

FLEISHMANHILLARD

CYBER SECURITY AND CRISIS COMMUNICATIONS

August 2021

CYBER SECURITY IS EVERYONE'S PROBLEM

Data breaches and cyberattacks are a fact of life for organisations today and sadly, it's largely not a case of 'if' but 'when'. With the huge increase in ransomware attacks globally, the operational and reputational challenges facing organisations today have arguably never been greater.

While threat actors continue to evolve their tactics, with an increasing focus on causing reputational damage, it's critical that businesses must evolve their approach to crisis comms to enable them to respond effectively should they find themselves on the receiving end of a ransom request one day.





OUR PERSPECTIVE ON CYBER SECURITY

Cyber security must no longer be viewed as the job of IT and risk departments

Planning across the business is crucial to establish processes and ensure an integrated response

Business must anticipate initial discovery coming from outside and be ready to move quickly in response

More unknowns than knowns – businesses often have to communicate publicly long before investigations conclude. Think ahead and anticipate where the story could go to avoid creating issues further down the line

All employees have a responsibility – businesses need to better educate on how they can help protect customer and business information

Line up external resources in advance and ensure a one team approach



OUR PERSPECTIVE ON RANSOMWARE

Reputational Priorities

Stakeholders need to see you as a credible source of information. Clear, consistent and accurate information is vital. Do not engage in speculation of any sort

To pay or not to pay

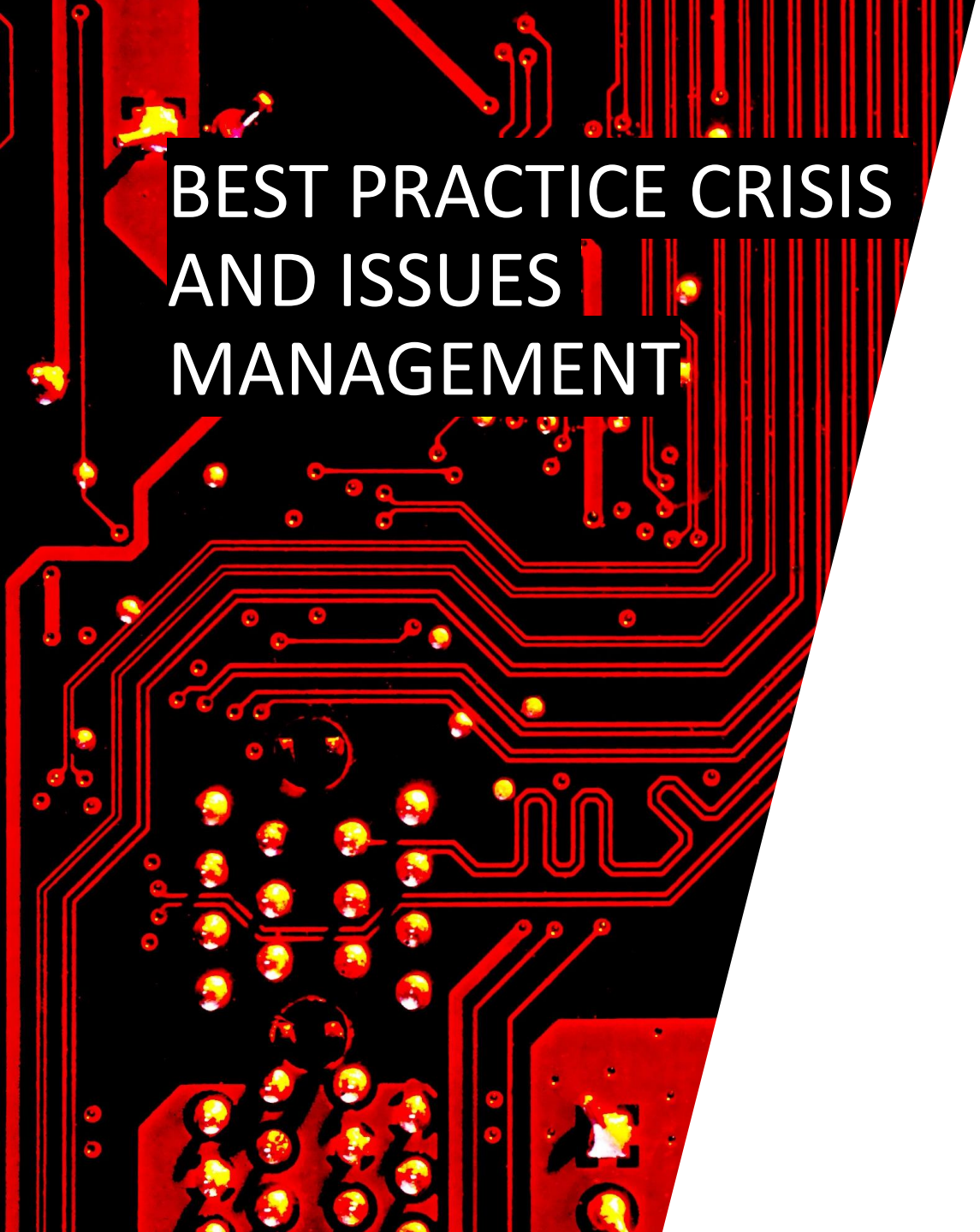
Often the starting point is ‘we don’t pay’ — either from a legal stance, ethical perspective, a technical point of view or a mix of all three. However, sticking to that line can be a challenge when critical operations are taken offline and sensitive or personal data is risk. Companies should get ahead of these decisions via crisis scenario exercises.

