISCLOSE

Significant breach of sensitive or personal data

Is disclosure mandatory?

Who is affected?

Is the data sufficiently 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

Yes

No

Consider

Should we disclose anyway?

- 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 a 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		Indirect
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	**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	**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"
Website • Less direct – data subjects need to visit site • Can contain FAQs, hotline nos.	**Telephone** • More personal / caring • Resource intensive • May not have current number	**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

Richard Knight and Jason R.C. Nurse, https://doi.org/10.1016/j.cose.2020.102036