A Framework for Effective Corporate Communication after Cyber Security Incidents. *Computers & Security, 99*.
https://kar.kent.ac.uk/82836/
https://doi.org/10.1016/j.cose.2020.102036

University of Kent | Institute of Cyber Security for Society (iCSS)

Effective Communication after a Cyber Security Incident

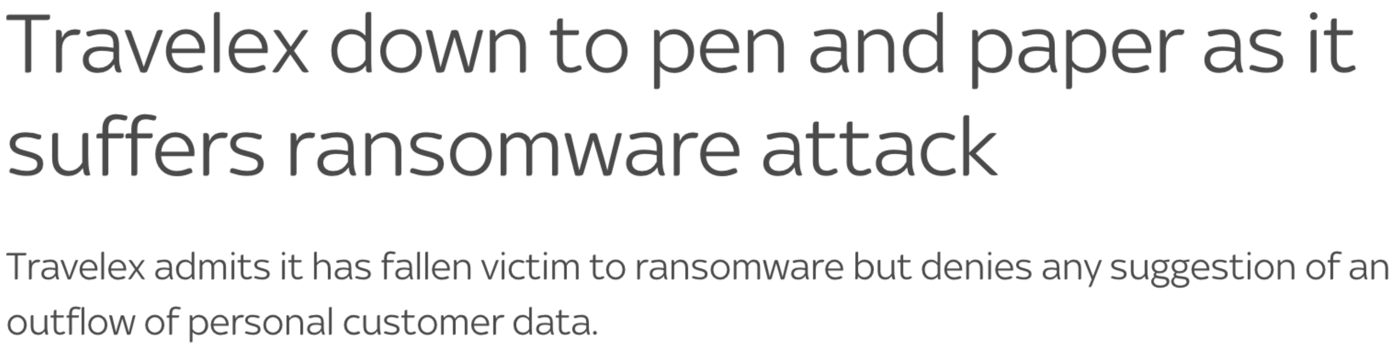
Dr Jason R.C. Nurse
Associate Professor in Cyber Security,
University of Kent

✉ j.r.c.nurse@kent.ac.uk

in jasonrcnurse   jasonnurse   jasonnurse.github.io

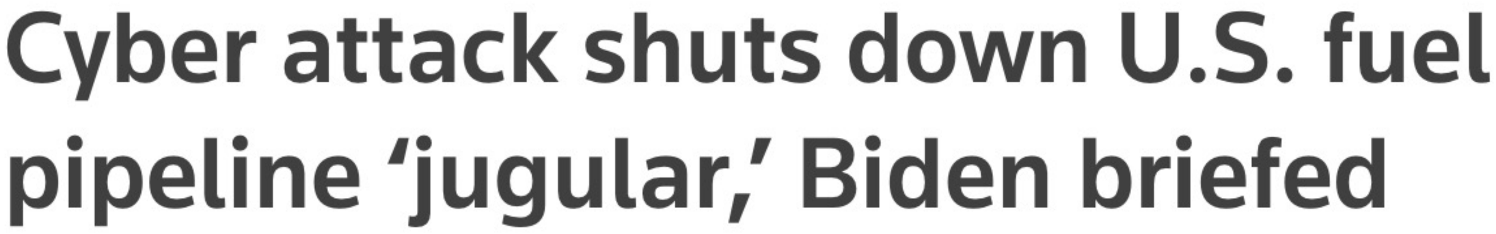
“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

Robert Mueller, Former Director of the FBI

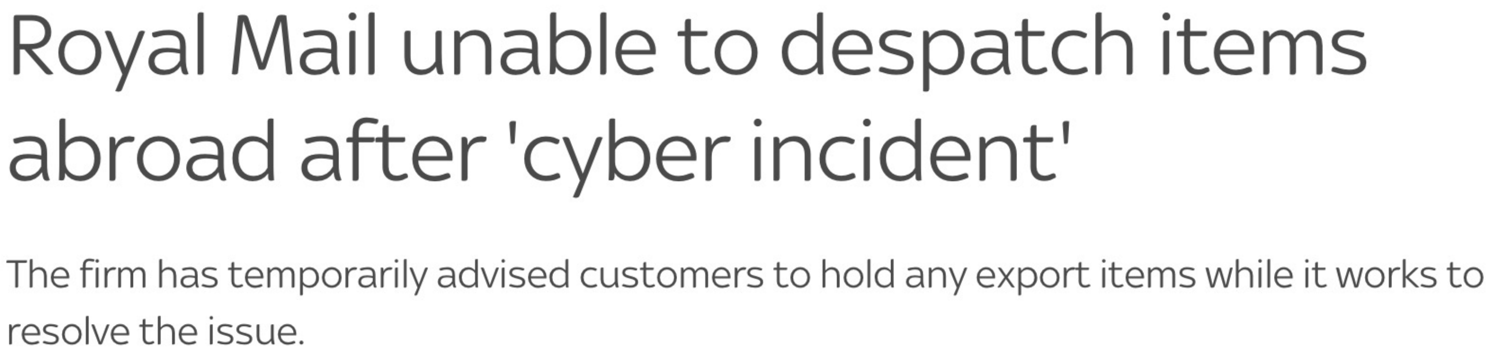


Travelex down to pen and paper as it suffers ransomware attack

Travelex admits it has fallen victim to ransomware but denies any suggestion of an outflow of personal customer data.



