BUSINESS RISK

04 MANAGING AN EXPLOSIVE CRISIS
Leaders must communicate with speed, honesty and compassion

06 RISE OF THE CHIEF CULTURE OFFICER
Chief executives must be flag bearers of brand reputation

08 ROUNDTABLE: WHAT THE LEADERS SAY
Risk management and resilience in a fast-moving digital age

REPUTATIONAL RISK

Why reputation could be your biggest future risk

As clients and consumers become more aware of social and corporate injustice, damage to company reputation, which could sink a business in an instant, is rising up the boardroom agenda

Michelle Perry

Since the global financial crash, public companies have faced what must feel like a barrage of new reporting requirements. Regulators have pushed for greater corporate transparency in the wake of the 2008 economic carnage in an attempt to regain trust and rebuild reputations.

But during the ensuing decade, new global media channels grew, evolved and spread, which enlarged the public's access to information and the speed at which they receive it, refocusing the spotlight on corporate actions.

The risk to reputation has traditionally been seen as an outcome of other risks and not necessarily a standalone risk. This view has been gradually changing because it is increasingly clear that reputation is critical to the viability of a company.

With this greater knowledge and means of communicating, societal norms and public expectations of companies have evolved too. People's voices are louder and opinions, valid or otherwise, can spread around the world in nanoseconds. Nevertheless, trust in companies has recovered somewhat, according to the *Edelman 2019 Trust Barometer*.

Trust has rallied so much so that 76 per cent of those surveyed by Edelman say chief executives should take the lead on change rather than waiting for governments to impose it. This suggests that despite the consistent demands for greater corporate disclosure, management are still not leading on change as quickly as the public want, and therefore still haven't understood how quickly reputation can be affected in a high-speed world of global communications.

"Traditionally, risk officers have seen reputational risk as a consequence of other things happening. Is it a risk of risks or a risk in its own right?" asks Mark Hutcheon, director of risk advisory at Deloitte.

> **How you are viewed in all manner of different aspects, not just products and services, but your impact on society as an employer is right at the top of the agenda now**

Mr Hutcheon says that most companies still see reputation as a risk of risk. In fact, he says, if that question had been asked five years ago, no one would have seen reputational risk as a standalone risk.

Another core reason why reputational risk is more vital is because the balance between tangible and intangible assets has tipped towards intangible value, such as trust, reputation and goodwill, elements that are not as easy to manage as physical machinery. Therefore, the valuation of a business can be increasingly found in its intangible assets.

"Companies are good at managing humans and physical assets, but they aren't good at managing intangible assets. We haven't got our heads around the idea that we have a whole new class of assets. We have to learn how to manage them, understand the risk and put strategies in place," says John Ludlow, chief executive of risk managers Airmic.

This shift, coupled with the rapid rise in social media usage, has made reputational risk much trickier to handle and therefore more important to manage. Suddenly, the incidents that can damage reputation are a lot more volatile, quicker acting and, in some cases, can become systemic risks to organisations.

Uber's decision not to report to police sexual attacks and other crimes by its drivers for fear of damaging its reputation massively backfired for the taxi-hailing giant when in September 2017 Transport for London revoked its licence. Uber claims to have turned over a new leaf by bringing in chief executive in Dara Khosrowshahi. Its reputation, however, remains tarnished in one of the most important markets for Uber outside America.

Companies that try to hide wrongdoing, such as German car manufacturer Volkswagen when its emissions scandal was uncovered in September 2015, are suffering for longer and deeper because news travels fast and you can't fix a brand like you can fix a misfiring machine.

"How you are viewed in all manner of different aspects, not just products and services, but your impact on society as an employer is right at the top of the agenda now. This is a new phenomenon in its importance," says Jon Terry, diversity and inclusion consulting leader at PwC UK.

Although it's high on the board's agenda, change seems to be slow. Traditional company structures aren't designed to manage the new risks to reputation, says Mr Hutcheon. They need to restructure their thinking and teams to build early-warning systems that detect reputational risk.

"Companies are getting there, but it's just not joined up enough yet," says Airmic's Mr Ludlow.

Traditionally, risk is dealt with by risk experts, while reputation tends to be managed by the corporate affairs or communications teams. When those two teams work in silos, lacking any meaningful collaboration, risks can rise up undetected.

"That's where it falls down," Mr Hutcheon says, "when the gap widens between the comms team, who are the antennae for the business, and the professional risk experts. That's when companies face real risk exposure."

Some evidence of this can be seen by the fact that with one week to the deadline of April 4, fewer than 4,000 of the 10,000 large UK companies required to report on their gender pay gap had still not disclosed the average difference between men and women's pay per hour. Increasingly, the gender pay gap is a focus not just for female employees, but for investors and other stakeholders too.

In contrast, FTSE 100 drinks giant Diageo, which has seen its share price rise exponentially over the past decade, is repeatedly held up as a company to be admired because of its progressive policies, such as its latest one on full pay for parental leave for the first 26 weeks for all its 4,500 employees.

