BABEL

Cybersecurity: Creating meaningful commentary in an industry full of **FUD**

June 2020

FOREWORD

Cybersecurity, by its nature, deals with the remediation of the nasty side of our digital lives and businesses. However, if you pick up any newspaper or publication reporting on the sector, you'll find the tone of the commentary is often based on fear and scaremongering. This approach of fear, uncertainty and doubt (or FUD, as it's affectionately called) is starting to wear thin, and doesn't paint a realistic picture of the things (if anything) that should be keeping businesses and citizens up at night.

We wanted to get to the heart of what is driving fear, uncertainty and doubt in the cybersecurity media landscape. Why has this become the default mode for narratives that both journalists report on and many vendors want to convey? Is there something more impactful and constructive that security vendors can be offering to journalists in terms of stories? What do journalists actually want to hear? And what do their readers care about?

To answer these questions, we spoke to a selection of experts in the cybersecurity industry and the media prolific in this sector. Our aim? To demystify FUD and provide businesses working in cybersecurity with constructive feedback– straight from the horse's mouth – on how to cut through a media landscape that has been stirring the 'FUD pot' for some time.

In the pages that follow, you'll hear the thoughts and opinions of communications experts who have built their careers on providing impactful, meaningful and relevant cybersecurity stories to journalists. You'll also hear from a selection of top tier security and technology publications which are on the receiving end of a barrage of pitches competing for column inches – what makes a good story? And what sort of pitch goes straight in the virtual bin?

To the reader – we hope you find the report useful in helping you to create more structure, relevance and punch in your current communications campaigns, without resorting to FUD. And thank you to all those who provided input into this report; your time and insights are hugely appreciated.

If you have any further thoughts or insights to share on this topic upon reading this report, please do get it touch. We'd love to hear them!

Jenny Mowat, Managing Director, Babel

"The cloud of FUD hangs heavy over cybersecurity." These are the words of Infosecurity Editor Dan Raywood, one of a number of influencers and cybersecurity firms Babel interviewed for this report. Our goal? To better understand how the media and the market create, respond to, report on, monetise, and mitigate fear, uncertainty and doubt (FUD). Rather than just holding a reflective lens to the situation, we sought to identify the most effective, authentic and accurate way of telling cybersecurity stories.

By identifying what's not working today (and as it turned out, hasn't been working for years), businesses can transform their approach to PR and communications strategies for tomorrow. And Babel, as a PR agency specialising in technology – and whose broad portfolio of clients includes a number in the cybersecurity sector – can bridge the gap between what your business wants to say and what the media wants to hear. But first: why cybersecurity?

THE RHETORIC OF DREAD

A brief skim through the morning's papers/scroll through the daily digital news agenda will reveal that in every industry, global conversation is dominated by FUD. The rhetoric of dread is what covets clicks, titillates readers and sells stories. However, in other sectors there arguably exists more of a balance between feel-good stories and doom and gloom. This has been highlighted recently, as the dominance of FUD in national media – due to COVID-19-related stories – has proven to be untenable, as ad revenues dry up due to brands' reluctance to advertise next to negative stories. Advertisers are even reportedly using 'blacklist' technologies to block digital ads running next to stories featuring words like 'attack' and 'death'.

Cybersecurity, on the other hand, is an industry seemingly driven by FUD. Trade publications, business press and national media are full of stories that push a narrative of constant threat: that hacks are inevitable, that businesses are always at risk, and that every individual can be victim. And feeding them these stories are PR agencies and cybersecurity businesses. It's not surprising: FUD is a major money-spinner. Invoke fear among business leaders and CTOs and suddenly every and any cybersecurity technology is a crucial must-have. Stoke anguish among managers and HR and suddenly every cybersecurity training course is a critical must-do.

Cybersecurity, by its very nature, deals with the remediation of the nasty side of our digital lives and businesses. In this respect, FUD is both accurate and, to some extent, necessary. But how much does the dominance of FUD really reflect reality? Who is pushing this agenda, and possibly pushing it too far? And has FUD fatigue created an opportunity for a new type of storytelling and news reporting?

