BABEL

A year of COVID-19 and its impact on the cybersecurity threat landscape

March 2021

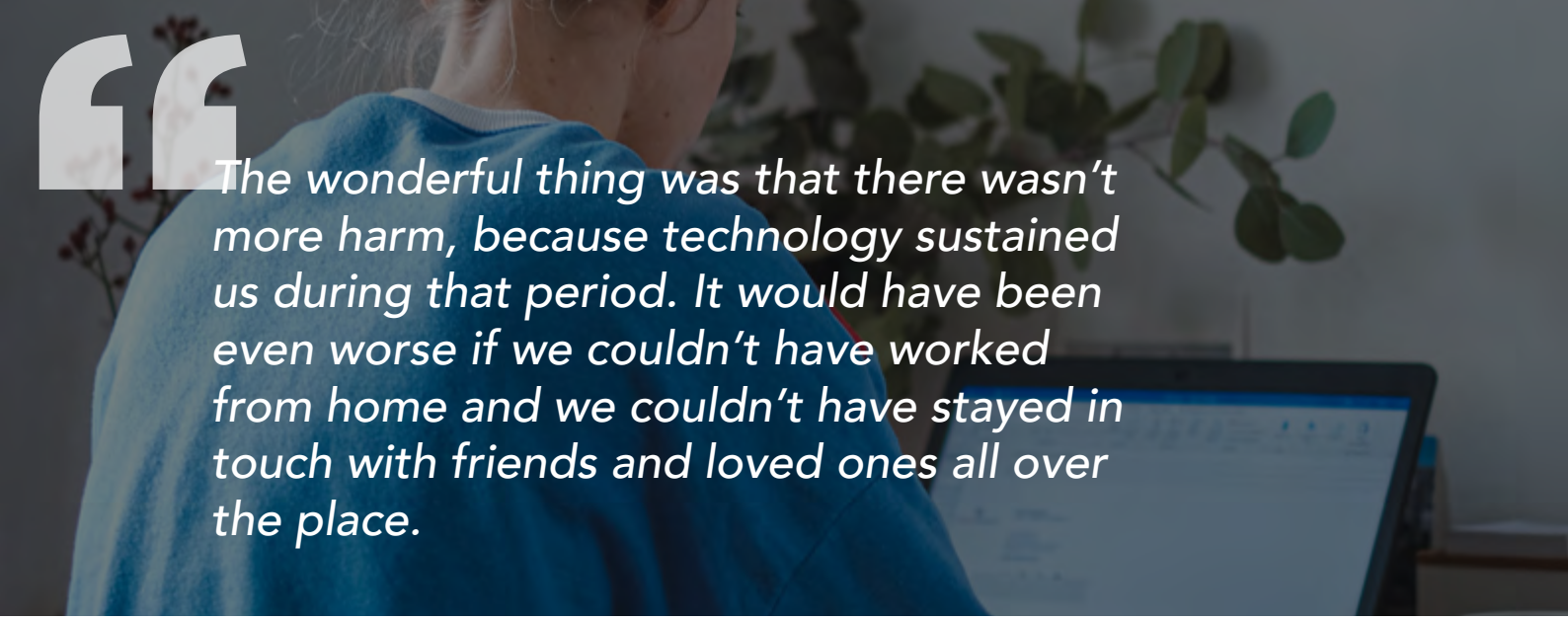
FOREWORD

11th March 2021 marked one year since the WHO declared COVID-19 a global pandemic. Since then, many of us have shifted to remote working, relying on a combination of work laptops, video calling, personal mobile phones, one-time codes, Google docs, SMS authentications and a list of passwords as long and complex as the government's changing lockdown rule book. This created a unique opportunity for cybercriminals. Now, ransom demands have become so routine that many go under the radar, unwitting consumers continue to divulge sensitive data to criminal gangs, and the game of cyber cat-and-mouse between the East and West plays on.

How has the pandemic influenced the nature of the cybersecurity threats that individuals and organisations face? How have these been covered by trade and business press? What insight do journalists need from cybersecurity firms to help explain evolving threats? And what can brands do to ensure that these insights make the pages of their target publications?