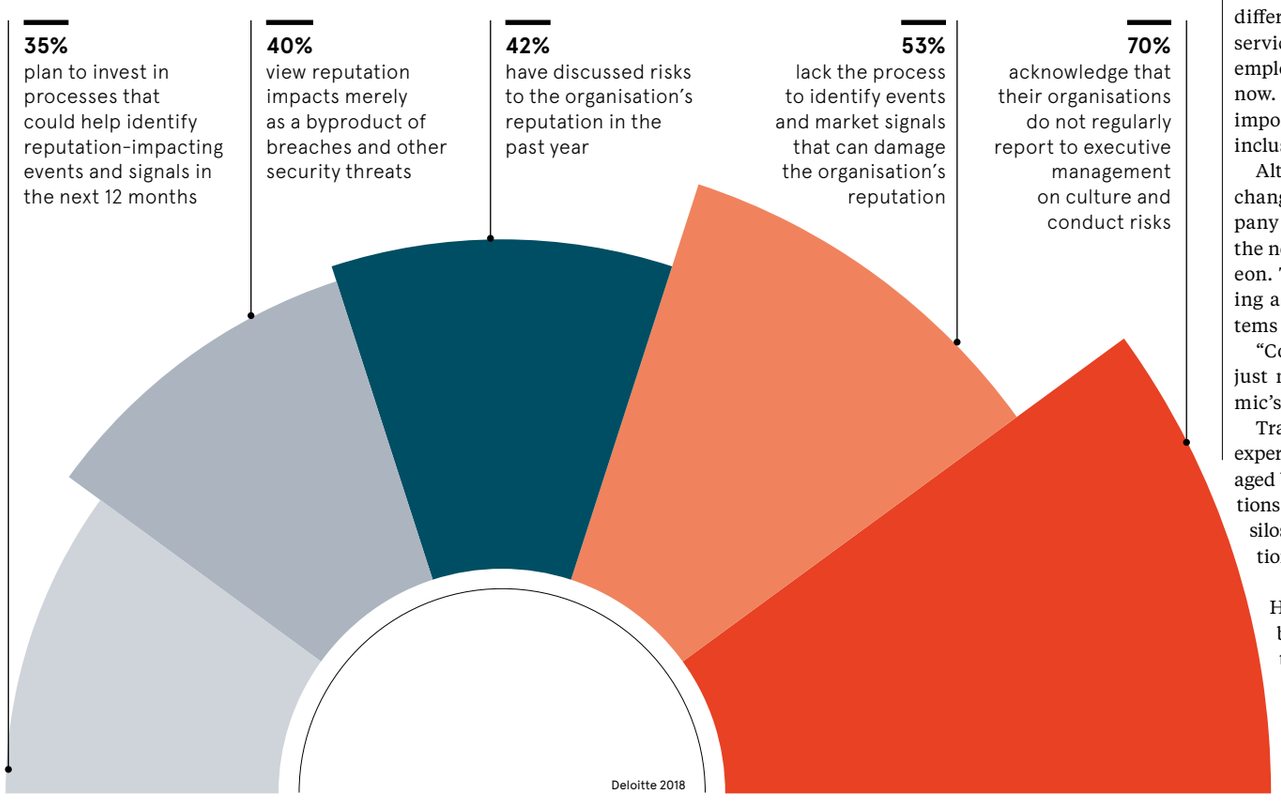
"It's a new era for business. Large businesses enjoy much less control and ultimately that's an empowering thing. A lot of control is moving out of the business to society. And that will align how business puts back things into society when they are constantly under scrutiny. It's going to feel hard for businesses, but that's the way things are going," Mr Hutcheon says.

Research consistently shows that more diverse companies are more profitable and current thinking suggests more open and transparent companies reap the rewards. As counterintuitive, and perhaps as painful, as it may be to meet the public's new demands, management need to disclose more, more frequently.

Understanding and managing reputational risk is all part of societal change. Aligning commercial interests with social ones shouldn't be such a hard place to start. More importantly, it's not a question of unlimited disclosure, but relevant disclosure. Whether we've reached a tipping point in disclosure terms will be determined perhaps by how corporates handle the next financial crisis. ●

REPUTATIONAL RISK REPORTING

Percentage of chief executives



76%

of employees say chief executives should take the lead on change rather than waiting for governments to impose it

Edelman 2019 Trust Barometer

Distributed in
THE SUNDAY TIMES

Published in association with
airmic

Contributors

Josie Cox
Freelance business reporter, commentator and broadcaster, she worked at *Reuters* and *The Wall Street Journal*, and was business editor of *The Independent*.

Nick Easen
Award-winning freelance journalist and broadcaster, he produces for BBC World News, and writes on business, economics, science, technology and travel.

Karam Filfilan
Business editor and writer specialising in human resources, future of work and innovation, he was previously deputy editor of *Changeboard*.

Jim McClelland
Sustainable futurist, his specialisms include built environment, corporate social responsibility and ecosystem services.

Kate O'Flaherty
Specialist writer on business and government technology, her work appears regularly in national, trade and business publications.

