THREAT MATRIX

NAVIGATING NEW CHALLENGES AND EMERGING RISKS

WIRED Consulting. x Bird & Bird

INTRODUCTION

Earlier this year, a study led by MIT Media Lab uncovered gender and racial bias in the algorithm behind Amazon's facial recognition software. Amazon's Rekognition, marketed to law enforcement – among others – in the United States, proved less than accurate when it came to identifying someone's gender if they were darker-skinned, with tests showing that it misclassified darker-skinned women 31 per cent of the time; by contrast there was a zero per cent error rate for lighter-skinned males. (Amazon disputed the study's findings.)

As AI-powered technologies such as facial recognition go mainstream, debate is raging as to how they should be deployed in the real world. From smart voice assistants and medical diagnostic tools to services such as Netflix offering personalised recommendations, AI is already stitched into our daily lives. But whether we're talking about its malign influence on elections, the flaws in crime-fighting by algorithm, or how it is open to abuse by authoritarian governments, it's clear that by their very nature great technological leaps forward often carry with them unintended consequences – ones which can quickly flare up into full-blown crises that hit organisations in the bottom line, as well as society at large.

This report zeroes in on four such challenges – where businesses are buffeted by new technology – and considers how the C-suite can lead their companies in response.

The first of these is regulators and the rise of "dawn raids" or unannounced inspections. These have become a fact of life for many sectors, especially in technology, telecoms and media, as regulators grapple with the transformative impact of digitalisation. With more regulations today and therefore greater potential for violations, alongside a broadening of regulatory powers, how should companies prepare and protect themselves?

Second, the threat of external data breaches to businesses is well documented and most treat cyber-security as a priority. But far fewer appreciate the very real risk of an internal breach – for instance, if an employee walks away with a company's data "crown jewels". Should the worst happen, how do you wrestle back the initiative?

The third challenge relates to AI and ethical frameworks. AI is nearing a real-world tipping point. But given the absence of comprehensive regulation, and the potential for abuse, companies are developing their own ethical frameworks. In a world in which consumers and employees increasingly expect businesses to take a moral lead, how should organisations set out their guiding principles?

And fourth, "clicktivism": it has long been a powerful force and a means of rallying mass movements to a cause. But now – in a trend that is set only to intensify – digital activism has arrived in the workplace with "woke" employees who are ready to hold bosses to account. How should businesses react, without stifling whistleblowers or legitimate criticism?

All of these themes have profound implications, and they will shape the decision-making of senior management for years to come. Preparation will not prevent every crisis, but it will equip companies with the right tools to respond.

This report seeks to navigate an evolving landscape, gauge the variety of challenges businesses face, and reveal how to mitigate the inevitable damage should disaster strike. It also focuses on two large organisations that have been in the eye of the storm, yet emerged not just unscathed, but with their reputations enhanced.

PART ONE

WRATH OF THE REGULATORS

Why beefed-up regulators are on the warpath – and how businesses can prepare

It was a dawn raid tailor-made for the social media age. When the Swiss authorities descended on a five-star hotel on the shores of Lake Zurich to arrest officials from FIFA on corruption charges back in 2015, the resulting images shared around the world inflicted reputational damage that football's world governing body has struggled to shake off ever since.

While few criminal or regulatory swoops involve executives being bundled into cars under bed linen and the glare of the waiting media, the risk of dawn raids – otherwise known as "unannounced inspections" where, for instance, competition or fraud authorities descend on companies en masse, sometimes across multiple territories simultaneously – are a fact of business life today.

"They are a real risk for many businesses and the volume of dawn raids has steadily increased in recent years," says Marjolein Geus, a Netherlands-based partner at the international law firm Bird & Bird,

Right: dawn raids are a threat that companies are taking increasingly seriously

and chair of its international Technology & Communications Group.

Geus identifies several factors that she believes are behind the rise. “First, and most obviously, there is just more regulation around, and if there’s more regulation then there’s greater potential for alleged violations. Second, with ongoing digitalisation there’s more data around, and more companies, consumers and countries involved, and that means there’s increasing awareness of regulatory investigations among politicians and in the media, which leads to pressure on the regulators to take action.

“All of that’s happened hand-in-hand with an ongoing broadening of regulatory powers and a growing number of supervisory authorities – there are just more rules, more powers to issue more and larger penalties, and to use forensic methods, and there’s also increased co-operation between authorities.”