Control the narrative

Part of communications planning should include a timeline of when to deploy certain messages to specific audiences.. It is imperative not to speculate or contribute to a narrative you do not control. Focus communication on transparency and avoid over-communicating when you have nothing new to share.

Call the Experts

Decisions and communication at the early stages of an attack can have significant implications further down the line. It is critical for clients to engage the necessary players from the outset - forensic IT, legal counsel and corporate communications — to potentially limit reputational and commercial impact in the long term.



BEST PRACTICE CRISIS AND ISSUES MANAGEMENT

FleishmanHillard UK is part of FleishmanHillard (FH) which is a global integrated communications company. We have offered our clients best practice crisis and issues management services since our agency was established in 1946 because, fundamentally, these areas have always been at the heart of managing a company's public reputation.

Our commitment to best practice is reflected in our unique crisis counsellor certification process – which we believe is the first programme of its kind. It ensures our global network of strategic counsellors is certified in the firm's proprietary A.R.C.™ methodology. To date, more than 150 counsellors have been A.R.C.™ Crisis Certified.

Although our core skills relate specifically to crisis communications, we also have a deeply held knowledge and understanding of the world of cyber security and the associated risks. In the last eight years alone, our teams have helped hundreds of clients globally manage and prepare for cyber incidents.



YOUR GLOBAL CYBER COMMS PARTNER

FH is one of the only global communications agencies to have a dedicated cyber security practice. Led out of the US with regional leads across the globe, this function centralises and cements our cyber expertise and means we have a wide range of experience relating to cyberattacks, data loss and leaks.

Whatever the brief, we come at it with an integrated mindset: from media relations to digital and social, employee and customer engagement to investor communications.

We are the global crisis communications partner for a number of the world's largest insurers and claims management specialists. Working alongside forensic IT and legal counsel, we have helped businesses – included listed companies – and other organisations prepare for and handle data breaches, including ransomware incidents.