These were among the questions explored at a recent live-streamed #BabelTalks event. Hosted by Babel's Simon Coughlin, our panel included Nicole Perlroth, cybersecurity reporter, New York Times, and Professor Ciaran Martin, CB, founding chief executive of the National Cyber Security Centre (NCSC), and currently Professor of practice in the management of public organisations at the Blavatnik School of Government, University of Oxford.

Jenny Mowat, Managing Director, Babel



> *The wonderful thing was that there wasn't more harm, because technology sustained us during that period. It would have been even worse if we couldn't have worked from home and we couldn't have stayed in touch with friends and loved ones all over the place.*

THE MASSIVE EXPERIMENT IN HOME WORKING

The event opened with a reflection on the wholesale shift to remote working prompted by the global outbreak and spread of COVID-19. In terms of worker productivity and business operations – and considering the size of some workforces – the move from office to home office/ kitchen table has been largely successful. The "massive experiment, a sudden unplanned experiment, in home working" commented Martin, "didn't go nearly as badly as I thought it would have done." This time last year, if you'd asked what would have happened if big organisations, small organisations, those with strong security cultures and those with very weak security cultures, all had to switch to large-scale home working, in one week, with no prior planning, said Martin, we'd have predicted an "absolute catastrophe."

He continued, "The wonderful thing was that there wasn't more harm, because technology sustained us during that period. It would have been even worse if we couldn't have worked from home and we couldn't have stayed in touch with friends and loved ones all over the place." This technology, in addition to "a bit of government help, a bit of sensible planning, a bit of goodwill, and everyone realising that things had to be different if they're going to work, meant that many businesses continued to operate successfully and networks held up. In fact, said Martin, "it's worth noting what didn't happen as well as what did happen."

"Government help" included the launch of the Cyber Aware campaign promoting behaviours to mitigate threats and, in response to coronavirus-related online scams, the NCSC, part of GCHQ, and the City of London Police launching the Suspicious Email Reporting Service, which received 2.3 million reports within just four months of going live. The private sector also used this as an opportunity to help educate end-users. Babel worked with Irdeto, for instance, to commission research into the COVID-19 cybersecurity threat landscape and the impact on businesses and consumers working from home. The resulting whitepaper offered advice and guidance to prevent incidents.

Although this concerted effort to educate and prevent attacks will have helped, Martin's perspective on the past 12 months still seems pretty rosy – perhaps a view that businesses and consumers on the receiving end of scams, hacks and ransomware demands may disagree with. It shouldn't come as a surprise that Martin did caveat his outlook: "in a sense I'm trying to be upbeat because there's so much pessimism around at the moment!" Yes, there is pessimism. But there is also reality.

THE COVID CYBERCRIME PANDEMIC

The new working from home set-up resulted in a complex IT environment, and a broader cybersecurity landscape ready for exploitation by hackers. And exploit they did. The ecosystem "became a very lucrative, ripe target for cybercrime," said Perlroth. "The main thing was all these organisations were trying to enable employees to work from home from their personal devices. They didn't have the same intrusion detection systems, the same security wrapped around personal devices." As a result, "at the beginning of the the pandemic we saw a huge jump in targeting work from home tools and remote protocols."

The NCSC handled 723 incidents between 1 September 2019 and 31 August 2020, an increase on previous years, with around 200 related to coronavirus. In the US, meanwhile, it was reported in August that the FBI had seen a 400% increase in reports of cyberattacks since the outset of the pandemic, with ransomware attacks increasingly targeting SMBs.

It seems few businesses were immune. According to a survey by Barracuda Networks, 46% of organisations across the UK, US, France and Germany have suffered at least one "cybersecurity scare" since the coronavirus lockdown began, as a result of the sudden shift to remote working. Attacks are no longer feared; they're expected. Almost half of businesses questioned said they expect to see a data breach or cybersecurity incident in the next month due to remote working. Among the most feared of all attacks for many businesses and individuals, will be ransomware.

BUSINESS HELD TO RANSOM: A CASE OF IF NOT WHEN?

Specialist insurer Beazley found that there had been a 25% spike in ransomware attacks during the first quarter of 2020 compared to Q4 in 2019. The manufacturing sector was the hardest hit with a 156% increase in incidents quarter-over-quarter.