The global telecoms industry is one of a number of sectors that has faced an increased risk of dawn raids over the years, according to Geus. As recently as January 2019, for example, Costa Rica’s Justice Department raided the offices of two of Spanish telecoms group Telefonica’s subsidiaries – Movistar and Tejisa – in an investigation into alleged tax fraud. “There have also been a number of competition investigations that have been upheld in the telecommunications sector, and they will often have been preceded by a dawn raid,” says Matthew Redding, a telecoms veteran who was until recently a senior legal advisor at BT.

Dawn raids are a threat that companies are taking increasingly seriously, he continues. “At every telecoms company I’m aware of, it’s certainly a regular subject of legal advisory work – to ensure there is a dawn raid response capability within the business. They have happened, they do happen, mobile companies in particular have been subject to them. That’s why it’s important to ensure that businesses always remain compliant with regulation.

Watchdogs with fangs

It is difficult to exaggerate the shift in the regulatory landscape in recent years. In fields as diverse as financial services, competition and data protection, many regulators wield ever greater powers today and have become ever more interventionist, regularly putting some of the world’s most valuable companies on the back foot. Nowhere is this more evident than in Europe, where Competition Commissioner Margrethe Vestager has led the European Union’s charge against many US tech giants. Over the past few weeks alone, most of the fabled FAANGs have been in Vestager’s crosshairs (or those of EU member states’ regulators).

At the time of writing, the commissioner had just fined Google €1.49 billion ($1.7 billion) for “abusive practices in online advertising” – or as Vestager phrased it: “for illegal misuse of its dominant position in the market”. It was the search giant’s third billion-dollar anti-trust fine from the EU since 2017. The commissioner also said that she was considering a competition investigation into Apple for allegedly using its app store to gain advantage over its rivals – telling a German newspaper that her commission would look into whether there were parallels with Google when it faced an earlier fine from her office of over €2.4 billion ($2.8 billion) in 2017, for abusing its market dominance. This latest twist came just two days after the streaming service Spotify lodged a complaint against Apple with the European Commission.

Meanwhile, Germany’s Federal Cartel Office, the country’s anti-trust regulator, “imposed on Facebook far-reaching restrictions in the processing of user data”, with Andreas Mundt, the cartel office president, saying in a statement: “As a dominant company Facebook is subject to special obligations under competition law. In the operation of its business model the company must take into account that Facebook users practically cannot switch to other social networks.” The platform, which has 1.56 billion daily active users globally, is currently appealing.

Unsurprisingly, increased anti-trust enforcement was a theme that reverberated around a competition conference that was held at the Federal Cartel Office in Berlin in March 2019. “One thing you heard repeatedly was that we’re at an inflection point,” reports attendee Maurice Stucke, Professor of Law at the University of Tennessee and a former trial attorney at the US Department of Justice anti-trust division. “The belief is that [until recently] we’ve had a grand experiment with a more laissez-faire type of anti-trust

policy, and there are significant questions as to whether that policy has delivered competitive markets."

Similarly, in the sphere of data protection and privacy, businesses face beefed-up regulation. GDPR – and the standard that applies internationally – means that companies now face eye-watering fines for non-compliance and data breaches of up to four per cent of annual global turnover or €20m (whichever is greater).

And fines are only part of the cost to corporations that suffer malicious data breaches. Telecoms group TalkTalk was fined a then-record £400,000 by the UK Information Commissioner's Office for its catastrophic 2015 hack; yet this pales beside the reputational fallout, which led to its share price plunging by more than ten per cent and the loss of at least 90,000 customers in the aftermath. "The reputational damage when it becomes known that a regulator is even investigating can do a lot of harm and can definitely have an effect on stock prices in the case of listed companies," says Geus. "And that's even in cases where the investigation ends up finding no violation, because by then the damage has been done."

THREE TIPS: REGULATION

MARJOLEIN GEUS
Partner, Bird & Bird

So how should companies better prepare themselves for potential dawn-raid scenarios and from sharper-toothed watchdogs?

