



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Communications During a Cyber Security Crisis

Leading, planning and delivering

**Hannah Kennedy-
Bardell**

Director, HKB Consulting Ltd



HANNAH KENNEDY-BARDELL
CONSULTING LTD



- I'm a Former MP but I've been a TV producer with GMTV, an Office Manager to The former First Minister of Scotland Alex Salmond, headed up Comms, Marketing and Change Management businesses in the energy Industry and worked for the US Dept of State.

- I've dealt with everything from Donald Trump and his Aberdeenshire golf course to the release of the Lockerbie bomber to a Helicopter ditching in the North Sea to the Wikileaks scandal when I worked for the US Dept of State. I saw 5 PM's, Brexit, Covid, and a fair number of political crises.

I've never - it would seem - been far from a crisis.

- I'm now putting my experience to use in;
 - Media, presentation & crisis comms training
 - Political commentary & activism
 - Public Affairs & Communications Consultancy
 - After dinner/ event speaking

I'm passionate about how we use different forms of communication, narrative and honest conversations to meet the challenges we face, change minds and make progress.



HANNAH KENNEDY-BARDELL
CONSULTING LTD

**What might a helicopter accident
in the North Sea have in common
with a cyber security attack and
comms preparedness?**



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Content Warning

My presentation will refer to accidental death and suicide.



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Sometimes life changing moments bring out the best (and worst) in people and companies. Or so I learned.

Inquiry says pilot error caused fatal Shetland helicopter crash

© 19 October 2020



| Four passengers lost their lives in the crash

An offshore helicopter crash in which four people died was caused by pilot error, an inquiry has ruled.

On Friday the 23rd August 2013 at 18.17 hours a super Puma Helicopter ditched into the sea off the coast of Shetland.

Duncan Munro, 46, from Bishop Auckland, County Durham; George Allison, 57, from Winchester, Hampshire; Sarah Darnley, 45, from Elgin, Moray; and 59-year-old Gary McCrossan, from Inverness, didn't survive.

The fatal accident inquiry held in 2020 also heard that one of the survivors, Samuel Bull, later took his own life in 2017 after suffering from post-traumatic stress disorder (PTSD).

He was 28.



What we did and how we did it

I was proud of our communications, they were (both internally and externally) clear, concise, empathetic and transparent.

We offered people support and counselling.

We recognised that the people in the company may have known, had contact with or worked with Gary.

Indeed it may have been a trigger for them or affect them personally.

What we had prepared

Media & Communications strategy

Template statements, press releases, stakeholder lists and associated content for each



Internal communications

External communications

Press & Social Media



Template graphics for social media and website



- Do the admin
- Do the strategic planning
- Don't leave yourself underprepared
- AI is your friend (most of the time!)
- Oxford Vaccine was about preparedness and knowing something was coming.

What happened next...

We went from bringing everyone together with clear, concise, well managed and empathetic communications that were person centred and open.

To.....

A crisis of communications

Why....