FUD: THE FRENZY AND THE REALITY

To determine a new and better way of telling cybersecurity stories, it's important to identify what's wrong with the current narrative and where accurate reporting of data breaches, hacks and the like strays into melodramatic FUD territory. Who better to grill on the nature of FUD in cybersecurity media than cybersecurity media influencers?

One of the topics that is spoken about/reported on with an over-emphasis on FUD, according to Gareth Corfield, a reporter at The Register, is the number of attacks organisations have fallen victim to over a certain time period. "This feeds into shit PR with FUDtastic subject lines such as 'X million businesses were cyber-attacked last year'," said Corfield. What's more, the prevailing mood of FUD too often means the use of 'attack' turns into abuse of the term. "The term 'attack' in an infosec context is meaningless these days; I've seen it being used to convey everything from 'hackers accessed customer credit card details' to 'someone port-scanned our web server'," he said. "We all know volume attacks are largely automated probing that may or may not be followed up by human operators. Tell us something unique."

Even companies operating in the cybersecurity sector acknowledge the disproportionate level of FUD.

Data breaches can be "sensationalised", commented the PR Director of a cybersecurity research and educational institute, "especially in cases such as ransomware hitting hospitals, or nation state hacks – or else, those which are reported to be nation state hacks. The temptation is to find some evidence that these are targeted attacks rather than simply widespread attacks of which hospitals and other key institutions have fallen foul." She continued, "There is often a focus on China or Iran or Russia being the villain of the piece. Whilst this 'may' be true, I think some spokespeople may be tempted to speculate when the full facts are not clear, and of course this kind of attribution is often likely to get coverage."

This was corroborated by another industry insider – a PR Manager for a cybersecurity solutions vendor – who said that nation state attacks, and particularly the use of Advanced Persistent Threats (APTs), are too often reported with an over-emphasis on FUD. "Media will jump on any commentary that claims nation states have used APTs or zero-days to attack organisations, often with little, if any, evidence," she explained. "Even the FBI has dismissed this as nonsense, yet it still gets media whipped up into a frenzy."

> *"Instead of reporting on the less-than-glamorous reality, the media resort to telling exciting tales that they think readers want to hear.*

WHO'S DRIVING THE NEWS AGENDA?

It's easy to point the finger at the media as the main driver of FUD. After all, villainous nation states, mega corporations playing fast and loose with our data, and sky-high data points all make for highly-shareable content. Consumers want their contacts to be aware of the dangers, while businesses want to expose the shortcomings of their competitors. The idea that bad news sells was supported in a global study published in the Proceedings of the National Academy of Science in 2019. The study concluded that, on average – and based on responses from people from a huge range of cultures and countries – people pay more attention to negative news than to positive news.

This point was highlighted by the PR Director of a cybersecurity research and educational institute. This is perhaps due to "journalists being asked to report on a story [who] are not always specialist or experienced in security, or are being directed to write a story in a particular (more sensational) way to fit with a publication's style of reporting and audience," she said. "They may also not be as well connected with spokespeople/organisations who will give a non-FUD view and may therefore connect with organisations that will give a more FUD view in order to get coverage."

The Register's Corfield agreed, commenting that, "There's certainly no appetite among The Register's readers for FUD (debunking FUD: completely different topic!), though I can see how it plays well in the Daily Mirror or the Independent when they're looking for clickbait churn to keep the news treadmill turning. If you're in the B2C market maybe that's a good strategy for you, but in B2B trade press we're just laughing at it."

A second PR Manager surveyed by Babel agreed, saying "It's a combination of media desire that is fuelled by their audience looking for 'exciting news'. For years cybercriminals/hacking was almost a dark art, with few really understanding what was going on – it's the stuff of Hollywood movies!". Popularised by the likes of The Net (for the '90s kids) and Mr.Robot (more recently), the idea of hackers as shady characters has helped to construct a narrative of 'us versus them', which works well for screenplays, but less so for accurate news reportage.

