BABEL TaylorWessing

PROTECTING BRAND REPUTATION AND STAKEHOLDER **ENGAGEMENT DURING A CYBER CRISIS**

A debrief of the Churchill War Rooms workshop with Babel PR and Taylor Wessing

2024

INTRO

Just like the digital world has become an intrinsic part of daily life, the possibility of cyber-attacks and data breaches has become a daily part of modern business. The security sector has been rapidly growing since its inception, but in the current environment, it's evolved from not only dealing with the constant threat of cybercrime but also having robust plans to respond to the nearly inevitable event of a breach. Recent findings from the UK government stated that 11% of businesses had experienced cybercrime in the last 12 months, rising to 26% of medium companies and 37% of large (enterprise) businesses.

Today, cyber-attacks represent a new battle frontier that businesses must prepare for. You can't just protect and prevent any more. You need to expect and plan for the worst. As the industry adjusts to this new reality, where some successful attacks are inevitable, modern security posture focuses more on dealing with, mitigating, and recovering from attacks. Prevention is still crucial, but incident response and recovery are becoming non-negotiables.

THE EXPERTS

Jenny Mowat,
Managing Director of Babel PR

Michael Yates,
Partner and co-lead of UK Cyber at Taylor Wessing

Responding to a cyberattack or data breach is a multi-dimensional undertaking. Beyond the operational or IT concerns, businesses need to understand how to respond and communicate to stakeholders, customers and the media in the wake of an incident. The good news is that in this day and age, headline-making incidents are all too common. Such events are not an automatic death knell for a brand's reputation, but how a brand communicates and responds with all stakeholders after such an event can make or break public perception.

To analyse and break down the importance of this, as well as workshop potential scenarios and how best to respond, Babel, alongside global law firm Taylor Wessing, ran an exclusive event. In the heart of the historic Churchill War Rooms, teams of PR specialists, legal specialists and communication leads of significant brands took part in an exercise to see how they would respond and react following a significant cyber event. The event also featured two current journalists to get the perspective of both national and trade media on how businesses should (and shouldn't) engage with journalists before, during and after a cyberattack.

Nick Huber - Freelance Cyber Security Journalist at the BBC, Financial Times, and The Guardian

Beth Maundrill - Editor at Infosecurity Magazine

THE NEED FOR EFFECTIVE CRISIS COMMS

Despite being more common than ever, cyber-attacks and data breaches can still significantly affect a brand's bottom line. According to IBM, the average data breach in 2023 cost $4.45 million. Despite this staggering number, the full impact of such events can be hard to quantify. Reputational damage can rear its head in many ways. Customer, partner or even employee relations can all be put under strain alongside tumbling share prices, legal consequences and negative media attention. These things can be mitigated or made far worse based on how a brand handles its communications amid the crisis.

In light of this, the need for a brand to manage the situation with various stakeholders is critical. For example, maintaining open and transparent lines of communication with regulators, clients, and the media can be vital. This helps contain the immediate fallout and rebuild trust in the long term. Similarly, addressing the concerns of the market and supply chain can mitigate business disruptions. Transparent communications with shareholders and partners can also help manage financial repercussions. Ultimately, handling these relationships - and taking specialist advice from your PR and legal support - in the aftermath of a cyber event goes a long way to preserving a brand's reputation in the eyes of all stakeholders.

For example, in 2023, Capita was hit by the Black Basta ransomware group, exposing the data of around 90 organisations. The attack reportedly cost Capita up to £25M and saw share prices fall 12%. An official statement by Capita admitted "disruption" to several clients but reassured that most client services were unaffected. The statement also claimed the incident was isolated and (incorrectly) stated that there was "no evidence that customer data has been compromised".

However, the media insisted that the attack was "far worse than reported". This significantly increased concerns over clients' leaked information, including the Ministry of Defence and other government bodies. As evidence of stolen Capita data – including school job applications, passport scans, Capita nuclear bank transfers, and architectural diagrams – began to surface, public trust in Captia plummeted.

For a more positive example of response to a cyber incident, the NGO International Committee of the Red Cross (ICRC) was hit with an attack in late 2021. The attackers accessed a database that contained names, addresses, and contact information for 515,000 people separated from their families by war and natural disasters. The Red Cross posted a detailed description of the hack and a lengthy Q&A to the public.