OUR EXPERIENCE

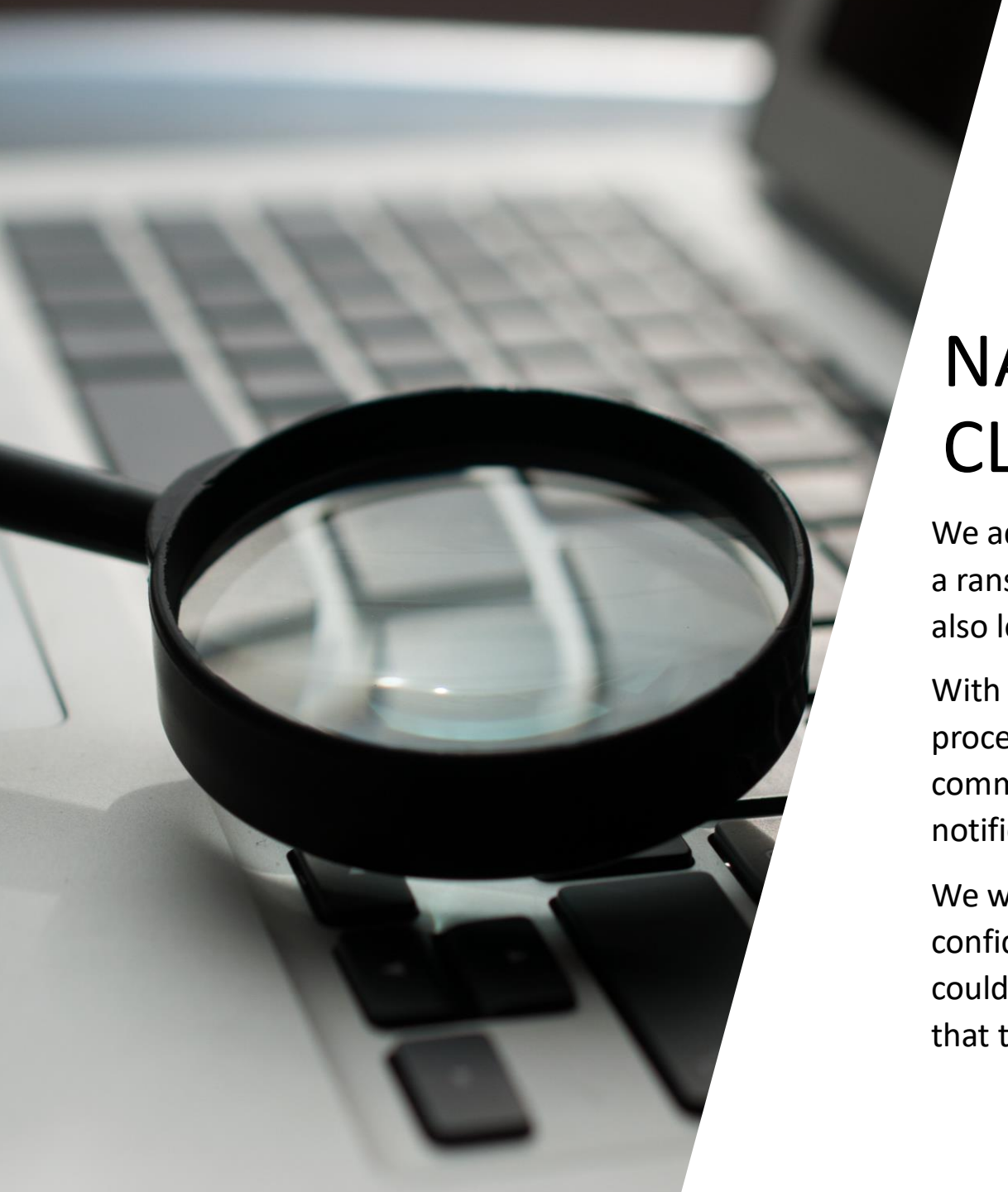


MANGING A COMPLEX STAKEHOLDER SET

When a global insurance business found itself on the receiving end of a ransom note, we were activated to advise on the comms response. Working into the Board, we drove the comms strategy and plan, as well as developed all the messaging and assets.

With an extremely complex stakeholder universe, the business faced significant pressures – from brokers to customers – and it was critical that the comms response took into account the individual needs without over-promising or over-stating the situation whilst the forensic investigation was progressing.

Throughout the incident, relationships were effectively managed with regular updates to stakeholders to reassure that the business was managing the situation as a priority and all necessary steps were being taken.