The result is that, instead of reporting on the less-than-glamorous reality, the media resort to telling exciting tales that they think readers want to hear – and which no doubt many do. "When a company suffers a cyber-attack/data breach, it's far more convenient to say that there was nothing they could do, as it was a nation-state sponsored attack, rather than the truth - they left a Windows server unpatched," continued the same PR Manager. "The result is that media allude to Russian/China backed gang activity and more fuel is added to the fire."

THREE SIDES TO EVERY STORY

There is always more than one side to every story. And there are multiple facets in the media/PR/cybersecurity industry relationship – a relationship that influences which stories get reported on and which fall by the wayside. The over-emphasis on FUD is not driven solely by over-zealous media. Instead, said Corfield, the tone is usually set by communication from "spray-and-pray PR spammers I've never heard of before or since."

Of course, the FUD story wouldn't be complete without that third and final facet: the tech industry itself. Create fear, stoke it, respond to every breaking cybersecurity story (however significant or realistic the danger) with your brand's messaging, and sit back while business leaders lap up your solutions and your training expertise. It's a shrewd business move, and one that seems to be paying off.

As such, cybersecurity businesses themselves have a role to play in changing the conversation and reducing FUD in the industry. They should, commented Corfield, "Stop presenting the world as a raging inferno of howlingly insecure threats to everyone, that only your business can solve." He continued, "The world doesn't work like that. Most good companies have two or three infosec vendors' products in use across their IT estate and the good infosec firms acknowledge that. Consistently telling us that everything is dangerously insecure unless you, the White Knight, are paid to ride in to the rescue merely breeds resignation and fatigue ("screw them, they're always saying that, it's just the boy who cries wolf")."

According to the 2019 Cyber Readiness report from insurance provider Hiscox, the average spend on cybersecurity now stands at $1.45 million and the pace of spending is accelerating. The total spent by the 5,400 firms included in the company's report comes to $7.9 billion, and two-thirds of respondents plan to increase their spending by 5% or more in the year following its release.

2019 CYBERSECURITY SPENT

$1.45m	$7.9b
AVERAGE	TOTAL

PLAYING ALONG NICELY

FUD seems to be pretty entrenched in cybersecurity, with each faction – the media, PR and vendors – all shrugging their shoulders and shifting the blame. This situation mirrors that of the FUD narrative, with lots of finger pointing, too little collaboration and not enough solutions. All parties have a part to play in creating accurate narratives that convey brands' messaging, and PR has a role to play in these with journalists in the most effective format. Finally, the journalists themselves have a responsibility to select FUD-minimising stories that give accurate insight into the threat landscape.

Businesses should work to ensure they're "better at communicating challenges" and present their technology as "one tool (rather than a total solution)," said Infosecurity's Raywood. "Better collaboration amongst communities to drive better standards," is also required, alongside an "effort by the media to play down unnecessary hype."

In short, everyone needs to "all play along nicely!".

Corfield's sentiment was similar. "More building of quality professional relationships between journalists and PRs," is needed to address the dominating FUD narrative. Some PRs would also benefit from "self-education", particularly around their use of data to drive stories. "Aggregated numbers do not usually tell a useful story unless properly categorised and there is a big difference between a large-scale intrusion from (say) a Chinese APT against a Western aerospace company and some skiddie repeatedly port-scanning a bank," said Corfield. "Similarly, it's useless knowing that there were X million 'attacks' against a given company or sector unless you break that down by type of attack (apparent origin, type, vector, payload, whatever), so we can see where the underlying threat actually is. A hundred exploits of recently-announced CVEs is of far more news and public value than a million spam emails."

EDUCATION FOR ALL

The need for greater education doesn't only apply to the PR industry – the media, too, could benefit from a deeper understanding of the cybersecurity space. "In the mainstream media, I guess the only way [to address the FUD conversation] would be to ensure that only experienced security journalists are writing cyber security stories, and that headlines and content do not get skewed by editors and subs once the journalist has filed a story," the PR Director of a cybersecurity research and educational institute. "This is the case with so many areas of life however, and not just security."