Cyber attack shuts down U.S. fuel pipeline ‘jugular,’ Biden briefed

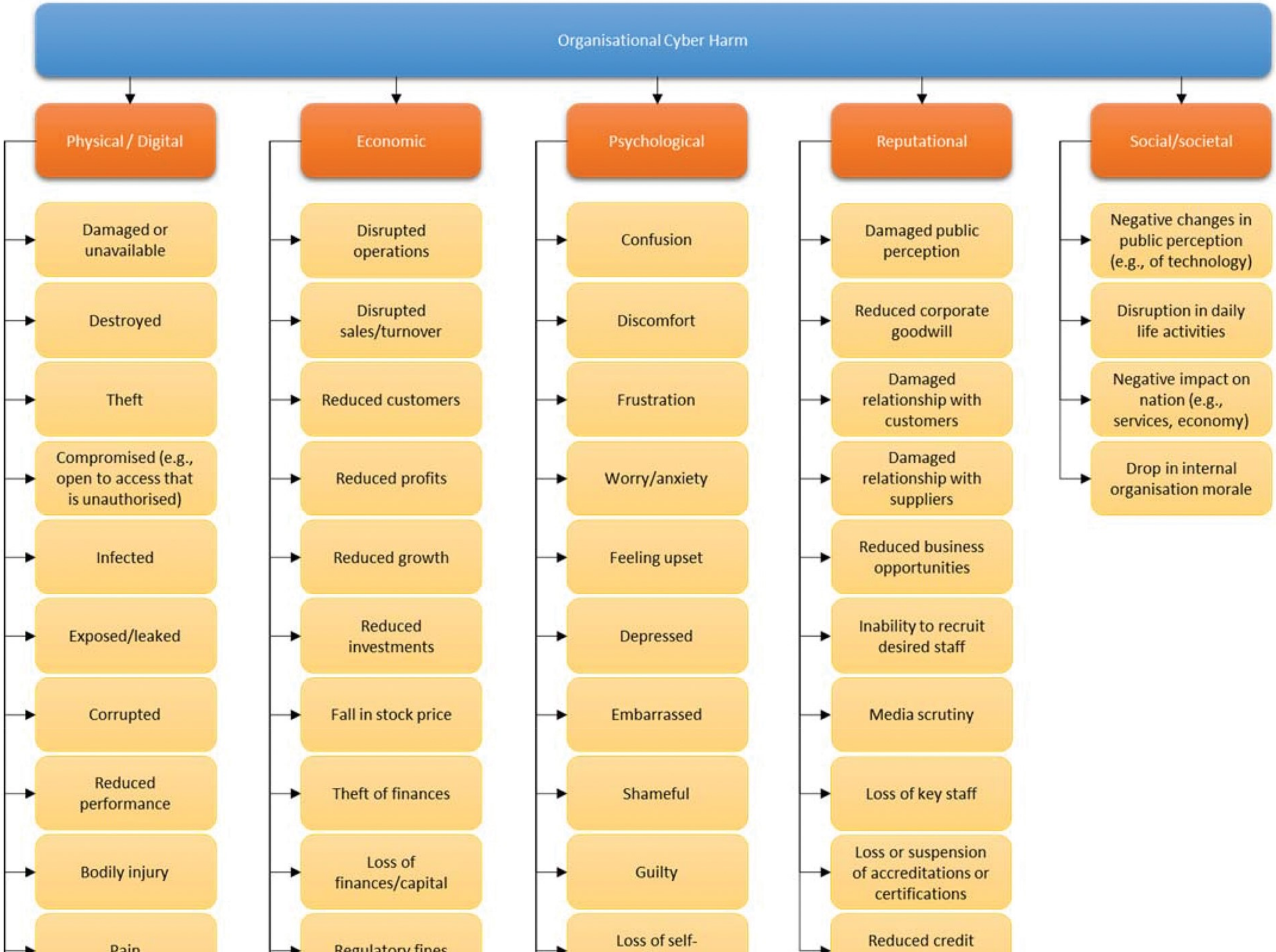


Royal Mail unable to despatch items abroad after 'cyber incident'

The firm has temporarily advised customers to hold any export items while it works to resolve the issue.

A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate

https://doi.org/10.1093/cybsec/tyy006



Organisational Cyber Harm

- Physical / Digital
  - Damaged or unavailable
  - Destroyed
  - Theft
  - Compromised (e.g., open to access that is unauthorised)
  - Infected
  - Exposed/leaked
  - Corrupted
  - Reduced performance
  - Bodily injury
  - Pain
- Economic
  - Disrupted operations
  - Disrupted sales/turnover
  - Reduced customers
  - Reduced profits
  - Reduced growth
  - Reduced investments
  - Fall in stock price
  - Theft of finances
  - Loss of finances/capital
  - Regulatory fines
- Psychological
  - Confusion
  - Discomfort
  - Frustration
  - Worry/anxiety
  - Feeling upset
  - Depressed
  - Embarrassed
  - Shameful
  - Guilty
  - Loss of self-
- Reputational
  - Damaged public perception
  - Reduced corporate goodwill
  - Damaged relationship with customers
  - Damaged relationship with suppliers
  - Reduced business opportunities
  - Inability to recruit desired staff
  - Media scrutiny
  - Loss of key staff
  - Loss or suspension of accreditations or certifications
  - Reduced credit
- Social/societal
  - Negative changes in public perception (e.g., of technology)
  - Disruption in daily life activities
  - Negative impact on nation (e.g., services, economy)
  - Drop in internal organisation morale

University of Kent | Institute of Cyber Security for Society (iCSS)