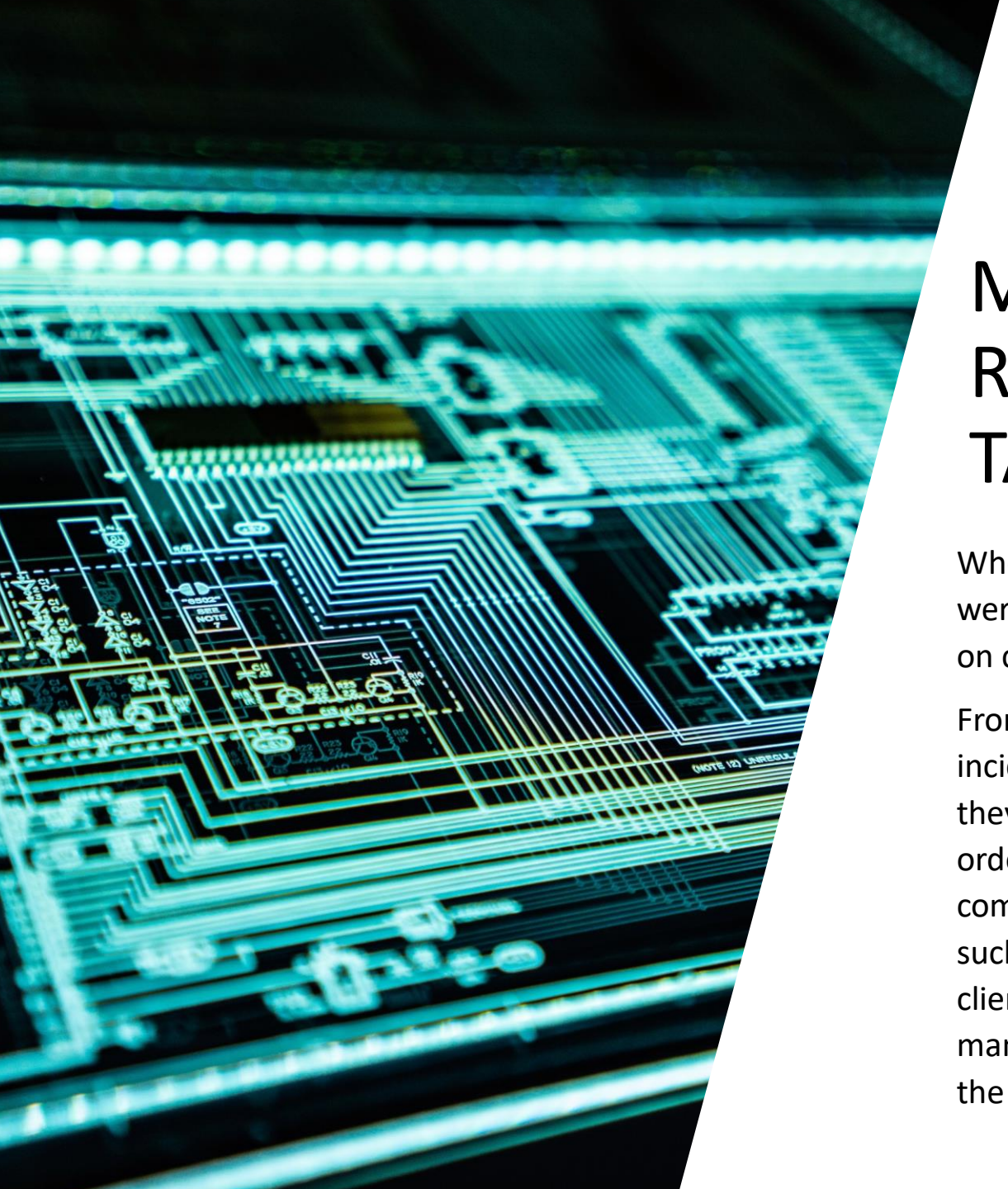


NAVIGATING A COMPLEX CLIENT UNIVERSE

We advised the market office of a global consultancy who had suffered a ransomware incident, leading to significant operational disruption. It also left the business facing a challenging data exfiltration situation.

With a complex landscape –the consultancy having both controller and processor status and a large number of high profile clients – we led the communications response from the start of the incident through to notification.

We worked closely with legal and forensics throughout to ensure client confidence was maintained – whilst there were many questions we couldn't answer at the start, it was critical that the clients understood that the consultancy was effectively managing the situation.



MANAGING COMMS IN RESPONSE TO THREAT ACTOR TACTICS

When a financial services company suffered a ransomware incident, we were responsible for driving the communication's response, with a focus on clients and employees.

From intelligence, we understood that the threat actor behind the incident had previously contacted employees and clients from companies they had breached, making claims about data they had exfiltrated in order to increase pressure. Recognising this as a possible scenario our company could face, we ensured that they were prepared to handle any such moves. Weeks later the threat actor did contact employee and clients but our preparation ensured the company was able to calmly manage the situation. The incident closed with positive feedback from the company's clients on how the business had managed the response.



SUPPORTING EDUCATION INSTITUTIONS

We have supported dozens of schools plus further and higher education institutions through ransomware attacks, at a time when the sector has been targeted by threat actor groups.

Disruption to learning centres can be extremely concerning for those involved and require quick, effective communications to offer reassurance and provide information.