In many cases this'll be easier said than done. The decline in print media consumption, an abundance of fake news, and our growing reliance on social media commentary from non-press parties have had a huge impact on the media industry. Editorial teams are dwindling, and the number of technology specialists is falling. Between 2008 and 2017, the number of newsroom jobs in US newspapers dropped by 45%, to 39,000, and all US newsroom jobs, including TV and radio, declined by 23% overall. The situation is more dire at present; according to the Press Gazette, 2,000 staff across the UK's national and regional press have temporarily lost their jobs as a result of the coronavirus outbreak.

Clearly, the onus cannot be on journalists alone to change their ways and address FUD. In fact, the majority are already doing as much as they can to report as accurately as they can. "Generally speaking, I think

the UK tech and security press are fairly balanced in their reporting of cyber security issues these days," said the PR Director of a cybersecurity research and educational institute. "Now a relatively mature discipline, there is so much competition to provide stories and comment that I think there is no temptation to include stories that maybe don't 'check out' as well as the reporter might like, and those who have been in the industry for some years have seen many of the same issues and topics crop up again and again. Certainly, I would say that seasoned tech journalists are usually pretty sceptical about any potential FUD stories that may be circulating and are well connected with experts in the industry to verify data."

Given the FUD fatigue and irritation felt by the media, as well as an abundance of scare stories dominating the media at present (due to COVID-19, this is pretty difficult to escape!), there's a real opportunity now to shake up the agenda and re-think cyber communications strategies. As intermediaries between cybersecurity companies and the media, this is where the actions of PRs really matter.

THE ROLE OF PR & COMMUNICATIONS

PRs can be educators, reacting to breaking news stories with solutions rather than stoking the flames of the FUD fire, as well as developing their clients' messaging in a way that's more educational and less dramatic.

We spoke to the Head of Corporate Campaigns at one of the world's largest cybersecurity solutions providers, who commented: "I don't think consumers really know about everything that happens beneath the surface and it's our job as a communications team to help educate them about the potential and real risks." There's a real opportunity here for businesses in the sector to stop pushing scare stories and instead to offer advice and education. "More brands need to be offering guidance - especially on their owned channels - and getting this to translate into media coverage," she continued. "PR teams need to ensure they work their media relations harder to ensure educational commentary is positioned more positively."

The PR Director of a cybersecurity research and educational institute says she too would "love to see more of a focus [in the media] on the basic steps that both individuals and organisations should have in place with regard to security and still so often don't." So why aren't we seeing this kind of educational angle to stories? According to her, focussing on the reality of cybersecurity stories (i.e. "that a lot of the breaches and hacks we see are still due to poor basic hygiene rather than some new clever attack"), simply "doesn't make great news."

However, it's here that we arguably return to the finger-pointing game, in which the three players – the cybersecurity industry, the media, and the PR sector – think the other is to 'blame' for FUD overload. The idea that the above stories don't make great news is not in fact supported by our discussions with journalists. Instead of overblown stories blaming consumers and businesses for hacks and breaches, Corfield wants to see PR and the tech industry "broadcasting simple and effective messaging such as 'use a password manager, enable 2FA, remember to log out on work devices after checking the account'. Or whatever. FUD makes end-users switch off and ignore infosec advice completely, and they're the people this industry is supposedly trying to protect."