1. Actively prepare

-

Make sure a compliance programme is in place that is properly implemented and kept up to date throughout the organisation. Make sure that the reception desk and the legal department alike are properly instructed in order to ensure that an investigation takes place in an orderly manner and with sufficient support. Downloading a dawn-raid assistance app (such as our own Dawn-Raid Survival Toolkit) to your phone also helps to control the situation.

2. Have a global response in place

-

If you're a multinational with offices across the world, be clear about which territories are of utmost importance to your business and the powers of the authorities locally. Have regulatory expertise in place on the ground, but should the scale of the crisis demand it, be prepared to fly in your lawyers from another country to help out.

3. Contain the PR fallout
(external and internal)

-

When a dawn raid takes place, the public affairs and communications departments need to be sitting alongside the leadership and the legal and compliance teams, and have their own crisis plans ready to activate. Not every investigation will leak publicly, but be prepared for that eventuality. Moreover, internal communications are always critical, because when anywhere between five and 30 people from a regulator turn up on your doorstep, word travels fast.

PART

TWO

INSIDE JOB

Your company's most sensitive data may be vulnerable to theft from within. Here's what to do about it

In January 2019, Jizhong Chen, an engineer in Apple's autonomous car division, was spotted covertly snapping pictures in a restricted area. According to prosecutors, Chen, a Chinese national, had 2,000 files on his personal hard drive, including manuals and schematics, and was applying for a job with a Chinese rival. The charges came months after a similar case in which another Apple worker was accused of stealing trade secrets and arrested by FBI agents while attempting to board a flight to China.

Such cases, particularly in rapidly evolving proprietary fields, are far from rare. However, they are only one of a range of – on occasion, existential – threats companies face today from individuals, groups or even nation-states that steal confidential information. From the Colonel's once-secret KFC fried chicken recipe and the Coca-Cola formula at one extreme, to key customer data, "black box" know-how about valuable processes, systems, market forecasting, R&D data, algorithms, expansion plans and key competitors at the other, in the digital age, every business has sensitive commercial data.

Yet many companies, according to Jason Hart, chief technology

Right: the threat from internal breaches, in which an employee or contractor steals data, is often underestimated

officer at Gemalto's data protection solutions, do not fully grasp the level of associated risk. "Board and C-suite level awareness around security generally has grown," he says, "but there's still much less understanding about what the different risks are around confidentiality and data integrity [where data is maliciously altered], the different types of data a company may hold, and the impact it would have if they were to be compromised."

Thanks to the ability to access cloud-stored databases remotely through multiple devices, businesses are far more efficient and yet simultaneously more vulnerable to attack. At the same time, many company leadership teams have a tendency to be "naïve" about what actually constitutes a trade secret or confidential information, according to Sophie Eyre, a London-based partner in Bird & Bird's international Dispute Resolution Group, who specialises in complex civil fraud. "I have spoken to certain businesses who don't seem to recognise that their internal sales figures or market penetration strategy, for instance, are highly confidential information – and it's only when you ask them what would happen if that information were to hit the market early, what it would do to their share price and market positioning, that they do recognise it," she says.

Broadly speaking, data breaches can be divided into two spheres. The first is external, in which an outside hacker or group exploits network vulnerabilities to cause harm or havoc, or steal industrial or military secrets. A recent example was the hack on an Australian defence contractor, in which around 30 gigabytes of data were stolen – including details about Australia's A$17bn ($12bn) F-35 Joint Strike Fighter programme, C130 transport plane and P-8 Poseidon surveillance aircraft. While it's not known – at least publicly – who was behind the hack, it raised issues of national security, and the publicity is certain to have had an adverse effect on the contractor's business.

In a (thankfully rare) worst-case scenario, a malicious hacker might hawk such stolen data on the Dark Web. That situation occurred in February 2019 when, as part of a series of data dumps, a hacker using the alias "Gnosticplayers" placed a set of hacked databases containing data from hundreds of millions of users for sale on the Dark Web. The data was stolen from many companies, including the storytelling platform Storybird and Gfycat, a GIF-making and sharing site; and the data breach would have caused considerable reputational damage. "A data breach can have a serious financial impact too," adds Hart, "where people lose trust in that brand, cancel their subscription, and move to a new provider. If we're talking about a public company clearly it affects stock price too."