A statement from Robert Mardini, ICRC's director-general, pleaded with the hackers not to use the information as the attack is an "affront to humanity" and spoke directly to affected victims, saying, "We want you to know we are doing everything we can." Their admirable efforts to contact affected people included sending teams to remote communities to inform people in person.

MANAGING A CYBER CRISIS

To demonstrate the array of comms decisions and potential consequences that businesses can face in the aftermath of a cyber incident, we challenged our attendees to put their crisis management skills to the test. Four crisis-response teams competed to see how to manage an evolving cyber crisis and the fallout it can bring across stakeholders, including partners, the media, shareholders, clients, regulators and even law enforcement. Below is a summary of the key takeaways and considerations that came up during the exercise:

RESPONSE

In the wake of a cyberattack, immediate action involves a balance of rapid information gathering and cautious communication. IT and corporate communications teams face the challenge of understanding the scope of the breach—identifying affected systems, understanding how the breach occurred, and determining the extent of data compromised. Amidst this, speculation is common, but decisions should be based on verified information, not early theories. Compliance with notification requirements under data protection laws and regulations is critical. This means (often alongside legal counsel) reviewing regulatory requirements and agreements that mandate breach disclosure.

COMMUNICATION

Deciding when to communicate with customers is also a delicate balance. Silence or delayed communication risks eroding trust and could result in reputational damage, especially if the media gets ahead of the story. Yet, the nature of the communication—whether to reassure or to be transparent about the uncertainties—requires careful consideration. Our teams aimed for a balanced approach, tailoring messages based on the audience and legal considerations and striving for consistency across all channels to avoid speculation and misinformation.

As news of the cyberattack spreads, interactions with the media become inevitable. This is often where companies misstep. For example, overly defensive strategies or aggressive litigation threats against misinformation can backfire. Instead, working closely with PR specialists to craft a measured response ensures stakeholders are informed and any inaccuracies in reporting are corrected quickly

RECOVERY

Post-incident, the journey towards reputation recovery continues. This can include navigating regulatory intervention or investigation, to dealing with potential claims from affected parties. Expert advice from PR and legal specialists on communication strategies to legal responses is essential.

The discussion demonstrated the vast decision tree for managing reputations with shareholders, employees, customers, suppliers, partners and the media. There was a healthy degree of debate within and between our four teams, showing that there is no easy decision or one correct answer in many cases. Appropriate action depends on the situation's specifics, any legal or contractual obligations that might be in play, and the business's priorities. Ultimately, having a well-defined team for handling such situations is the best way to be prepared to weather the storm.

THE MEDIA PERSPECTIVE

While communications during a cyber crisis need to include and account for all relevant stakeholders, one party requires a dedicated approach - the media. Naturally, trade and national journalists hold a tremendous amount of sway, especially when it comes to newsworthy cyberattacks. If, when and how media reports on a cyber event greatly influence public, partner and customer perception. Managing the media during such an event requires skilled spokespeople, consistent and clear messaging and, ideally, existing relationships with journalists.

Building the latter is a longer-term project, however. This is where a proactive PR strategy to generate positive media coverage year-round can pay dividends during a crisis. Journalists may come directly to you for comments or to check facts. So, with this in mind, media engagement must be a priority at all times, not just during a crisis.

Nick Huber
Freelance Cyber Security Journalist at the BBC, Financial Times, and The Guardian

Beth Maundrill
Editor at Infosecurity Magazine

BBC

FINANCIAL TIMES

The Guardian

Infosecurity

RESPONDING TO A BREACH IN THE MEDIA

So, what advice did our journalists, Beth Maundrill, Editor at Infosecurity Magazine, and Nick Huber, Freelance Cyber Security Journalist for the BBC, Financial Times, and The Guardian, have for companies engaging with the media during a cyber crisis? Beth suggested looking at specialist security companies that have suffered a breach themselves for examples of best practices.