SOLUTIONS & CREATIVE CONTENT

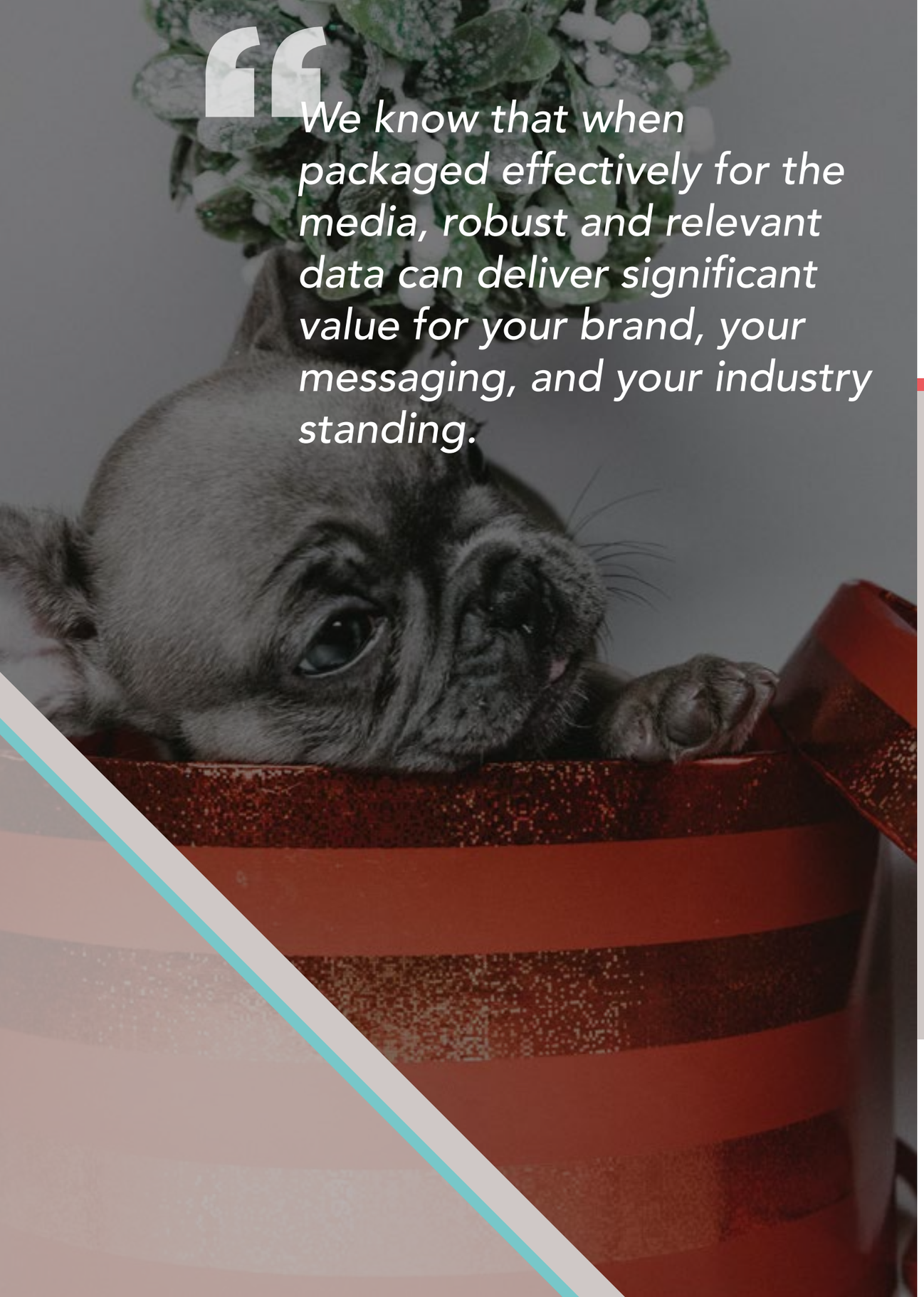
Note the importance of education and advice as solutions here – not just the solutions (i.e. products and pieces of kit) themselves. No one buys technology, they buy a solution to a challenge. This mantra governs our approach to creating a wide variety of content and PR and marketing services at Babel; We deliver a complete communications service for technology brands, which is focused on an individual client's organisational KPIs and translating these into business impact. We interpret the complexities of technology into stories, and then create content that engages with the right audiences, enabling our clients to achieve their end goals.

Finally, while educational messaging is one step towards minimising FUD, the way these messages are conveyed and the relationship between media and PR remain crucial. As our PR Director of a cybersecurity research and educational institute says, the difficulty many companies face is, firstly, telling stories "in a creative eye-catching way" and secondly, "working with industry to get this message very clearly across to audiences." It may be a challenge, but it's one that must be overcome if a business wants to engage effectively with influencers – because creativity is exactly what the media want! Evidence of this is Corfield's response.