'Every organisation's worst nightmare'

However, in many ways it is the second sphere – internal breaches, in which an employee or contractor takes advantage of access to steal or leak proprietary information – that are arguably the greater risk, precisely because the threat is underestimated. On the milder end of the spectrum, a typical scenario might involve an employee leaving a company and (mistakenly) seeing the dataset, marketing or code they developed almost as part of their CV. "They may think they are entitled to take it with them, when they're not," says Eyre.

One step away from that more "innocent" misappropriation of confidential information comes the employee who not only believes that they are entitled to take that data, but plans to use it in their next business, continues Eyre. "They're not doing it for malicious reasons, but uploading someone else's source code or keeping the sales figures or go-to-market strategies to use in their next business, can cause an employer huge damage."

From there you step into a more sinister world, she says. "We have seen quite a few cases where you have very senior management or company founders, who have taken on external investment and are so fed up with how the company is going, or how they're being treated, that they set up in competition and take databases of clients, manuals or imprints of source code or strategies. They feel like they created it, so can do what they like with it."

At the extreme end of the spectrum are employees paid to acquire information for competitors; and people who simply set out to cause harm. Indeed probably every organisation's worst nightmare is a hack in which the attackers end up publishing stolen data on social media, perhaps using it to hold the company to ransom.

So what should companies do? First get your PR people involved, while from a legal perspective send take-down notices to all the publishers concerned, says Eyre. "And if you don't know who has posted it, you'll not only be seeking injunctions, but disclosure orders for the IP addresses of the people who hosted the leak. What you need to do is not just the one-dimensional thing, which is stop what is currently in the public domain, but find out who else has got it, how many people have seen it – and shut it down that way."

She would seek a permanent mandatory injunction to restrain people with whom the data has been shared from ever talking about or referring to it, and have every copy of that leak destroyed. "You'd do all of above within 36 hours, because that's the level of importance. But you wouldn't sleep much in the meantime."

DATA THEFT
SingHealth's megahack

In July 2018 the authorities in Singapore announced that the island city-state had suffered its worst ever data breach, with hackers stealing the personal information of 1.5 million patients including that of Prime Minister Lee Hsien Loong. The unknown attackers (thought to be a state-sponsored espionage group) infiltrated the computer systems of SingHealth, Singapore's largest group of healthcare institutions, accessing the non-medical personal data including names, addresses, gender, race and dates of birth of patients who had visited specialist outpatient clinics and polyclinics between May 2015 and July 2018.

As many as 160,000 of those hacked had their outpatient prescriptions stolen, too. "This was a deliberate, targeted and well-planned cyber attack," according to David Koh, the chief executive of the Cyber Security Agency of Singapore.

The sheer scale of the attack – the details of approximately one quarter of the population were breached – was a public relations catastrophe for the technologically advanced country, which recently ranked fifth in the global innovation index (ahead of the United States) and whose much vaunted Smart Nation initiative aims to further transform Singapore through innovation.

However, the way in which the authorities dealt with the aftermath of the attack – which included publishing a detailed 453-page report on the hack just six months later, contacting affected patients individually, and assembling a committee to review data security practices right across the public sector – has earned them plaudits. PwC partner Tan Shong Ye said the government had "responded quickly" to the breach. "It is good that action was taken immediately after the threat was detected to minimise the risk of further data exfiltration," he told financial daily *The Business Times*.

SOPHIE EYRE
Partner, Bird & Bird

Here are the steps organisations should take to protect themselves from an internal data breach

1. Have very clear policies in place

-

Have total clarity about what employees can and can't do. Put security in place in relation to confidential information, particularly trade secrets – whether firewalls or security barriers – and send regular bulletins to employees to ensure they know just what they can and can't access, and why.

2. Ensure the right people have access

-

Does someone in the accounts department really need to have access to market projections? Do the marketing team need to see historical sales data? Because if they don't need to, then don't allow them access. And if they need one-off access, then establish a chain of command to authorise that on an ad hoc basis.

3. What to do if the offender is unknown

-

Life's a lot harder, but that doesn't mean you're stymied. The High Court has recently granted injunctions against persons unknown, where a company knew someone within a class of people who all had access to stolen data is behind a breach. Everyone in that class got served, and the individual was eventually uncovered.