BBC

Mass
hits 1

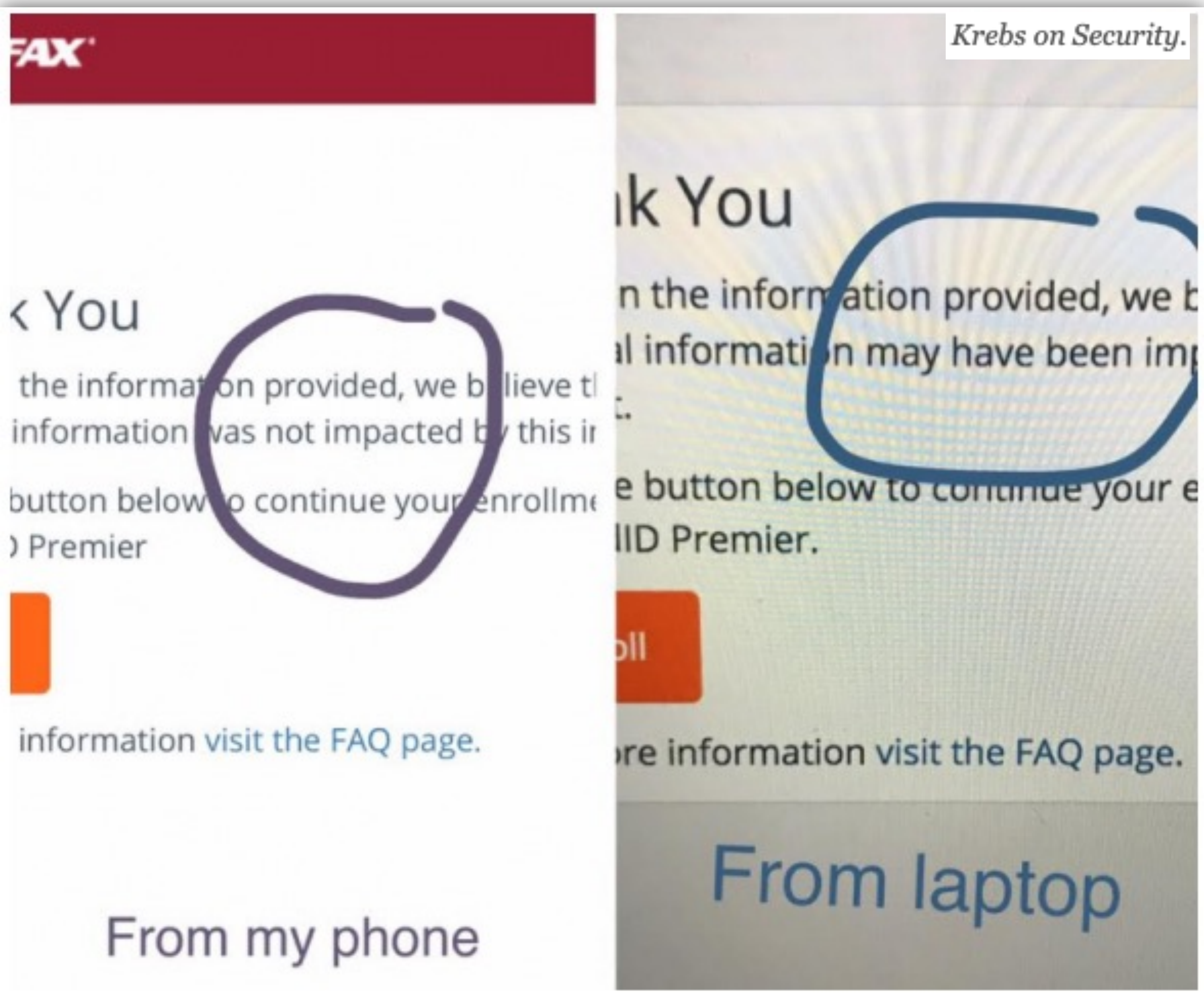
7 September 2

THE WALL STR

States Push close Hack

Equifax faced a patch nd to whom

- Using a se s phishing by some b
- Official Tw nes, instead of



k You

the informat on provided, we b lieve t
information was not impacted b this i

button below o continue your enrollm
Premier

information visit the FAQ page.

From my phone

k You

n the information provided, we b
l information may have been imp
.

e button below to continue your e
ID Premier.

oll

re information visit the FAQ page.

From laptop

the key question

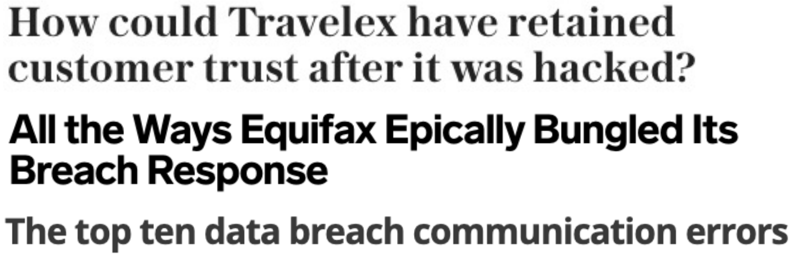
What is effective communication / public relations after a cyber security incident?

the approach

Systematic review of literature

Academic
best practice

Real-world case analysis



How could Travelex have retained customer trust after it was hacked?

All the Ways Equifax Epically Bungled Its Breach Response

The top ten data breach communication errors

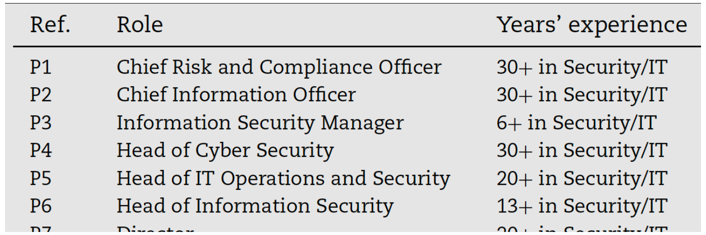
. . .

Industry
best practice

Evaluation of literature review and case analysis findings

Best practice
guidance

Develop, evaluate and refine framework

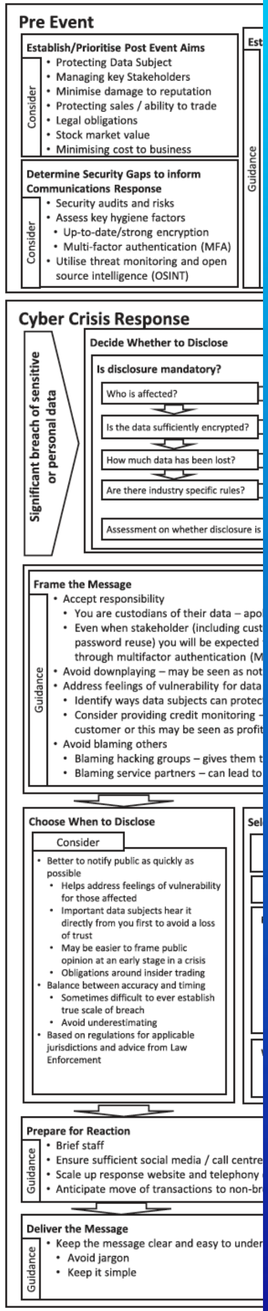


Ref.	Role	Years' experience
P1	Chief Risk and Compliance Officer	30+ in Security/IT
P2	Chief Information Officer	30+ in Security/IT
P3	Information Security Manager	6+ in Security/IT
P4	Head of Cyber Security	30+ in Security/IT
P5	Head of IT Operations and Security	20+ in Security/IT
P6	Head of Information Security	13+ in Security/IT
P7	Director	20+ in Security/IT

validated framework / playbook

Knight, R., & Nurse, J.R.C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security, 99.*

https://kar.kent.ac.uk/82836/



Pre Event

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)