Ransomware may have increased during the pandemic, but it's nothing new. Martin recalls sitting with Chris Krebs, first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, "in the Munich Security Conference in February 2020, before it was clear how bad the pandemic was going to be, talking about how ransomware was getting out of control." Even then, he said, it was clear that "we were losing the battle on ransomware."

The battle is ongoing, but it's also changing. Cybersecurity, said Martin, is essentially about "confidentiality, integrity and availability of information." Original ransomware was just about availability: "they locked you out and you couldn't use it." Turns out this was actually reasonably easy to defend against: "all you need is backups you can access in due course. You suffer a bit of damage but you can get it back. If all you're worried about is availability, then if you've backed up, why would you pay a ransomware for something you have a spare copy of?" Nowadays, failing to back up data "is almost a morally unacceptable place to be."

Ransomware has also evolved into criminal gangs looking to leak data to damage a business or an individual's reputation. The targets and sums which are extorted have also evolved. Perlroth describes the "huge jump" in sums: "something like $300 and holding an individual PC owner with ransomware maybe seven years ago to maybe $10 million for giant healthcare companies" today.

Big businesses have subsequently made sure that they have backup including making essential spare copies of files and drives. But they also increasingly have backup of another kind: insurance. And herein lies a problem. "The business model is wrong. The incentives are wrong," said Martin, as "it's pretty easy to insure against."

Insurers are simply telling businesses to pay the hackers, because, as Perlroth points out, the cost to remediate, to build back data from scratch, and to build new systems will be less than the costs involved with wiping the systems clean and starting from scratch. As a result, hackers will continue to demand payments and payments will continue to be made.

Ransomware is a serious and escalating problem, yet it's one which is little policed and is subject to little governmental and regulatory oversight. Without proper governance and legislation, commented Martin, decisions that could or should be matters dictated by public policy, are "left to a bunch of individuals to make on their own in situations of crisis." With payments going up, at what point does this all stop? We're "funding this gigantic criminal enterprise," said Perlroth, and as such, this could be the year that serious conversations take place regarding whether it should be made illegal for ransomware victims to pay.

"The battle is ongoing, but it's also changing. Cybersecurity is essentially about confidentiality, integrity and availability of information

HOW CAN WE RESPOND TO RANSOMWARE?

Accordig to our pannelists, there are three things businesses can do to fight back against ransomware perpetrators:

1. **You can improve defenses.**
   This includes backing up important files and backing up data in a separate location offsite or in a dedicated cloud facility. Make multiple copies of backups and ensure these are not connected to your network. Always scan backups for malware before restoring.

2. **You can change the incentive structure.**
   Perlroth agreed with Martin that "incentive structures in cybersecurity in general are all backward." The incentive for businesses is to get product to market as quickly as possible to beat the competition. As a result, they'll often "deal with security problems later or maybe establish a moat around their organisation." The incentive for governments is also misaligned. "They want to conduct espionage and battlefield preparations," said Perlorth, "and sometimes that involves vulnerabilities and software that they need to exploit."

3. **There are technical options – sometimes.**
   As and when options one and two fail, there are technical options, "if you've got good intelligence and you can do controlled operations" said Martin. You can take technical disruptive measures that "basically stop stuff from working and can't be used to attack you," he continued. However, there are all sorts of challenges around this, reflecting a real problem in international cybercrime.

   Cybercrime is arguably very different to other forms of crime. As Martin pointed out, for the first time in human history, it's possible to inflict large-scale, consistent damage to a society without ever setting foot in its territory or that of its allies. Compare this to something like terrorism, where criminals can plot, conspire, money launder etc. from abroad but then have to physically enter a foreign space to do harm.

   With transnational cybercrime "none of that applies." You could have groups operating out of Russia, you could present Russia with all the evidence that they're committing crimes happening but "until Russia changes its constitution, you're never going to disrupt it [criminal activity] through law enforcement." And because Russia doesn't extradite cyber criminals, said Perlroth, "we have to wait until they go on vacation on the Maldives and we might be able to pick them up there!"

   The internet is a largely ungoverned space, so to fight effectively against cyber criminals, you need really good intelligence and "you need to know that you can control it." This sort of direct action should be "a last resort," continued Martin. "It tends to be deployable principally against non-state actors; it doesn't tend to work as a response to state attacks just because it's so escalatory."