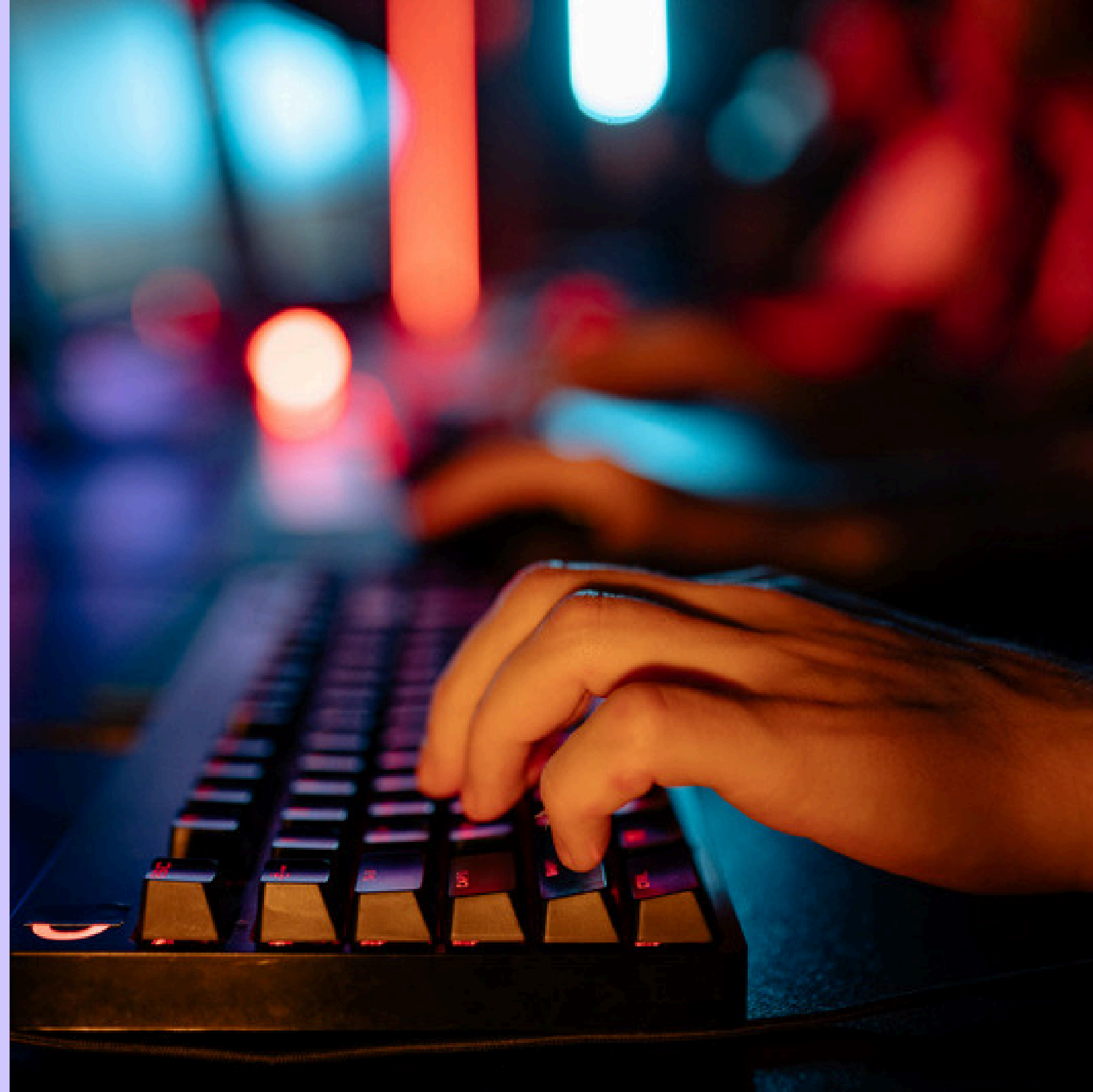
Because we had a different kind of death in the organisation.....

Suicide;



HANNAH KENNEDY-BARDELL
CONSULTING LTD

The good, the bad and the ugly of crisis communications in the face of a cyber attack.