Est
Guidance

Cyber Crisis Response

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

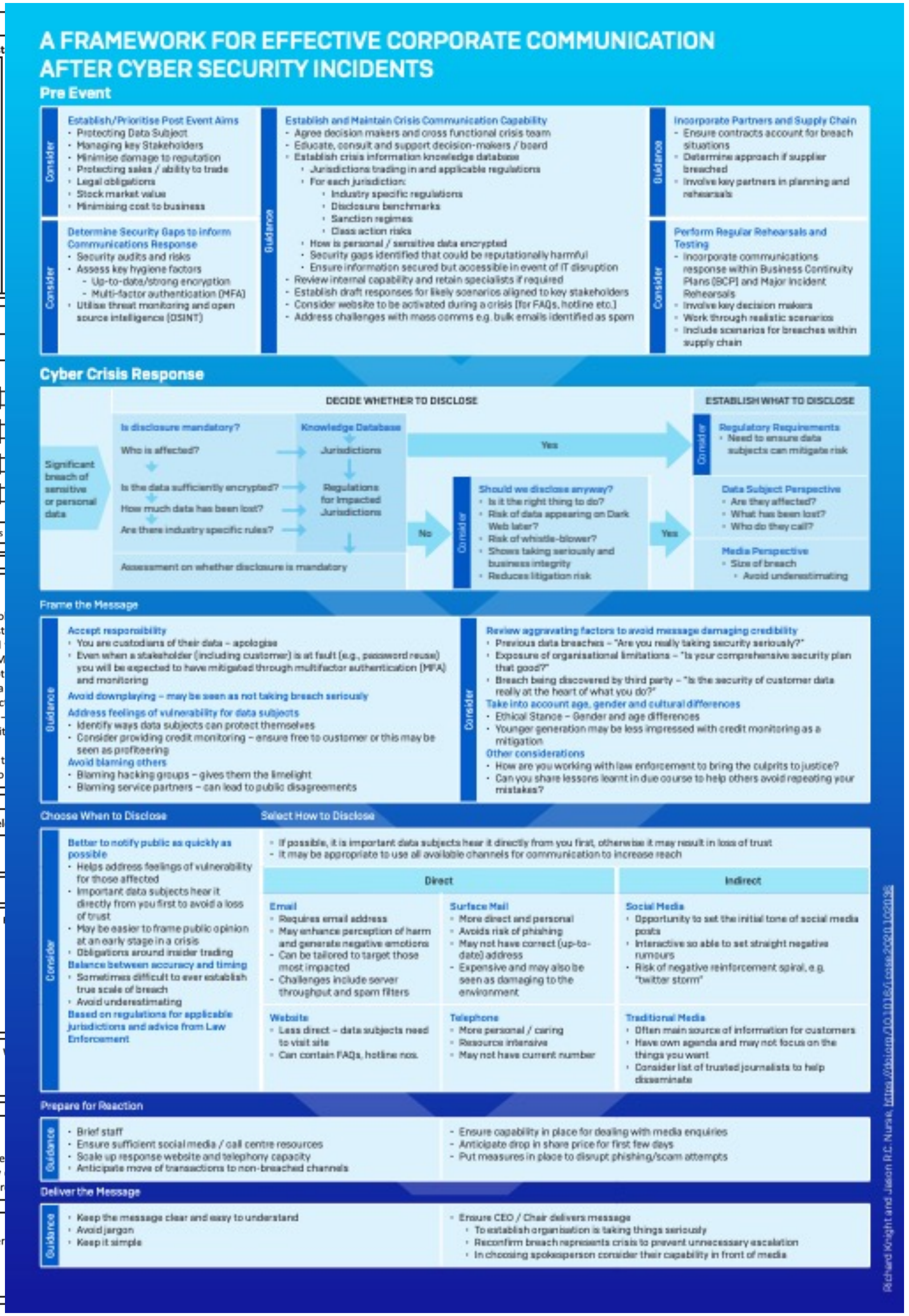
Frame the Message
Guidance
- Accept responsibility
  - You are custodians of their data – apo
  - Even when stakeholder (including cust password reuse) you will be expected through multifactor authentication (M
- Avoid downplaying – may be seen as not
- Address feelings of vulnerability for data
  - Identify ways data subjects can protec
  - Consider providing credit monitoring customer or this may be seen as profit
- Avoid blaming others
  - Blaming hacking groups – gives them t
  - Blaming service partners – can lead to

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

Sel

Prepare for Reaction
Guidance
- Brief staff
- Ensure sufficient social media / call centre
- Scale up response website and telephony
- Anticipate move of transactions to non-br

Deliver the Message
Guidance
- Keep the message clear and easy to under
  - Avoid jargon
  - Keep it simple



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

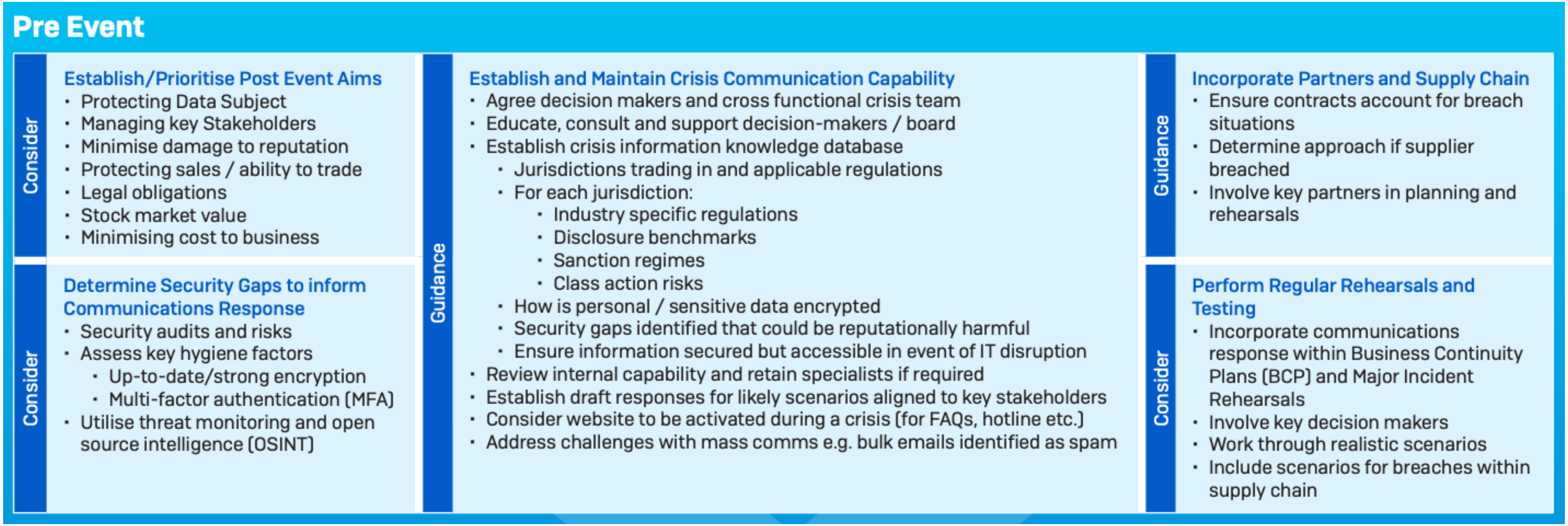
Guidance
- Brief staff
- Ensure sufficient social media / call centre resources
- Scale up response website and telephony capacity
- Anticipate move of transactions to non-breached channels
- Ensure capability in place for dealing with media enquiries
- Anticipate drop in share price for first few days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