This last point about the difficulties of dealing with nation state attacks is growing ever-more important. The idea of a hacker in a hoody in a bedroom is very early noughties. Instead, many of these operations are large-scale, government-sanctioned, intelligence-led – and always denied. They're also great fodder for the media.

NATIONAL INTEREST IN NATION STATE ATTACKS

Take SolarWinds: a name few had ever heard of a few months ago. Now, the brand is synonymous with the snowballing effect of cyberattacks, which has included accusations by US Intelligence Services of Russia's involvement – and counter-claims by Russia – and ongoing media posturing on what happened, how it happened, and who is to blame.

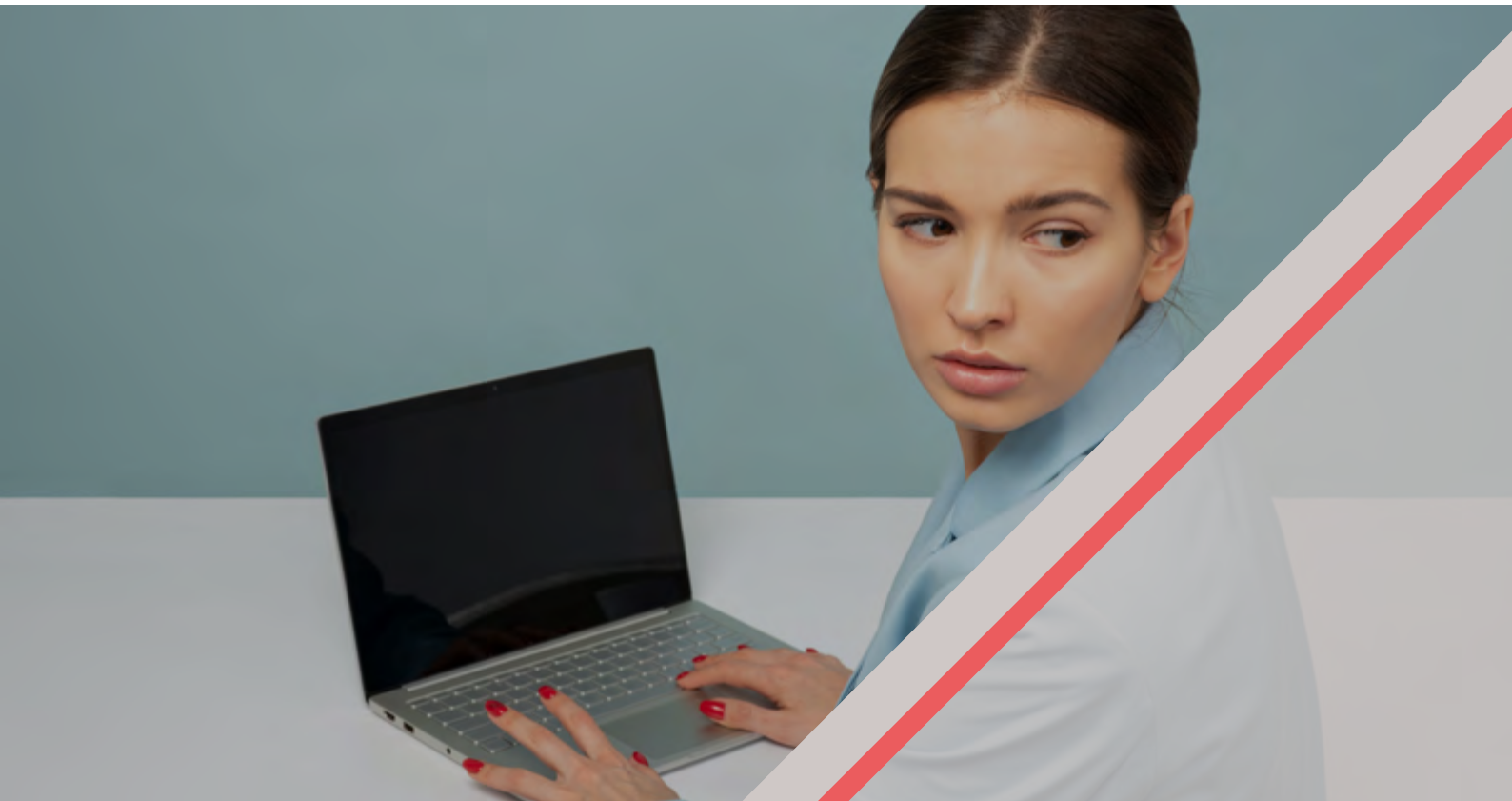
The software company – little-known to many of us prior to December 2020 – was used as a gateway by hackers to access thousands of companies and government departments that use its software. The result, according to Microsoft Corp President Brad Smith, was, "the largest and most sophisticated attack the world has ever seen."