Education institutions often have a complex stakeholder group (ranging from students to government to private and commercial delivery partners), and can attract interest from media.

We have led the strategy development and execution of these responses from initial disruption through to notification and final communications. We ensure that our full response strategy delivered consistent messaging at all times and effectively protects the reputation of the centre.



COACHING A HIGH PROFILE FASHION BRAND

When a fashion brand loved by celebrities and royals suffered a card skimming attack, we activated on a Saturday evening, had a communications strategy in place within hours and supported with daily calls throughout the process.

The royal and celebrity link meant media interest was inevitable, but we successfully managed this dynamic, with all coverage on message, on brand and informative for any customers who may have been impacted by the incident.

Working closely with legal ,we navigated around numerous risks of litigation.

Finally, difficult customer complaints were managed effectively and in keeping with the brands tone of voice.


HOW WE CAN HELP

HOW WE CAN HELP

PLANNING AND PREPARATION

- Crisis playbook including ransomware playbook
- Communications risk assessment
- Establishing monitoring systems
- Data breach response planning
  - Team/roles
  - Process/protocols
  - Resources/systems
- Action plan mapping
- Template communications
- Media training
- Cyber event response drills

INCIDENT RESPONSE

- Rapid response team support
  - Comms strategy and counsel
  - Message and FAQ development
  - Notification planning/writing
  - Media relations counsel
  - Online resource development
- Communications action plan
  - Development/activation
- Real time media/social monitoring
- Spokesperson preparation

REPUTATION RECOVERY

- After-action comms reports and plan adjustment
- Reputation audit and repair plan
  - Monitoring and response
  - Stakeholder relations
  - Ongoing customer security and recovery communications
- Litigation communications



OUR CYBER COMMS SPECIALISTS



judith.moore@fleishman.com

+44 (0)20 8618 2979

+44 (0)7860 607 696

JUDITH MOORE

SENIOR PARTNER AND EMEA CRISIS LEAD

Judith has more than 20 years of experience in communications, working both agency and client side. In issues and crisis, Judith has worked with a broad range of corporate clients across sectors including FMCG, food and drink, aviation and leisure.

At FleishmanHillard, Judith manages the agency's global relationships with insurer and claims management companies in respect of breach response and in this roles, is responsible for co-ordination of response across multiple markets.

Judith has led a large number of breach incident responses, including advising a well-known airline who was breached by a highly sophisticated source. A particular focus for Judith over the last 18-months, has been advising clients on the communications response following a ransomware incident. Judith has advised across business and organisations of varying sizes and sectors including professional and financial services, manufacturing, education, legal and consumer goods.

In addition, she also works closely on the planning and preparation side, and has been part of a number of crisis simulations at Board level.



hannah.cambridge@fleishman.com

+44 (0)7976 927 467

HANNAH CAMBRIDGE

DIRECTOR

Hannah is an A.R.C.™ accredited crisis counsellor and has extensive experience in crisis and issues communications, working to protect brand reputation in the face of some of the most challenging threats.

Hannah's academic background in the Law makes her adept when working at the intersection of communications and legal process or government scrutiny, and an ideal partner for a multifunctional response team. She provides pragmatic counsel, with a solutions focussed approach that will address both the immediate and longer term challenges.

As the UK continues to see an increase in ransomware incidents, Hannah has led the communications response for many impacted organisations, including those with extremely complex and sensitive stakeholder relationships.

Away from ransomware, Hannah continues to work on one of the UK's most high profile cyber incidents and has led the communications around many broader malware, spyware and data breach incidents.

Beyond cyber response Hannah works on matters such as workplace culture issues and employment disputes, fatalities, Public Inquest, Public Inquiry, litigation, business restructure and closure and white collar crime.

Previous client experience includes, Tata Consultancy Services, Manchester Arena, Sodexo, Samsung, Swissport, SC Johnson as well as many retailers, professional services brands and educational institutions.



nic.daley@fleishman.com

+44 (0)7979 851132

NIC DALEY

DIRECTOR

Nic has advised many global, US and UK (FTSE-listed) organisations on issues and crisis communications including Associated British Foods, Compass Group, GSK, Huawei, Intel, LG, P&G, Spotify, Shell, and WWF (Worldwide fund for Nature).