Past learnings

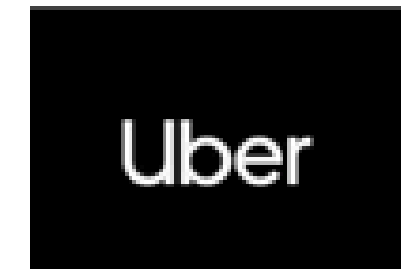
The Good

01



The Bad

02



The Ugly

03





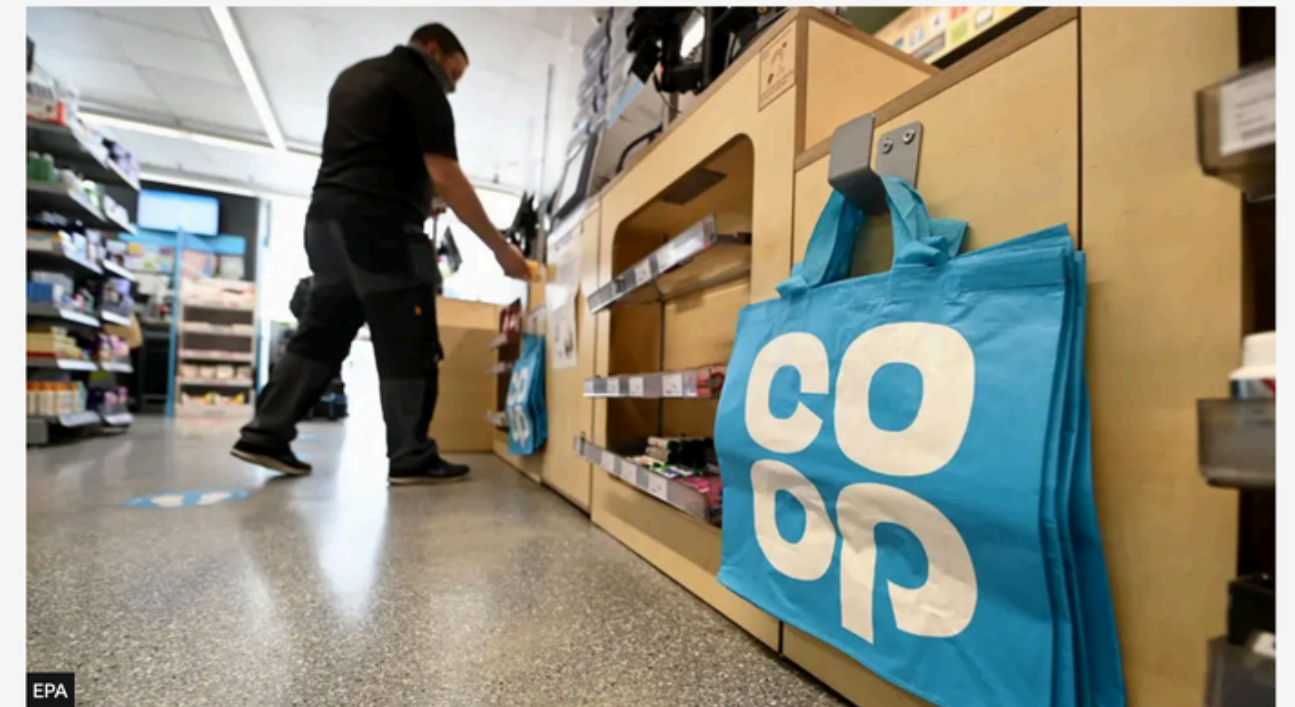
HANNAH KENNEDY-BARDELL
CONSULTING LTD

The Good

In 2025 when the Co op detected a potential ransomware attack, they "yanked their own plug," deliberately cutting their own systems to prevent data encryption and exfiltration. This proactive, self-imposed disruption created challenges in the short term but prevented and minimised long-term damage.



'They yanked their own plug': How Co-op averted an even worse cyber attack



EPA

Joe Tidy

Cyber correspondent, BBC World Service

15 May 2025

Co-op narrowly averted being locked out of its computer systems during the cyber attack that saw customer data stolen and store shelves left bare, the



HANNAH KENNEDY-BARDELL
CONSULTING LTD

The Good

In 2014, Home Depot suffered one of the largest retail data breaches in history. Attackers stole 56 million payment cards over five months.

CEO Frank Blake took immediate responsibility, apologised directly to customers, and offered free identity theft protection immediately, helping maintain customer trust despite such a major incident.