This was, of course, followed by another large and sophisticated attack – on Smith's own Microsoft. The scale of the hack on Microsoft's Exchange email server is still emerging, but it's likely to have affected tens of thousands of organisations. Russia is let off the hook for this one; instead, Microsoft says the perpetrators are "state-sponsored and operating out of China".

Both Russia and China have denied involvement in the SolarWinds and Microsoft incidents. Yet both will continue to be the focus of media attention – along with Iran, US intelligence, world leaders and governments – as different stakeholders attempt to apportion and avoid blame for what often turn into global incidents. And these are just the ones we hear about.

Media interest and sustained coverage of stories of nation state attacks – with all the finger-pointing and blame-apportioning that come with them – are perhaps no bad thing. If law enforcement is currently limited in what it can do, then continued interest from the media and a steady drumbeat of messaging from brands operating in the space, will help raise awareness.

In the US, said Perlroth, "we've been doing a pretty sustained naming and shaming campaign: of North Korean cybercriminals, Iranian state-backed hackers, and Chinese military soldiers who are responsible for thousands of attacks on US electoral property." Despite this, "there's really no chance we'll ever have those people in prison."



MILITARY VS MESSAGING

Instead, there have been attempts this year to impose penalties in the US, as well as campaigns such as that run by Cyber Command. Following an earlier operation in Europe, the US's Cyber Command sent teams to the Middle East and Asia over to identify Iranian, Chinese and North Korean hacking teams and uncover tools they were using to attack networks. These approaches are more about the strength of messaging, rather than the might of military. Perlroth used the example, in the 2016 midterm elections in the US, of Cyber Command hacking into the Internet Research Agency in Russia and posting messages to their computers alerting the organisation that the US had visibility of its operations. In effect, messaging them to say: "we know who you are, we know where you live, we know where you work, and if you do something to these elections, we will find you."

The power of messaging is clear. This is something that brands operating in the cybersecurity space will know all too well. This is a crowded market with businesses competing for media attention in order to get their name, their expertise, their opinions and their products in front of the decision-makers who matter. Journalists also operate in a very busy space, covering seemingly constant breaking news of cyber attacks and developments in the space. Perlroth, for instance revealed that she gets 2,000 emails a day: "It's really hard, it's a fire hose, its every day," she said.

SO HOW CAN BRANDS EFFECTIVELY COMMUNICATE THEIR MESSAGE TO JOURNALISTS?

Know your journalist

Don't email a journalist about a story they have written with the introduction, 'you may have read a story about this cyber attack…' and then use your brand's spokesperson as a mouthpiece. They know about the story…they wrote it! They're not going to cover it again and they're well aware that you're "blasting every journalist on earth. It's not going to go over well. You might as well not send it. It's a little bit embarrassing," said Perlroth.

Dig deep for data

Your organisation is likely sitting on a wealth of data. Dig deep and see if you can re-purpose facts and figures to provide a new angle on an existing narrative or breaking news story. Is there data you can pull from your networks? From your clients? Do your marketing and product teams have insight that could be useful? Or, get fresh data. Could you commission a new survey around an upcoming trend/ hot talking point you've identified?

Think about the development of the story

A story has broken and been covered extensively. Opportunity lost? Not always. You've done your homework and researched your target journalist and their beat. You know which element of the breaking story they've already covered so it's obvious they're not going to cover it again…with your client shoehorned in. So, "think creatively about: what's the day two story? The day three story?" How is the story going to develop and what can you add to the story to progress the narrative, shine a new light on an emerging threat, provide solutions etc.