validated framework / playbook



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

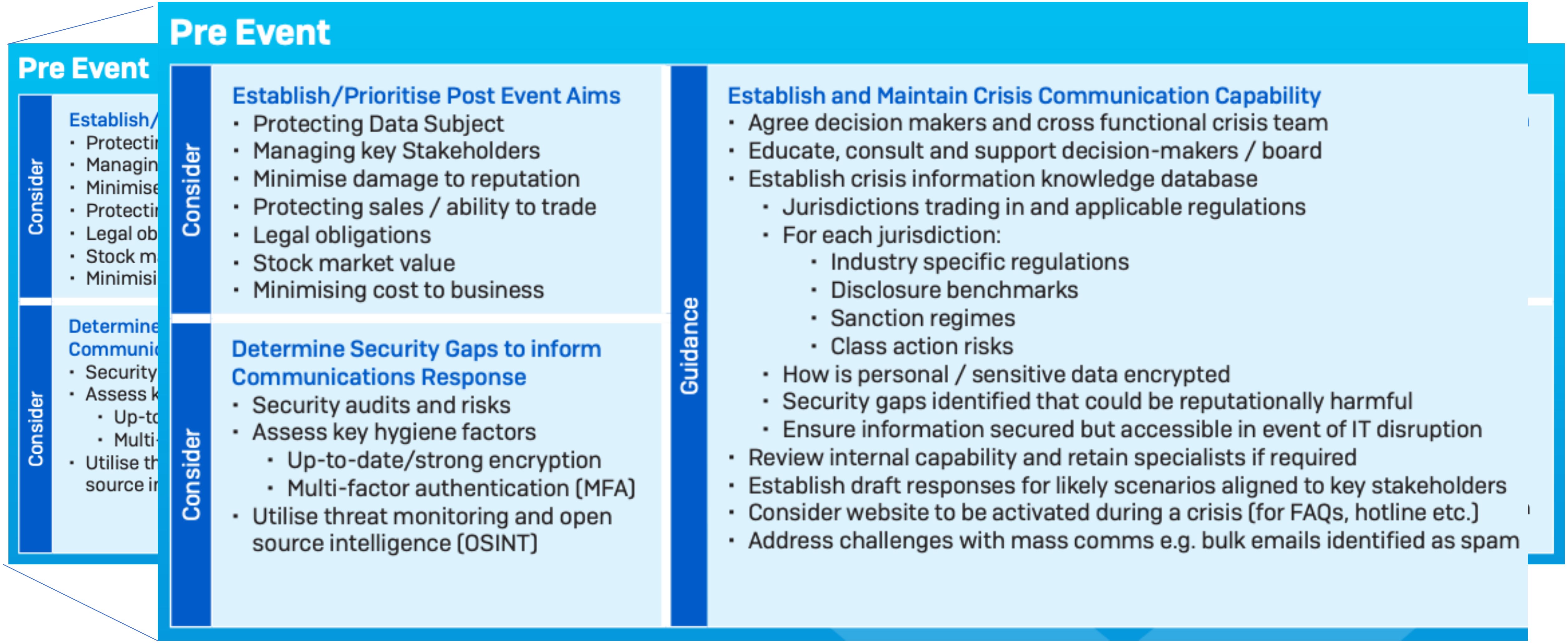
Consider

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

…

validated framework / playbook



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

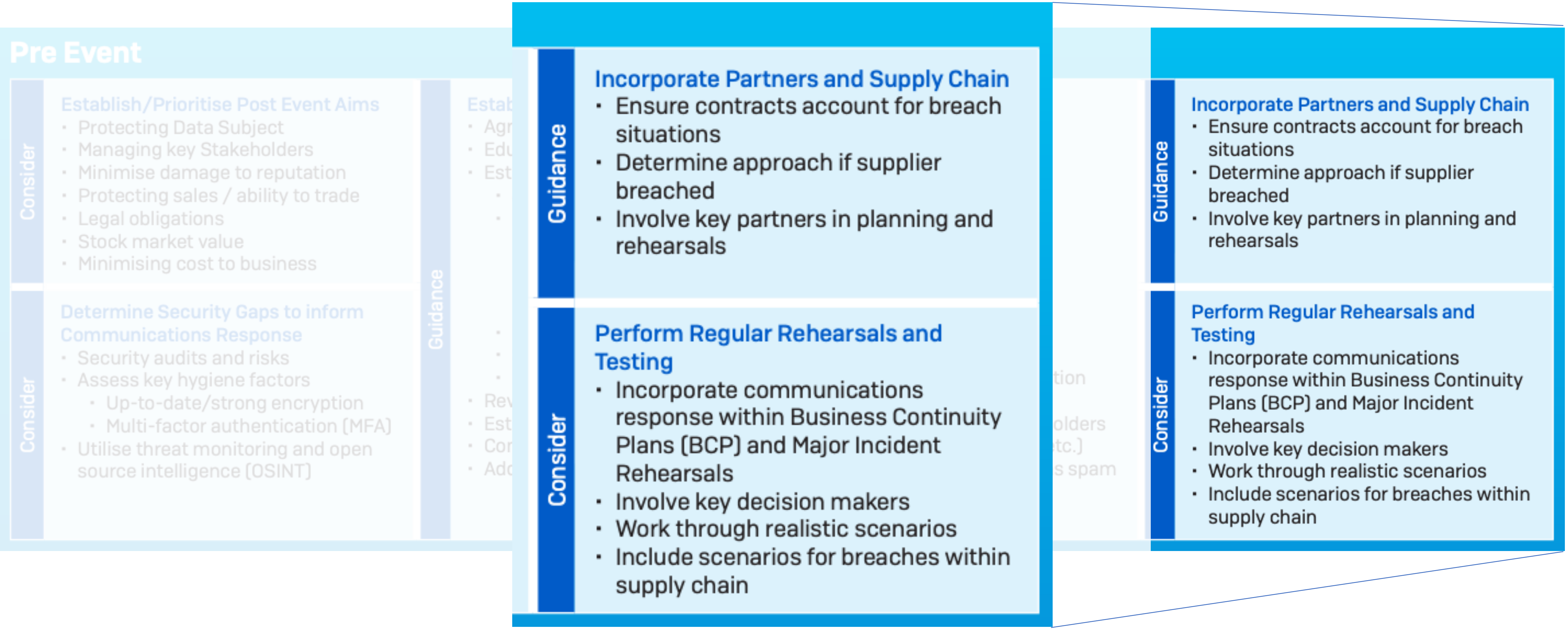
Establish and Maintain Crisis Communication Capability