The screenshot shows a CNBC news article from September 9, 2014. The article is titled "Home Depot confirms data breach" and is categorized under "CYBERSECURITY". It includes a sub-header "Home Depot confirms data breach" and a byline "CNBC With Reuters". The main image shows a white Home Depot pickup truck parked in front of a store. The article text states: "Home-improvement retailer Home Depot officially confirmed a data breach on Monday. Home Depot's investigation is focused on transactions made as far back as April." and "There is no evidence that shoppers' debit PIN numbers were compromised, according to a statement the retailer released Monday." The page also features a "WATCH LIVESTREAM" button, a "Squawk Box" section, and a "Discover how Japan is engineering its next-gen innovation" advertisement.



HANNAH KENNEDY-BARDELL
CONSULTING LTD

In 2016 Instead of reporting a breach affecting 57 million users, Uber paid the hackers \$100,000 to delete the data and kept it quiet for over a year.

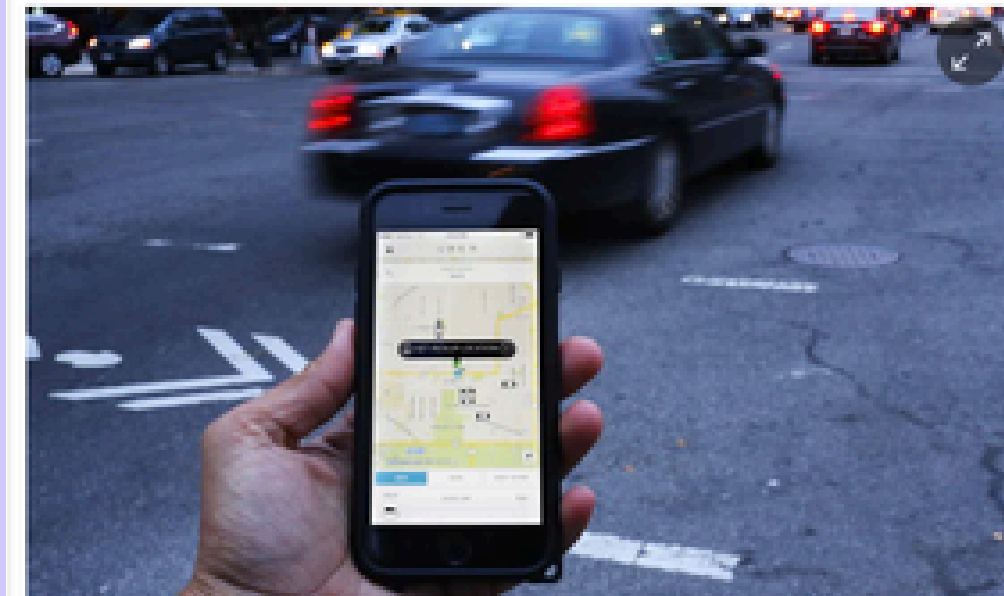
The Bad

Uber

This article is more than 8 years old

Uber concealed massive hack that exposed data of 57m users and drivers

- Firm paid hackers \$100,000 to delete data and keep breach quiet
- Chief security officer Joe Sullivan fired for concealing October 2016 breach



Uber's CEO, Dara Khosrowshahi, said: 'None of this should have happened, and I will not make excuses for it.' Photograph: Andrew Caballero-Reynolds/AFP/Getty Images

Uber concealed a massive global breach of the personal information of 57 million customers and drivers in October 2016, failing to notify the individuals and regulators, the company acknowledged on Tuesday.

Uber also confirmed it had paid the hackers responsible \$100,000 to delete the data and keep the breach quiet, which was **first reported by Bloomberg**.

"None of this should have happened, and I will not make excuses for it," Uber's chief executive, Dara Khosrowshahi, said in a **statement** acknowledging the breach and cover-up. "While I can't erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes."



HANNAH KENNEDY-BARDELL
CONSULTING LTD

The 2013-2016

Yahoo data breach is widely recognised as one of the largest and most significant cybersecurity failures in history.