Think about the reader

Readers want to learn how to protect their business and users from attacks, but every business is different, the threats may be different, their objectives and motivations will be different. The cybersecurity and tech trade press are not a homogenous mass. Titles have different readerships, so make sure you have a strong knowledge not only of your journalist, but of your reader. And don't forget: readers want to be entertained and engaged. "If it's not interesting for the reader then forget it, you might as well not send it at all."

2020 was another busy year for journalists reporting on the cybersecurity space, not least because a significant number of them have also been working remotely. This year, businesses will have to adjust to a hybrid working environment, while our communications networks will only get busier. Activity in the cybersecurity space will therefore continue – and change. Brands must be ready to adapt their messaging and their communications strategies accordingly.

SO HOW DO OUR PANELLISTS SEE THE LANDSCAPE EVOLVING IN 2021, AND WHAT KINDS OF MESSAGES AND STORIES AND ARE THEY INTERESTED IN HEARING?

1. **Securing a permanent, remote workforce**
   Yes, it was a theme of last year, but secure remote working is to remain a major talking point in the cybersecurity space – and press – in 2021. This year, the longer-term roadmap for many businesses has become (slightly!) clearer, with many businesses, including Silicon Valley and global tech heavyweights, having announced that the hybrid working environment is to be a permanent fixture.

   Last year there was room for error as businesses had to move fast and adapt quickly. Lessons (should have) been learnt. The media may not be so kind in response to sloppy security practices. There's also a need to move a step on from how to secure a remote workforce, to "how will it continue?" said Perlroth. There's an opportunity for cybersecurity vendors here, due to continuing demand for solutions. But, with no end in sight to the remote working security narrative, you'll have to ensure messaging remains relevant and stands out from the crowd.

2. **Responding to nation state attacks**
   Nation state attacks are also here to stay. We know they happen, we think we know who's behind them, and brands will continue to comment on them as journalists will continue to report on them. What'll change and become "the big story this year," said Perlroth, is "how we're going to respond, and if we can respond, and what the deterrent strategy is."

   This may require brands and vendors to take a more controversial approach in their commentary and messaging - bold move, but one that could pay off for the brave

3. **Surveillance**
   WhatsApp's privacy update made headlines for the wrong reasons at the start of the year, prompting users to switch to more private and secure alternatives like Telegram and Signal. In Hong Kong, meanwhile, protestors have been coming up with means of avoiding police surveillance technology, including dismantling 'smart' lampposts, and using laser pens to disrupt cameras.

   Cameras at self-checkouts, digital identity, beefed up security at airports, innocuous chip-embedded street furniture: call it surveillance or call it monitoring, governments and private businesses tracking, watching, measuring and assessing us is ever-more prevalent. With borders opening up and the need to prove a clean bill of health likely coming into play this year, expect more on surveillance in the coming months.

   It's an area that's long interested Perlroth: "I'm always fascinated by where surveillance is drifting, not just from government but from which industries are engaging in surveillance and how to thwart that surveillance."

4. Cybersecurity is far bigger than networks

Cybersecurity is no longer just about networks and endpoints and a business securing its IT infrastructure. We should now talk about 'cyberspace', which is global, borderless and driven by geopolitical events and tech supremacy. The battle is on, essentially, between the US and China, commented Martin, and it's a battle "that will define a lot of things." Where's Russia in all this? We've all grown accustomed to living lives dependent on systems and devices that have been built and are operated by the American private sector. Russia, said Martin, isn't attempting to build an alternative to this ecosystem, "it's just messing around on the one that exists." China, on the other hand, is: "exporting it, it's trying to build a better one, a more authoritarian one, a more economically powerful one." As a result, security of cyberspace will emerge as something distinct to what we thought of as cybersecurity, which is about networks, devices etc.

"Security of cyberspace becomes a lot more about who owns it who runs it, how it's built, who controls the materials, how the surveillance systems work, what the model is etc." For businesses and governments – and users of technology, it'll be challenging, "a lot more complicated and more existential," said Martin.

A challenge perhaps, but also an opportunity, for brands to weigh into the debate and pose solutions. 'Solutions' should be read here as game-changing ideas to tackle problems and not simply messaging on 'solutions' as products.

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