- 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

Pre Event
Consider
Establish/
Protecti
Managin
Minimise
Protecti
Legal ob
Stock m
Minimisi
Consider
Determine
Communi
Security
Assess k
Up-to
Multi-
Utilise th
source in

• • •

validated framework / playbook



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

Estab
- Agr
- Edu
- Est
- Rev
- Est
- Cor
- Add

tion

olders

tc.)

s 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

Guidance

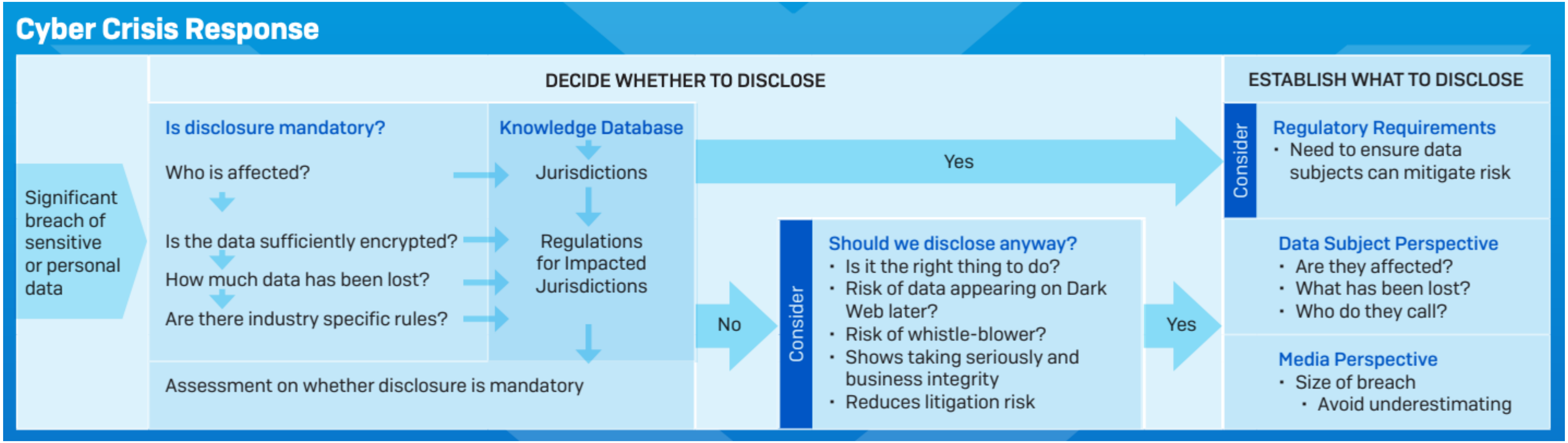
Incorporate Partners and Supply Chain
- Ensure contracts account for breach situations
- Determine approach if supplier breached
- Involve key partners in planning and rehearsals

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

• • •

validated framework / playbook



Cyber Crisis Response

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?

Knowledge Database

Jurisdictions

Regulations for Impacted Jurisdictions

Assessment on whether disclosure is mandatory

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

ESTABLISH WHAT TO DISCLOSE

Regulatory Requirements

- Need to ensure data subjects can mitigate risk

Data Subject Perspective

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

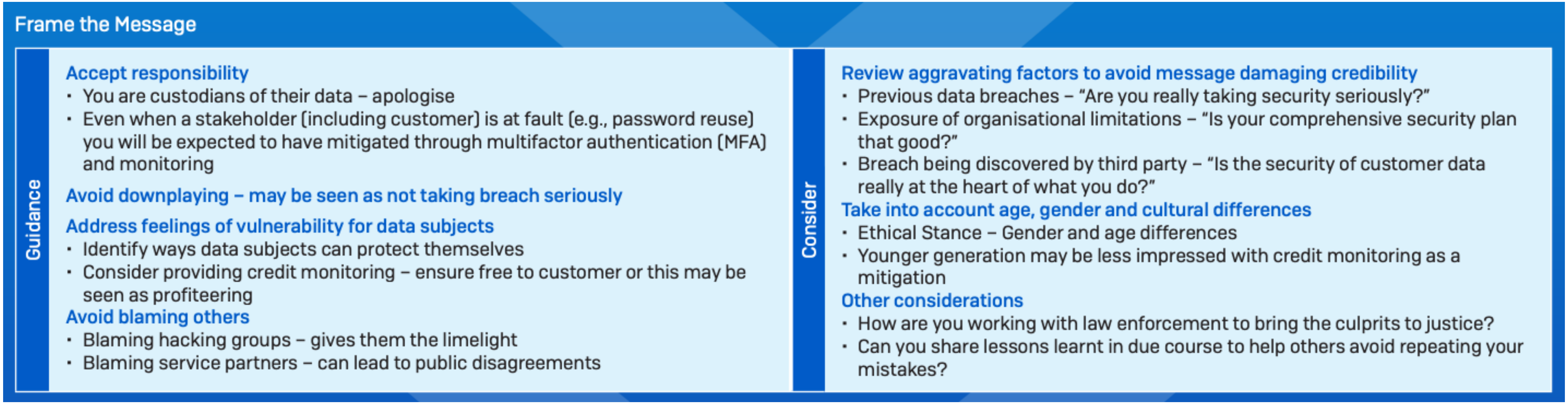
Media Perspective

- Size of breach
  - Avoid underestimating

…

validated framework / playbook

...