PART

THREE

‘TECH IS NOT VALUE-NEUTRAL’

Artificial intelligence and why crafting ethical frameworks offers competitive advantage

Born out of a research project between the Los Angeles Police Department and UCLA (the University of California, Los Angeles), PredPol bills itself as the market leader in predictive policing. It uses a machine-learning algorithm that draws on continually updated historical datasets to “predict critical events and gain actionable insights” for police. The attractions of predictive policing, and similar tools powered by artificial intelligence (AI), to law enforcement authorities are obvious: policing resources can be deployed more efficiently, and particular types of crime and criminal hotspots can be identified and blitzed, while police chiefs are better equipped to spot longer-term trends.

There’s comfort in cold, hard data too. Yet algorithmic policing, in force across the United States since the early 2010s, has long proved highly contentious. Programmer biases and pre-existing discriminations can become self-perpetuating with, for example, intensification of police patrols in crime-ridden neighbourhoods leading to higher arrest rates and therefore further patrols. Those born into such areas are likely to suffer stigmatisation and often worse, whether they have ever broken the law or not.

Indeed, the use of algorithms within the criminal justice system has been the focus of a recent inquiry by the Technology and Law Policy Commission of the Law Society of England and Wales: Algorithms in the Justice System took evidence from a wide range of experts from the world of technology, government and commercial and human rights law on, among other things, whether the use of algorithms within the justice system should be regulated – and if so, then how this needs to be done.

Criminal justice is just one area in which the mainstream adoption of rapidly improving general purpose technologies such as AI and machine learning is gathering pace. From medicine to manufacturing, and retail to finance, AI already brings huge benefits to both business and wider society. However, it has a flipside, too. As a 2018 European Parliament study states: with AI systems becoming increasingly autonomous, “safety, transparency and accountability concerns, including those related to poor decision-making, discrimination biases, job losses and malevolent uses of AI (eg in weaponry and cyber-conflicts) become more and more relevant”. At the time of writing, the European Commission had just launched a pilot phase to develop ethical guidelines for achieving “trustworthy AI”.

Amid heightened awareness of the implications of the technology, startups, global platforms and large corporates alike are crafting DIY ethical frameworks – or pre-regulation – around a technology that is evolving so quickly it has largely bypassed lawmakers and regulators. “Frameworks are definitely a good starting-point,” says Bryony Hurst, a London-based partner at international law firm Bird & Bird. “They are also a good way to answer critics, in effect saying: We’re not just running headfirst into the development of this new and mostly untested technology, and we’re thinking ahead and being considerate in the way we develop it.”

An executive at the British chip-designing giant ARM goes further, arguing passionately that because AI is at a critical moment of evolution, external regulation risks stifling innovation, and practitioners are therefore duty-bound to seize the initiative. “The reality is that technology innovation has always moved faster than regulation – and now exponentially so,” says Carolyn Herzog, the Silicon Valley-based EVP and General Counsel at ARM, which has established an internal cross-functional working group to explore the issues surrounding AI and ethics and what they mean for the wider tech ecosystem. “Regulation feels very much like a blunt instrument and the risk is that governments could over-regulate as they try to create this future-proof legislation. But that could really damage efforts to advance AI.”

Pioneers in the field have long grappled with these issues, acutely aware that deep research in this field carries grave responsibilities. Before DeepMind was acquired by Google for $500 million

in 2014, the company's founders wanted to be sure that Google's leadership shared their approach to AI and would agree to set up an ethics board to oversee both companies' research. "Having some ethical oversight was important to us," recalls DeepMind co-founder Demis Hassabis. "And you can see that in [Google's] AI Principles that they published [in June 2018], which we helped out with." However, it's worth noting that Google's AI ethics council, the external advisory board charged with ensuring the company adheres to its AI principles, was dissolved after just one week, in the wake of a row over one of its members.

In 2017, DeepMind announced the creation of a new research unit devoted to understanding the real world impacts of AI. "Technology is not value neutral," declares its website, "and technologists must take responsibility for the ethical and social impact of their work." Similarly, Swedish telecoms giant Telia Company, which to date has restricted its deployment of AI "in a few narrow use cases", has developed its own Guiding Principles on Trusted AI Ethics. This is good AI governance – and could be a market differentiator for Telia.