Although the main breach occurred in August 2013, Yahoo did not publicly disclose the incident until years later, with full details about the extent of the breach (affecting 3 billion accounts) not revealed until 2017, resulting in a \$35 million fine and 41 class-action lawsuits.

The Ugly



Yahoo data breach payout blocked by judge

© 29 January 2019



GETTY IMAGES

The data breaches occurred at Yahoo prior to its takeover by Verizon

A judge has rejected Yahoo's attempt to draw a line under a series of breaches it experienced between 2013 and 2016.

The firm had proposed a payout to lawyers acting on behalf of affected US and Israeli users.

But while the deal said the attorneys could claim up to \$37.5m (£28.5m) in fees and costs, it did not disclose the sum reserved for victims.



HANNAH KENNEDY-BARDELL
CONSULTING LTD

The cyber-specific comms problem - Why cyber is different?

- Facts are often uncertain early
- Attackers may manipulate the narrative (leaks, extortion)
- Your normal channels might be unavailable
- National Cyber Security Centre (NCSC) advice explicitly suggests planning alternative communications if usual channels fail.



**What does
good look like
for your
business?**



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Live by the grid

Crisis Communications Planning Grid

Crisis Comms Planning Grid

Filters: Priority

Prepared Content

Key Deliverables

- Template Statements
- Press Releases
- Stakeholder Lists
- Linked Content

Channels

Stakeholders

Internal Communications

Key Deliverables

- Staff Emails
- Intranet Updates
- Internal Memos
- Internal FAQs

Channels

Employees

External Communications

Key Deliverables

- Press Statements
- Social Media Posts
- Website Updates
- Media Briefings

Channels

Press & Social Media

Graphics & Templates

Channels

- Social Media Graphics
- Website Banners
- Email Templates
- Info Sheets

Channels

Social Media Website

Status	Type	Priority	Owner	Approver	Link	Notes	Notes
<input type="radio"/> Not Started	<input type="radio"/> Status	<input type="radio"/> Priority	<input type="radio"/> Owner	<input type="radio"/> Approver	Links...		
<input type="radio"/> In Progress	<input type="radio"/>	<input type="radio"/>			Notes...		

The first message “Holding statement” done right

Structure:

- Acknowledge incident
- What you’re doing now
- What people should do (if anything)
- When next update will be
- How you can protect and support- Home Depot example



Key rule from NCSC: avoid anything you may have to retract later—especially early “no impact/no data affected” claims.



HANNAH KENNEDY-BARDELL
CONSULTING LTD

The “facts–assumptions–next update” discipline

- **Facts (confirmed)**
- **Assumptions (labelled as such)**
- **Next update time (commitment)**





HANNAH KENNEDY-BARDELL
CONSULTING LTD

The 72 Hour Timeline

The first 72 hours timeline

0–60 minutes

- Activate spokespeople + approvals lane
- Switch to alternate channels if needed (what are those channels - WhatsApp, gmail etc)

1–4 hours

- Internal staff note (what to say / not say; where to send queries)
- Start media/social monitoring to manage rumours

4–24 hours

- Customer-facing holding statement + FAQ stub (an underdeveloped support article containing little more than a title or a placeholder, often used to reserve space for future content or to mark a topic that needs expansion)
- Decide “single source of truth” page (status page / microsite)

24–72 hours

- Regulator notifications where relevant; keep comms aligned with those filings
- For personal data breaches, the Information Commissioner's Office says notify them where feasible within 72 hours when the breach is likely to risk people's rights and freedoms.
- For some UK cyber reporting regimes, government factsheets describe initial notification within 24 hours and fuller reporting within 72 hours (sector-dependent).



HANNAH KENNEDY-BARDELL
CONSULTING LTD

The practical checklist

Key Questions to ask yourself

- Where is your business continuity/ disaster recovery and comms plan held for back up?
- Do you have hard copies?
- Do you have a WhatsApp group/ Signal chat set up already?
- Are you making sure you are GDPR compliant?