When we asked The Register journalist what businesses could do to best support a change in conversation, Corfield advised: "Be creative, be a bit more upbeat, don't be afraid to say 'yeah, actually things are improving and the world's getting better' once in a while."

TOP TIPS

1. Educate your audience on the potential and real risks, but avoid hyperbole
2. Focus on solutions, not the nitty gritty of technology to deliver a business proposition
3. Provide simple, but effective tips or guides to demonstrate solutions in action
4. Step outside of the FUD and say something positive and constructive to move the conversation forward
5. Work with the media to learn what they need to build a clearer story for their audience



We know that when packaged effectively for the media, robust and relevant data can deliver significant value for your brand, your messaging, and your industry standing.

BIG DATA'S HUGE VALUE

Instead of going for shock value and click-bait, provide advice on cybersecurity best practice and establish your brand as a thought leader via other means of story-telling. One of these other means involves data. Babel has extensive experience in working with brands to obtain new data via market research, or to help identify where data may already exist (but is sitting unused) within an organisation. This approach is well-received by the media; Corfield, for instance, advises: "Start talking more about interesting findings from your threat intel team, or a way of approaching a persistent infosec problem that's paying good dividends for your company or team. Dare I say it, maybe even your core product does a good job that you can back up with appropriate use of stats."

CASE STUDY

THE CHALLENGE

Twice a year, NETSCOUT launches its global Threat Intelligence Report which explores cyber risks to both organisations and nations. Babel was asked to cut through the noise of the media landscape and position NETSCOUT as an authority, driving awareness of its cloud-ready cyber security solutions and its acquisition of DDoS specialist, Arbor Networks.

THE SOLUTION

Babel developed a visibility programme, leading a campaign that was executed across three creative media pitches: smart device security, DDoS attacks on vertical industries (e.g. travel) and state-sponsored cyber attacks.

THE OUTCOME

Highly targeted and bespoke outreach to UK, US, France and German business press which led to media coverage in over one hundred publications including Forbes, The Washington Post, BBC Radio Four and AFP, and fed into social media channels. In turn, this drove website registrations and report downloads. Additionally, the campaign content was used to hijack a breaking news story on the Iranian hackers who targeted key UK infrastructure, highlighting NETSCOUT's integrated DDoS capabilities and cyber security expertise.

Babel's work with clients across the technology industry shows that the right PR partner can help any company generate real value from data. We understand the importance of maximising the value and longevity of data: instead of solely focussing on quick wins, we develop strategies that fuel sustainable, long-term visibility among both target media and target customer markets. We know that when packaged effectively for the media, robust and relevant data can deliver significant value for your brand, your messaging, and your industry standing.

‘MORE MATURE, LESS AGGRESSIVE’

When asked what could be done differently to lessen the dominance of FUD, Infosecurity Editor Raywood said that, “A more mature and less aggressive sales and PR strategy employed by businesses would be welcomed” – for many journalists this is likely an understatement!

