CRISIS COMMUNICATION TRAINING

Cyber Breach Simulation

Practical, Real-World Training for Cyber Resilience

STEARNS IMPACT

Who We Are

Ed Stearns and Lorraine Fletcher are award-winning crisis communications specialists with frontline experience in some of the UK's most high-profile incidents.





Following the Paris terrorist attacks, we led the review and rewrite of the Metropolitan Police's major incident communications plan, with a focus on social and digital media. This plan was rigorously tested across multiple organisations and successfully deployed during subsequent terrorism incidents. It became a gold standard model for first responders worldwide, winning multiple awards including PR Week and Corporate Comms (2017).

Since then, we've advised on major incidents across the private and public sectors — from sports and entertainment venues to the fire service and government — bringing calm, clarity, and strategy to moments of extreme pressure.

Why Train For A Cyber Attack ... and Why Focus on Communication?

Cyber attacks are rising in both frequency and sophistication. High-profile cases have shown how quickly they can cripple even the most established organisations. The risk is no longer theoretical — it's a matter of when, not if.

When a cyber crisis hits, multiple teams are pulled into action:

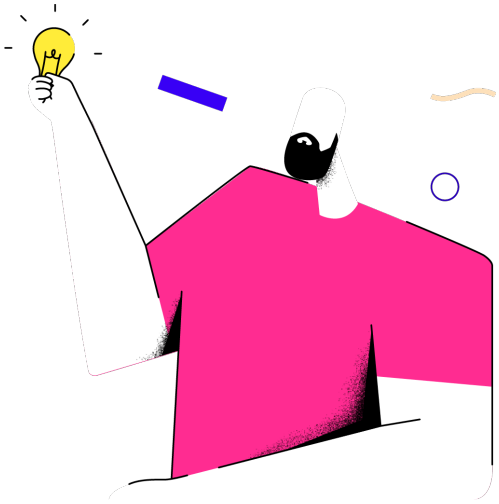
- **IT** – contain the breach, restore systems, and safeguard operations
- **Security** – manage threats and respond to extortion attempts
- **HR** – address staff impact and data compromise
- **Customer Service** – maintain business continuity
- **Executives** – protect stability, reputation, and future

At the centre of all these moving parts is one critical function that binds them together: communication. Clear, timely, and credible communication enables coordination across departments, maintains trust, demonstrates competence under pressure, and protects reputation.



Cyber Breach Simulation

Practical, Real-World Training for Cyber Resilience



Why Our Training Stands Out

- Fully customised scenarios
- Real-world insight
- Strategic feedback
- Transparent pricing

What The Training Looks Like

1. **Pre-Training** – discovery, scenario design, pre-event briefing
2. **Training Day** – interactive scenario, injects, media tasks, role challenges, recovery/trust rebuilding, strategic implications
3. **Post-Training** – written report with readiness assessment

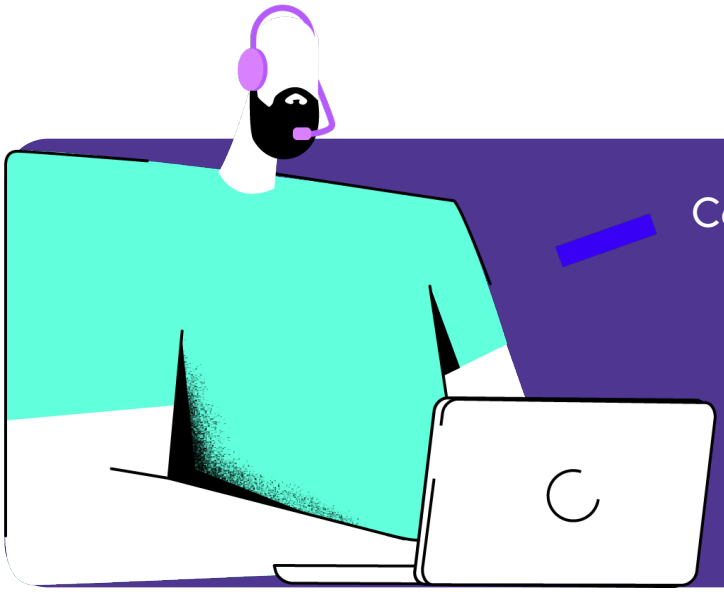
The Outcome

By the end of the exercise, your teams will:

- Understand dynamics of fast-moving cyber crises
- Coordinate clear, consistent, timely communications
- Know internal roles between comms, IT, security, execs
- Protect reputation and maintain trust under pressure

Your organisation will:

- Update crisis plans based on outcomes
- Better understand responsibilities and skills gaps
- Be more resilient and customer-focused if the worst happens
- Understand how the organisation can be protected by first class communication



Contact us or a free consultation on your readiness for a cyber crisis:

ed@stearnsimpact.com

+44 (0)7939 188889

www.stearnsimpact.com