Yet some industry players are highly sceptical about the very idea of allowing such an impactful technology, with so many far-reaching applications, to police itself. "Right now you've got some people who do it completely ad hoc," says Suranga Chandratillake, an entrepreneur turned partner at Balderton Capital, who has invested in a number of AI-based startups. "So it's literally a CEO eyeballs a particular situation and decides whether it's ethically right or wrong. That's clearly insufficient. Then you've got larger companies policing themselves, but that's completely self-serving."

However, Chandratillake does concede that – for startups at least – in the absence of formal regulation, company-devised ethical frameworks are a necessary first step. "I don't think that there's any downside in doing it, especially if you are a new company where [AI] is central to what you do. I would definitely do that in the vacuum that exists today, because it's better than nothing. But in my mind, over time, regulation would have to be done centrally, by

Left: AI systems are becoming increasingly autonomous, causing safety, transparency and accountability concerns an unrelated body, and ideally it would be something blessed by people who don't directly benefit from it."

This push for ethical clarity in the development of AI takes place against a wider backdrop in which consumer ethics and corporate social responsibility are now significant drivers of change. Today, companies increasingly wear their hearts on their sleeves. The continuing backlash against Big Tech also shows that being one of the top-ten companies in the world by market cap is no longer the only important metric businesses are benchmarked against. Values are scrutinised alongside valuation; reputation alongside revenues. JUST Capital, for example, ranks companies in the US based on issues Americans care about most, including good jobs, fair pay, employee education and environmental impact. These rankings are now used by investors looking for ethical businesses, with Goldman Sachs' JUST US Large Cap Equity ETF the first exchange-traded fund to be based on JUST Capital's research.

"Consumers, investors and employees are increasingly putting pressure on companies to do the right thing and think about what they are creating and the impact it can have," says Hurst, who argues that having a credible and positive story to tell can help a business stand out. "If done well, it can also help demonstrate a company's commitment to corporate social responsibility, and in an industry where there's a war for talent, it can engage ethically minded employees and help attract the best people."

Furthermore, if a company finds itself embroiled in litigation that has emerged from an AI-related issue, having proactively developed an ethical framework helps provide a better defence, she adds. "The first thing I would ask anyone when defending a claim arising out of AI is: 'What have you done to think ahead on this? What are the measures you took to try to stop it from happening?' Developing a corporate conscience and having a story to tell (this isn't limited to AI, but covers everything from climate change and sustainability to diversity policies and privacy practices) definitely goes a long way."

THREE TIPS: AI AND ETHICS

BRYONY HURST
Partner, Bird & Bird

Developing a corporate ethical framework must be rooted in responsibility and a sense of purpose

1. Don't do anything cynically

-

While there are potentially real benefits to having ethical guidelines in place, always be authentic. When your company's in the spotlight, anything that's half-baked will be seen through.

2. Foster an ethical culture throughout your entire business

-

From the leadership downwards everyone in the company has to conduct themselves in accordance with the ethical behaviour you're trying to encourage. Hire, promote and reward based upon those values too. And train down: if you've got a sales team being approached by customers wanting to use AI in potentially questionable ways, for example, make sure they have the tools to recognise what those might be.

3. Put external checks and balances in place

-

Companies with ethical frameworks that have failed to be fully transparent about them, or subject them to independent reviews, are coming under fire. Those responsible for ethical practice should not be in charge of protecting the bottom line. Implement an external review board and ensure it represents a diverse range of people: representatives of customers, business partners, suppliers and sectors of society who may be particularly impacted.

PART

FOUR

THE WOKE WORKFORCE

Digital activism has come to the workplace, with staff publicly holding leadership to account. Bosses should tread carefully in response

In June 2018, news leaked to the US tech website Gizmodo that Google would not be renewing its contract with the US Defense Department, which was deploying Google artificial intelligence tools for the analysis of military drone footage – an initiative known as Project Maven. The decision came after intense pressure from more than 4,000 Google staffers, who signed a petition calling for the Pentagon contract to be terminated, despite leaked internal emails showing that Google's senior leadership "was enthusiastically supportive" of the project.

Weeks later the search giant responded further to the revolution in its ranks, first unveiling a set of AI Principles [see Section 3: Tech Is Not Value Neutral] and then, in October 2018, also withdrawing from the bidding for the contract for a Pentagon cloud-computing project known as the Joint Enterprise Defense Infrastructure (JEDI) – which was reportedly worth $10 billion over ten years. Campaign group the Tech Workers Coalition hailed the decision in a Medium post, in which the group stated: "During the last few months, we have seen unprecedented levels of unrest within the tech industry from fellow disgruntled workers who are opposed to technologies that their own companies are developing."