He has extensive experience of cyber security-related crises, including cyber attacks, nation state threat actor intrusion, data breaches, high-profile and multi-million pound ransomware and extortion demands. He has led the communications response to cyber incidents in a range of sectors including healthcare, education, technology, finance, law, aviation, consumer goods, and more.

More broadly, Nic has led crisis response on a variety of issues including: product recalls, redundancy and restructuring, industrial disputes, emergency response incidents, brand attacks by news media/environmental campaigns, and several high-profile court cases.

Nic has experience of working with multinationals, SMEs, and charities, as part of short-term crisis activations, on-the-ground response or as part of client-side communications teams – seeking to manage the initial issue or incident and restore and manage long-term brand reputation. A former news journalist, he also runs crisis preparedness training and crisis simulations.



cody.want@fhflondon.co.uk

CODY WANT

ASSOCIATE DIRECTOR

Cody has over seven years' experience working in crisis and issues communications, helping organisations maximise their influence and protect their reputation in a wide range of challenging scenarios. He has guided clients through undercover media investigations, cyber breaches, major restructures and union disputes and many other regulatory and reputational challenges.

As a media-trained spokesperson, on-call crisis press officer and trained speechwriter his approach focusses on developing robust messaging strategies to navigate complex, contentious issues under heavy national media scrutiny.

He has worked with clients including Facebook, Swissport, Google, BBC TV Licensing and a large agro-chemical company on internal, external and multi-market issues. Cody joined FleishmanHillard from Markettiers, an international broadcast- public relations specialist, where he secured regular national and international coverage for clients.



juliette.monnet@fhflondon.co.uk

+44 (0) 208 6181 710

+44 (0) 7510 153 737

JULIETTE MONNET

ACCOUNT DIRECTOR

Juliette delivers crisis and issues management for organisations across a number of sectors, from food & drink, to education and healthcare. She is a core member of the Ferrero press office team, where she advises the company on how to manage a number of issues, including announcing retail closures, defining their position on plastic packaging, and responding to a petition from a European campaign organisation on their supply chain.

She also leads the crisis account for Alliance Medical, where she helps the business navigate sensationalist headlines when production issues result in cancer patients having their appointments cancelled.

On top of her retained accounts, Juliette works closely with FleishmanHillard's legal and insurance partners offering crisis counsel on a broad range of issues, from cyber security incidents to police investigations and health and safety court hearings.

WHAT CLIENTS SAY ABOUT OUR WORK

We really appreciate everything that you have done to support us during this difficult time and couldn't have done it without you."

CEO, household name jewelry brand who experienced a data breach

Your experience in ransomware came across and was of reassurance.
It was very telling that while the business has their own PR people, the experience of FHF shone through in a non- confrontational way.
Thank you for your excellent work.

Insurer partner

The Insured is quite happy with the services provided and said they wished they had notified Insurers sooner as the support received was very helpful in managing the incident.

Feedback from a cyber insurance firm on our work supporting a leading academic institution that suffered a ransomware attack. Fleishman Hillard assisted the Insured within the tight deadlines for ICO notification and the short notice of schools being reopened and eased a lot of the Insured's concerns around both of these.

The crisis communications support that FleishmanHillard gave to us throughout our cyber incident response was exceptional. They quickly jumped in to support our communications team, offering specialist and strategic advice. This was an integral part of our response as they were able to develop messaging and help us understand the sequence of events that would therefore impact our approach to communications. They were a huge support to our team, always available to offer advice and guidance, and we are very grateful that we were able to work with them.

Communications Manager, Education Institution

It was a genuine pleasure to work with you and your team in a crisis – we really benefitted from your calm and certain demeanour.

Director of Communications, Global Insurance Company who experienced a ransomware attack

During a period of uncertainty, I greatly valued the counsel FHF provided as well as the hands on support. Across several months, FHF worked as an essential and trusted part of our crisis team, providing advice and guidance every step of the way. I believe the counsel they provided helped us to manage the incident really effectively, reassure our various stakeholders and protect our reputation. Throughout the entire process I had a personal sense of reassurance that we were in safe hands.

CEO, UK membership organisation

THE FLEISHMAN HILLARD NETWORK

Founded
1946

2,600+
employees worldwide

85+ OFFICES
in more than 30 countries

150+
crisis counsellors





GET IN TOUCH

24/7 CRISIS LINE:

+44 (0)208 618 1736

crisisuk@fleishman.com