- How often do you test and review the resilience of those plans?
- How often do you check and update contacts, internal, external and media, ICO, police and any key agencies you need to interact with.

- Training for staff- how often do you run that and what do you cover? Spotting threats and patterns is key.



HANNAH KENNEDY-BARDELL
CONSULTING LTD

The key principles of crisis response

01

Have the plan in place, do regular desktop exercises to keep everyone sharp.

When needed activate the plan.

02

Remain calm and open.

You can practice and pre record - watch yourself back.

03

Show empathy and communicate effectively.

Consider media and presentation training for key people.



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Designing and planning your internal Communications- Key principles

Effective comms are:

- **Clear**
- **Consistent**
- **Authoritative**
- **Accessible**
- **Timely**



This applies internally first, because staff will become your loudest channel (intentionally or not).



HANNAH KENNEDY-BARDELL
CONSULTING LTD

The Do's and Don'ts

Do

- Use one “core line” everyone can repeat (1–2 sentences)
- Label uncertainty honestly (“we’re still investigating”)
- Give staff a place to send sightings (screenshots, phishing lures, suspicious messages)
- Remind staff attackers may impersonate execs (AI voice, spoofed email)
- Consider a central team or inbox for internal concerns and reporting (almost like a first responder/first aid person)

Don't

- Say “no data affected” unless confirmed
- Share technical details that help attackers or compromise investigation
- Over-lawyer internal updates so much that people fill gaps with guesses



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Speaking and presentation techniques



Communications During a Cyber Security Crisis



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Body Language - Non-verbal communication is a vital

Professor Albert Mehrabian, a well-known psychologist and communication expert established this classic statistic for what an audience will typically remember from any communication they witness:

- **10% Content.**
- **30% Sound of the voice.**
- **60% Physical impression.**

Great content is vital BUT We remember far more when there are no physical distractions, 'irritants', taking our minds off the content.

Using and Interpreting Non-Verbal Communication is key;

Audiences will always reflect what it sees - if you look nervous or anxious, very quickly we as an audience will as well. **There has to be a congruence between what you're saying and how you're delivering it.**

A good strong neutral position is:

- Feet hip-width apart facing slightly out – not pigeon toed or splayed.
- Weight evenly distributed between the two feet and standing to your full height, square on to your audience.

Just not this tho... PLEASE!





HANNAH KENNEDY-BARDELL
CONSULTING LTD

- An appropriate degree of **animation in the face** is perfectly acceptable - and encouraged - we've all seen politicians with fake smiles....
- **Use your hands** naturally and go in for direct eye contact when you can - to emphasize your points as this will help give emphasis and gravitas.
- Look out for and **Identify habits** (fidgeting, repetitive terms, annoying phrases etc.) (*hand wringing, so basically...*) repeated word use etc. Film yourself (painful I know!)
- **Find a comfortable hand position** - so that when not using them, just have them resting in front of the body. **No hands in pockets.**
- **Connect** with your audience (The Kennedy Sweep).
- Remember any **movement should ideally be specific** as too much aimless flailing can distract and dilute your message.
- Aim for 70% professional energy- **try to get the rise and fall-** not monotone and use breath pauses for emphasis.
- Breathe, relax and enjoy! **Use the breath pause where you can** - and practice!



JFK was famous for
'sweeping the room.'
Taking a pause, looking
right across the room and
making people feel like he
was speaking directly to
them individually.



HANNAH KENNEDY-BARDELL
CONSULTING LTD

**Observation
exercise- what
do you notice
about this
broadcast?**

<https://www.youtube.com/watch?v=fP5R4xZVvDg>

How did he break it all down and make it digestible?



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Gravitas

Caroline Goyder

Knowledge+ Purpose + Passion (- anxiety) = Gravitas



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Useful resources

<https://www.ncsc.gov.uk/guidance/effective-communications-in-a-cyber-incident>



HANNAH KENNEDY-BARDELL
CONSULTING LTD

Thank you!
h_k_bconsulting@outlook.com