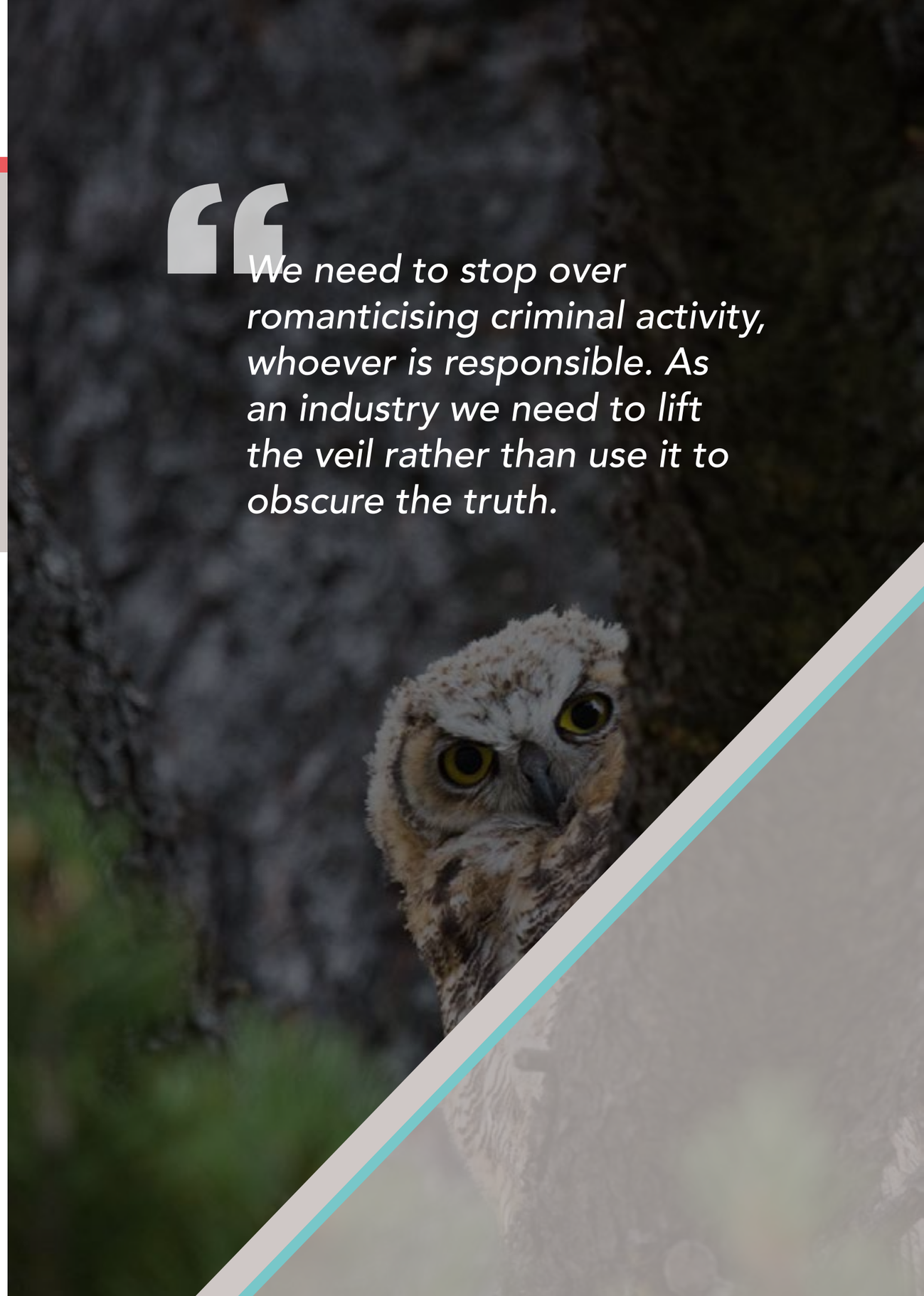
We also offer a number of services to help ensure brands’ stories are heard by the right people – and that the right people can then tell the right stories to their readers.

These services include roundtable events, which involve a number of clients and influencers discussing an industry topic, providing media attendees with a well-rounded and multi-angled perspective. Whilst in the past these have involved dinner events, we’ve reworked the concept for a new virtual-first age – with the hope of resuming in-person roundtables in the not-too-distant future.

TACKLING FUD: A COLLECTIVE RESPONSIBILITY

Approaches such as these, combined with accurate, responsible storytelling and news reporting will help to address and overcome the enduring issue of FUD in the cybersecurity industry. However, it’s not going to disappear overnight. While readers still succumb to sensationalist fodder, FUD is never going to go away entirely. Furthermore, just as creating FUD is a collective responsibility, reducing FUD is also a collective responsibility: companies, PRs and media must work closely together to ensure effective content creation and accurate reporting. One PR Manager we spoke to summed it up perfectly when she said that, “We need to stop over romanticising criminal activity, whoever is responsible. As an industry we need to lift the veil rather than use it to obscure the truth.”

Babel is playing its part in helping to lift that veil. We employ a mixture of approaches to help to bridge between what the client wants to say and what the media wants to hear.



GET IN TOUCH:
https://babelpr.com/contact/
+44 (0)20 7434 5550
newbusiness@babelpr.com