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

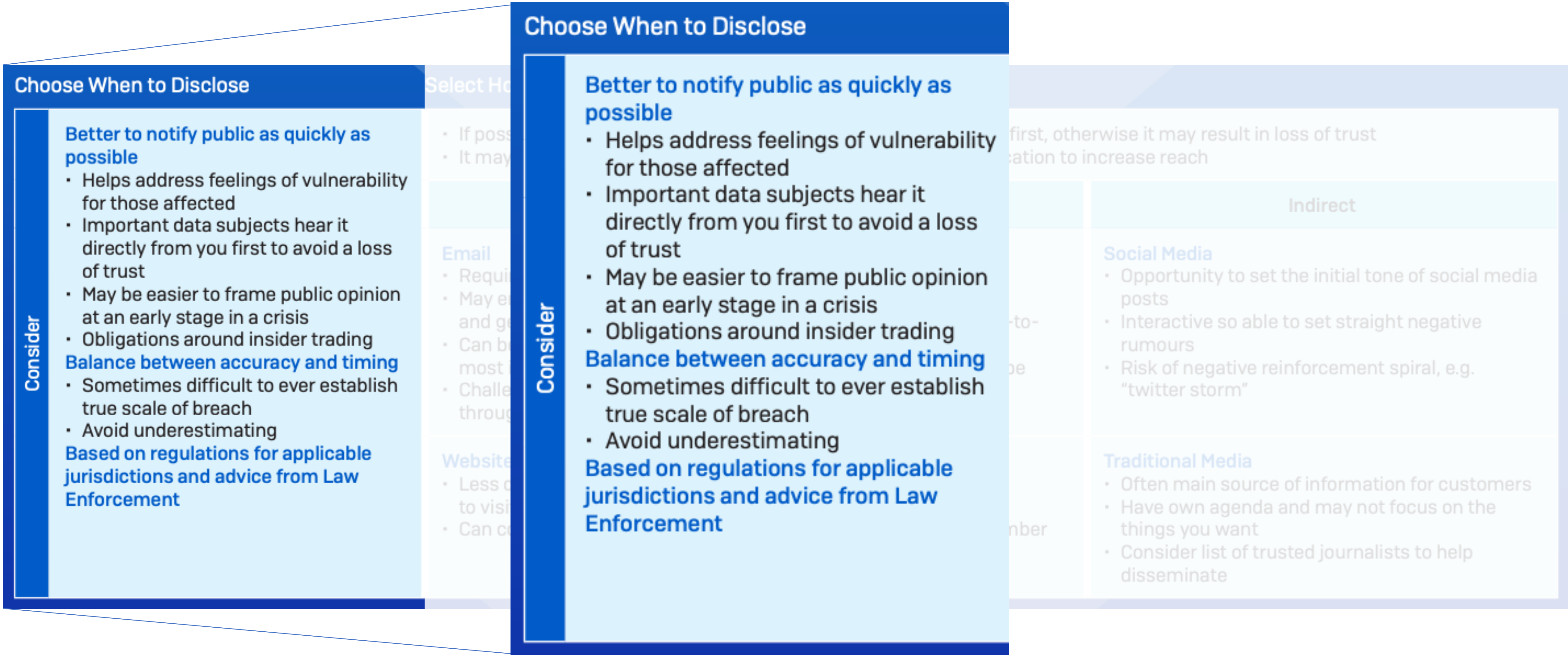
- Ethical Stance – Gender and age differences
- Younger generation may be less impressed with credit monitoring as a mitigation

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?

...

validated framework / playbook



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 Ho

- If poss
- It may

first, otherwise it may result in loss of trust

ation to increase reach

Indirect

Email

- Requi
- May e and g
- Can b most
- Challe throug

Website

- Less c to visi
- Can c

-to-

be

nber

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

Choose When to Disclose

Consider

Better to notify public as quickly as possible

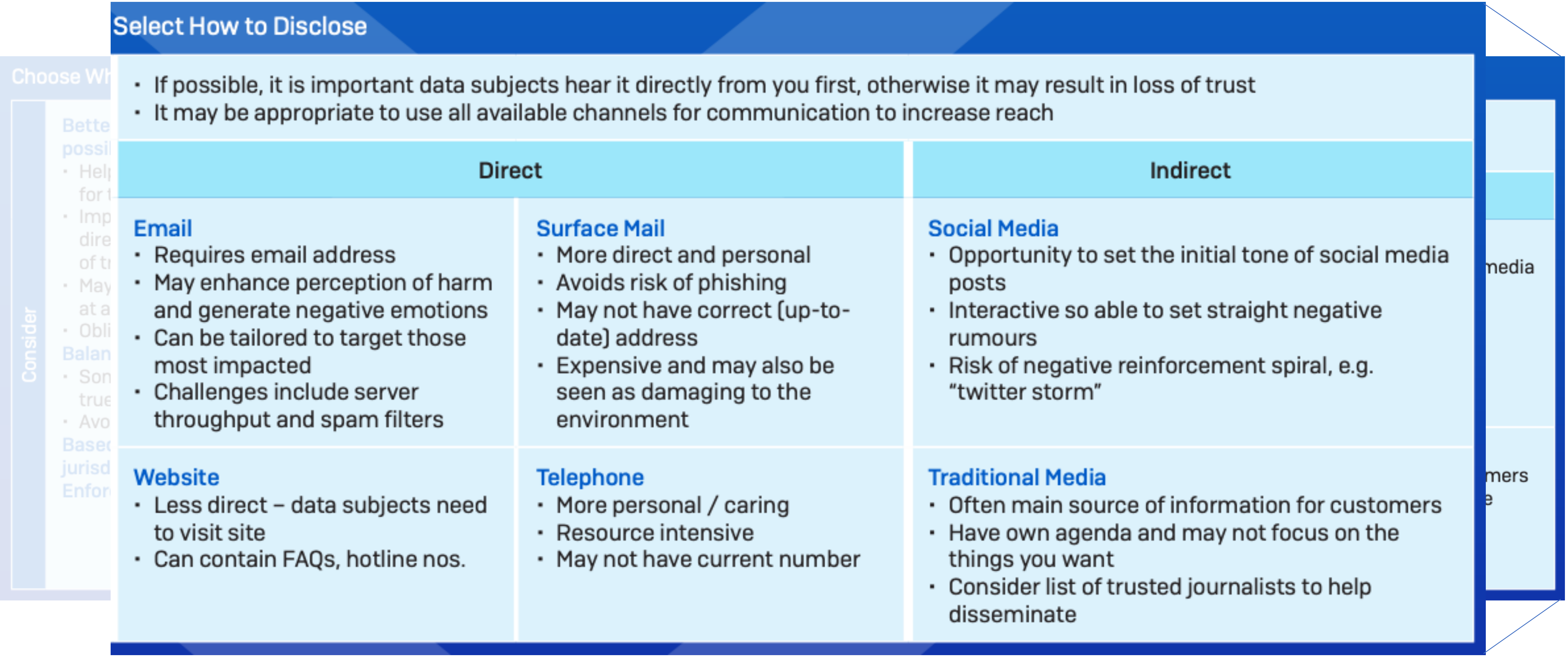
- Helps address feelings of vulnerability for those affected
- Important data subjects hear it directly from you first to avoid a loss of trust
- May be easier to frame public opinion at an early stage in a crisis
- Obligations around insider trading