For example, LastPass suffered a major incident at the end of 2022 involving the breach of customer data and LastPass's internal systems. In response, LastPass issued several updates as the situation unfolded, giving a full breakdown of what happened. Its report included what happened, what data was accessed, what actions LastPass had taken, advice and guidance and what customers needed to do to protect themselves. Beyond this, our journalists outlined three things to bear in mind.

Be accurate

Don't share information or updates that aren't true, including unintentionally. If you are not entirely sure of the facts, sharing details with the media that could later be found to be untrue can damage your reputation more than not saying anything.

Add value

When you respond, you need to say something - don't just make empty statements. Tell the media and, by extension, the public what's happened, how you're dealing with the issue, and who's affected. Nick advised brands to 'give the impression you've got it covered' and suggested doing so was far better than not doing anything: 'Silence tells its own story."

Don't panic

Finally, our journalists advised that while organisations should take these events seriously, they shouldn't panic. In the modern environment, most large organisations will have some kind of breach. Nick argued that it's not the 'badge of shame' that it was a decade ago. So, respond swiftly and concisely, but don't panic and send the wrong information or message.

PROACTIVELY ENGAGING WITH MEDIA

While during a cyber crisis, the goal is often to minimise media coverage as much as possible, when it's business-as-usual media coverage is crucial for building brand awareness and building a voice in a market that stands out from competitors. We asked our guest journalists what they're looking for from businesses during the day to day news cycle and how best to secure coverage in trade and national media.

When engaging with the media year-round, it's crucial to be aware of the current stories and broader trends being covered across the industry.

When asked about some of the critical cybersecurity trends they are likely to cover more of in 2024, our journalists pointed to:

- Artificial intelligence
- Increasing law enforcement takedowns of cybergangs
- The ongoing ransomware pandemic.

Above all, however, journalists covering cyber are looking for the same things as journalists in any other sector: stories. They need the 'so what?' that captures attention and moves the conversation forward. New angles, perspectives, and updates are critical.

Knowing your audience is vital when distributing reactive commentary on a cyber incident. Journalists like Nick and Beth write for national and trade media for different audiences and are looking for different things. With trade media covering the industry for the industry, you can afford to get more technical, but with nationals, it's better to keep it high-level and tailored to a general audience.

Either way, journalists receive such a high volume of comments about attacks that statements and spokespeople must have something to add to the conversation. Make sure your comments add value and move the conversation forward. Provide context (what's happened), expertise (what does it mean), and a healthy pinch of opinion (what's likely to happen next?)

In addition, while most subject matter experts will have excellent knowledge of what they're talking about, that's not enough. The key is to communicate clearly and explain complex stuff easily in simple terms—this is particularly important for national publications.

Losing the jargon and providing relevant examples, anecdotes, or even metaphors can help spokespeople come across well and stick in the mind.

CONCLUSION

Suffering a cyber attack or data breach is not part of any business's best-laid plans. Unfortunately, such events are almost inevitable for large organisations in the current environment. As such, comms teams must be prepared to manage such situations and protect brand reputation in the eyes of customers, partners, and the media. Managing the latter is pivotal. Without a well-informed strategy to manage the media during a crisis (from both a messaging and legal perspective), brands can quickly lose control of the narrative or do more harm than good by making the wrong decisions or communicating the wrong message.

Thank you to those who attended, our fantastic guest journalists and Taylor Wessing for helping us make the event such a success. Contact us today if you'd like to learn more about how Babel can support you with media relations during a crisis and year-round.

BABEL TaylorWessing

ABOUT BABEL

Headquartered in London and with affliates across the globe, Babel is a technology PR and integrated communications agency. Babel works with established global brands, market challengers and emerging disruptors.

Clients rave about our ability to understand their business, bring strategic insights and deliver amazing results that transform their companies and personal reputations. They come to us because they know they will gain access to some of the smartest communications strategists and implementers in the business.

It's why our clients consistently rank us highly in terms of overall agency satisfaction, why staff give us high job satisfaction scores, and why journalists, analysts and other influencers are happy to speak to us.

For more information, visit:
www.babelpr.com

- UNDERSTAND
- CREATE
- DELIVER

BABEL TaylorWessing

UNDERSTAND
CREATE
DELIVER

www.babelpr.com
enquiries@babelpr.com
+44 (0)20 7434 5550

2024