It's hardly a hot scoop that anyone with an axe to grind and access to a Wi-Fi connection can be a digital activist today, using social media platforms to spark mass movements, drive social change and hold the powerful to account. In the United Kingdom, for example, the pro-migrant campaign #StopFundingHate has convinced brands such as The Body Shop to cease advertising (at least temporarily) with a number of British tabloid newspapers. "Social media can supercharge campaigns, connecting people all over the world directly with those in power in a way that wouldn't have been possible even a few years ago," says Bert Wander, Campaigns Director at Avaaz, a campaigning group which counts 51 million members worldwide.

Yet a far more recent – and growing – trend is the way employees are mobilising against their own bosses, whether it's to call out individual behaviour, or to protest about the overall strategic direction of the company, which was once the exclusive preserve of executives and the board. In the tech industry alone, protests at Amazon, alongside the aforementioned Google petition (and Google Walkout, which saw thousands of staffers stage walkouts in the wake of claims of sexual harassment and gender inequality), show that "woke" – or politically engaged – staffers are no longer afraid to put their heads above the parapet.

In the wake of the success of headline-grabbing digital social justice movements such as #BlackLivesMatter, #MeToo and #TimesUp, social media storms have shattered storied reputations, humbled magnates and ended careers in sectors as diverse as retail, entertainment, media, politics, education, medicine and financial services. In many cases, the employer's brand has seen collateral damage too, as viral coverage makes the leap from Twitter storm and Facebook feeds to news websites and broadcast bulletins. A company's bottom line can be seriously impacted too, particularly if the individual concerned is personally associated with a brand.

'Fundamental wrongdoing'

So how then should organisations respond when they find themselves on the receiving end of campaigns – or in the crosshairs of an individual's anger – that wells up from within their own ranks?

According to Pattie Walsh, a partner in Bird & Bird's international Employment Group, based in Hong Kong, companies have to strike a careful balance between the rights of the business to protect certain fundamentals, such as their confidential information and reputation, while also accepting that their staff have access to a raft of communication tools as well as insider information – a potent mix in the wrong hands. "So it's about accepting that there's going to be that continual tension," she says.

The majority of organisations don't want to stop whistleblowing or the communication of fundamental wrongdoing, Walsh continues. "Any organisation I speak to today would say, we don't want to be part of trying to close down legitimate comment. But the myriad stuff in the middle is very difficult to navigate. From an employee's point of view, it's also difficult to understand the ground rules when you are on someone's payroll, where the employer has legitimate expectations that certain things do remain inside that 'family' structure. That's a legitimate request or obligation and is not in any way trying to stop people having their own views."

Walsh advises companies to develop ground rules for employees that capture expectations and responsibilities on both sides. "I don't think you can take those for granted and assume people will just know them, so there have to be written-down clear indications about what is expected, and like all workplace policy, a policy's just a policy if it lives in people's drawers or on a corner of the intranet. If nobody talks about it properly or lives by it, then it's a pretty ineffective tool."

She adds: "Organisations often struggle when it comes to their senior leadership, or stars in terms of revenue generation, or people who are held up as success stories. When those individuals break the rules, then you've got to be strong enough to say these are our ground rules and they apply to you just as much as anyone else."

Meanwhile, cultural attitudes to whistleblowing and digital activism

Right: employees are increasingly mobilising against their own bosses via social media

vary wildly around the world – and not just between continents, but between individual countries too, continues Walsh. "You'll find the approach is entirely different between Germany, France and the UK, which will be entirely different to Australia and Hong Kong. So the importance of culture can't be underestimated."

However, she urges companies with an international presence to look closely at jurisdictions where there's a low level or complete absence of reporting of illegal or inappropriate behaviour through the business's official channels. "In fact, the absence of reporting or communication using internal mechanisms is often a cause for concern, because it implies that people don't have the power to speak up, or that culturally there are some reservations and often real issues have just not been captured," she says. "That's one of the big shifts – getting organisations to consider what they're not hearing about, as well as what they are."