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

validated framework / playbook



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

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

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

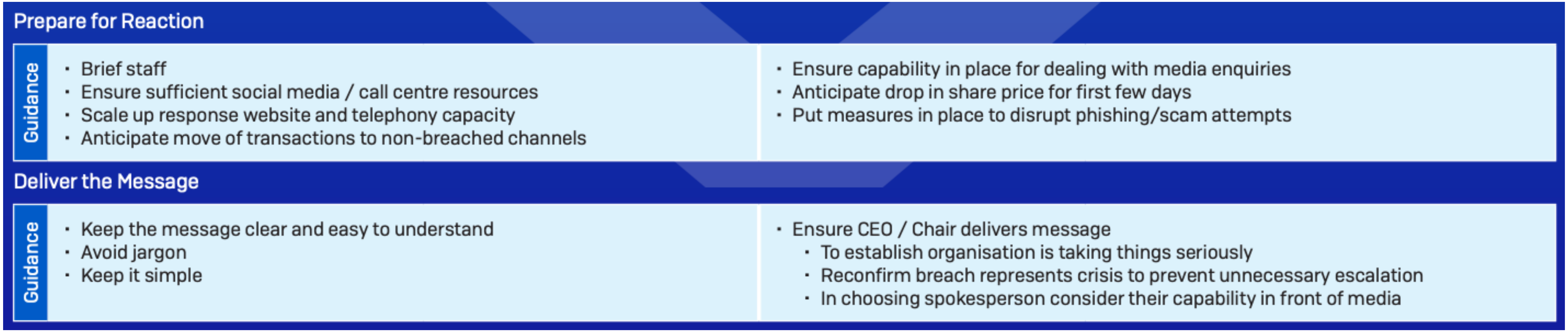
Indirect

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

validated framework / playbook

…



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

publicity / news / interests

infosecurity

STRATEGY | INSIGHT | TECHNOLOGY

Interview: Jason Nurse, University of Kent

The Register®

Wondering how to tell the world you've been hacked? Here's a handy guide from infosec academics

ucisa

Cyber Incident Communications Toolkit - Preparing for, and responding, to a cyber attack

CyberScotland

Scottish Business Resilience Centre

IEEE

United Kingdom and Ireland Section

SOPHOS EVOLVE

sasig

Any questions?

Dr Jason R.C. Nurse

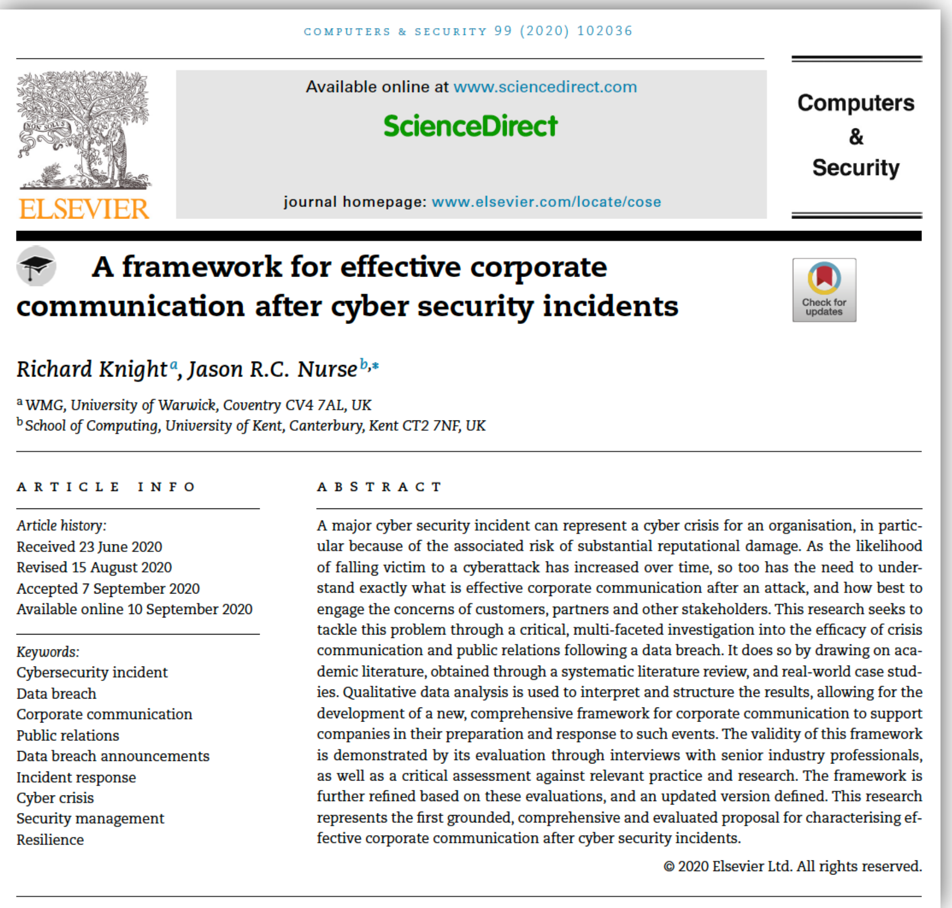
Associate Professor in Cybersecurity,
University of Kent

✉ j.r.c.nurse@kent.ac.uk

jasonnurse

jasonrcnurse

jasonnurse.github.io



COMPUTERS & SECURITY 99 (2020) 102036

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A framework for effective corporate communication after cyber security incidents

Check for updates

Richard Knight[a], Jason R.C. Nurse[b,*]

[a] WMG, University of Warwick, Coventry CV4 7AL, UK

[b] School of Computing, University of Kent, Canterbury, Kent CT2 7NF, UK

ARTICLE INFO

Article history:
Received 23 June 2020
Revised 15 August 2020
Accepted 7 September 2020
Available online 10 September 2020

Keywords:
Cybersecurity incident
Data breach
Corporate communication
Public relations
Data breach announcements
Incident response
Cyber crisis
Security management
Resilience

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.

- https://www.sciencedirect.com/science/article/pii/S0167404820303096
- https://kar.kent.ac.uk/82836/
- https://arxiv.org/abs/2009.09210