THREE TIPS: DIGITAL ACTIVISM

PATTIE WALSH
Partner, Bird & Bird

It pays to develop ground rules that balance the rights of organisations with the expectations of employees

1. Develop ground rules and write them down
-

Leave no one in any doubt what the entire organisation's responsibilities and entitlements are, from top to bottom.

2. Don't just publish these ground rules, talk about them too
-

Just having a policy in isolation won't work. We all know people won't necessarily read it. So make sure that whatever you've adopted is culturally appropriated and communicated throughout your organisation – especially if you're in multiple jurisdictions and locations around the world.

3. Live by your commitments and lead by example
-

You've got to do what you say you're going to do. And the same rules apply to everyone, no matter who they are.

DIGITAL ACTIVISM
Starbucks' race row

One afternoon, in April 2018, two African American men pitched up at a Starbucks in downtown Philadelphia asking to use the toilet. As they hadn't made a purchase, an employee informed them that the restroom was for paying customers only. When they declined to leave, the police were called. What happened next made international news.

In a viral video shot on a smartphone by another customer and posted to Twitter, where it has been viewed 11.4 million times, the two young men – Rashon Nelson and Donte Robinson – can be seen being led away in handcuffs by police, arrested on suspicion of trespassing. The incident lit a social media touchpaper, with #BoycottStarbucks trending on Twitter, and sparking protests in Starbucks coffee shops across the US. A near week-long barrage of unfavourable news coverage followed, as well as a grovelling apology from the chain's CEO, Kevin Johnson, who pledged to "make any necessary changes to our practices that would help prevent such an occurrence from ever happening again".

However, while the toxic fallout might well have had a serious impact on the Starbucks bottom line (and has done in similar cases), the company actually saw revenues grow by 14 per cent in the wake of the Philadelphia incident. It turns out that the company's mature response helped enhance its reputation. This included shuttering all 8,000 Starbucks shops for an afternoon to put 175,000 employees through "racial bias" training, as well as coming to a financial settlement with Nelson and Robinson, and offering them university scholarships. "Our approach to this will pay long-term dividends to Starbucks," said Johnson in an earnings call at the time.

ABOUT US

Bird & Bird

Bird & Bird is an international law firm with a focus on helping organisations being changed by technology and the digital world. With more than 1,300 lawyers in 29 offices across Europe, the Middle East, Asia-Pacific and North America, we are ready to help you, wherever you are in the world. Please visit: *twobirds.com*

WIRED Consulting

WIRED Consulting uses the collective power of the WIRED network to help organisations adapt to the fourth Industrial Revolution. Through our unrivalled network of startups, entrepreneurs and technology pioneers, we help organisations forge connections to make sense of the epochal shifts in business and society. Please visit: *wired.co.uk/consulting*

Report author **James Silver**
Report Art editor **Jeffrey Lee, WIRED**
Art direction **Andrew Diprose, WIRED**
Illustrator **Alex Mellon**
Sub-editor **Andrew Mayers**
Project leads
Emma Cowdray, Senior Projects Consultant, WIRED Consulting
Sophie Bowkett, Head of Marketing Communications, Bird & Bird

Contact:
sophie.bowkett@twobirds.com,
emma.cowdray@condenast.co.uk
The Condé Nast Publications Ltd
Vogue House, 1-2 Hanover Square
London WIS 1JU

REGULATION

-

Marjolein Geus
Netherlands-based Partner at Bird & Bird, and chair of its international Technology & Communications Group

Matthew Redding
Telecoms veteran who was until recently a senior legal adviser at BT

Maurice Stucke
Professor of law at the University of Tennessee and a former trial attorney at the US Department of Justice anti-trust division

DATA THEFT

-

Jason Hart
CTO at Gemalto's data protection solutions

Sophie Eyre
London-based partner in Bird & Bird's international Dispute Resolution Group

AI & ETHICS

-

Bryony Hurst
London-based Partner at Bird & Bird.

Demis Hassabis
Co-founder of DeepMind

Suranga Chandratillake
Entrepreneur turned partner at Balderton Capital

Carolyn Herzog
Silicon Valley-based EVP and General Counsel for British chip designer ARM

DIGITAL ACTIVISM

-

Bert Wander
Campaigns Director at Avaaz

Pattie Walsh
Partner in Bird & Bird's international Employment Group, based in Hong Kong

WIRED Consulting. x Bird & Bird