Michelle Perry
Freelance business journalist, she is editor of *UK Landlord* magazine and *PropertyEU* correspondent.

raconteur reports

Publishing manager
Reuben Howard

Managing editor
Peter Archer

Data editor
Tom Watts

Head of production
Justyna O'Connell

Digital content executive
Fran Cassidy

Design
Grant Chapman
Sara Gelfgren
Kellie Jerrard
Samuele Motta

Head of design
Tim Whitlock

Technological arms race against identity fraud

Companies are struggling to maintain a great digital experience while preventing identity fraud, but security and assurance need not be blockers to speed and convenience online

Understanding identity is crucial to any business or personal interaction. In the digital age, it's a necessity to being able to consume a service or complete a transaction. But when the key information typically required to verify an identity – name, date of birth and address – can be easily obtained, consumers are highly vulnerable to fraud.

The threat of identity theft has driven greater customer demands for more privacy and security when it comes to their personal data. High-profile data breaches have fuelled a fear among consumers about how their information will be used and driven a desire for more control.

While the internet has opened up a multitude of new ways for fraudsters to steal information, identity requirements in the UK have been slow to evolve in line. Many companies still just ask for that trio of identity markers, which are also the standard information required to sign a contract, to obtain someone's sensitive details.

"We're so reliant on those pieces of information to define who we are that it has put us in a situation where your name, date of birth and address become very valuable for someone to steal," says Paul Weathersby, senior director of product management at LexisNexis Risk Solutions UK. "This has driven the rise in the theft of information online. If you rely only on that information, it's self-fulfilling in terms of the problems it causes."

Part of the challenge relates to consumers who don't perceive their identity as having any value. Most people expect the identity verification aspect of accessing services to happen in the background and certainly don't think it's something they should pay for. To that extent, identity has become something of a commodity, yet one under constant threat.

More than nine billion[1] consumer identities were stolen in the last five years and identity fraud represents half of all consumer fraud, according to LexisNexis Risk Solutions.

While new regulations, such as the European Union's eIDAS set of standards for assurance checks related to electronic transactions, are beginning to recognise that identity needs to evolve for the online world, they still don't allow different signifiers to identify a human being outside of name, data of birth and address. It's clear this needs to change.

Internal processes at companies must evolve too. Before the internet transformed commerce and vital services such as banking, requesting name, date of birth and address was sufficient in preventing identity theft because they were very difficult to guess. Nowadays, however, obtaining that information is simply too easy for fraudsters, through either the details people willingly share online or from prior data breaches.

"The data breaches that have occurred have almost allowed the bad people to know that information," says Mr Weathersby, "and it allows them to go and commit other frauds. Because data has been breached, and digital services and information are easier to pass between two people, companies need to do more than just check that those pieces of information are real. They need to ensure who they're transacting with is that same person."

"Banks are already doing this, but because everyone isn't meeting a high standard, names, date of births and addresses are still valuable to fraudsters. We'll still experience other data breaches or fraudsters trying to obtain that information until everyone is ensuring it is not just correct, but also belongs to the person they're engaging with."

Stephen Topliss, vice president of product strategy at LexisNexis Risk Solutions, says: "There is so much of our data in the public domain, and the digital age provides such easy access to services and products, which are still generally relying on you validating basic identity information – name, address, date or birth – or other personal information. That means identity data is available and very useful, which is why the threat is so prevalent."

The greatest challenge companies face is balancing this need for secure identity verification and control over personal data with consumer expectations for a faster and more convenient digital experience. Simply adding barriers to authentication will do nothing to enhance the user journey at a time when customers are more likely than ever to abandon a transaction and buy somewhere else if their expectations aren't met.

This creates a very difficult situation for organisations and a hesitancy to implement additional security and assurance checks, for fear of jeopardising sales and product adoption. Consumers expect their data to be kept secure and they won't accept a slower or more complicated service to ensure that. The route to success is providing added security and identity assurance without harming the user experience.

"The journey of digital transformation that's occurring across businesses really needs to touch all parts of the organisation," says Dr Topliss. "If a new website is being launched, new services are being created online or a new app has been developed, they need to take the opportunity to embrace all the latest digital fraud prevention technologies as well."

LexisNexis Risk Solutions is a leading provider of such innovation, harnessing the power of data and advanced analytics to provide insights that help organisations reduce risk and prevent fraud. It advocates a layered approach, through a broad range of protection, acknowledging that no single method can stop identity fraud.

By implementing complex combinations of technology, including biometrics and passive authentication, companies such as LexisNexis Risk Solutions could make identity fraud nearly impossible. Those who do find a way will be deterred by the complexity, while consumers continue to enjoy speed and convenience because the technology is invisible to them.

The company's ThreatMetrix solution, in particular, looks at the digital identity of a person, including the device they're using, the location they connect from and the information they pass, such as user name and email addresses, enabling companies to perform both physical and digital identity verification. If the physical and digital identity don't match, organisations can quickly and easily identify suspicious activity that could be fraud.

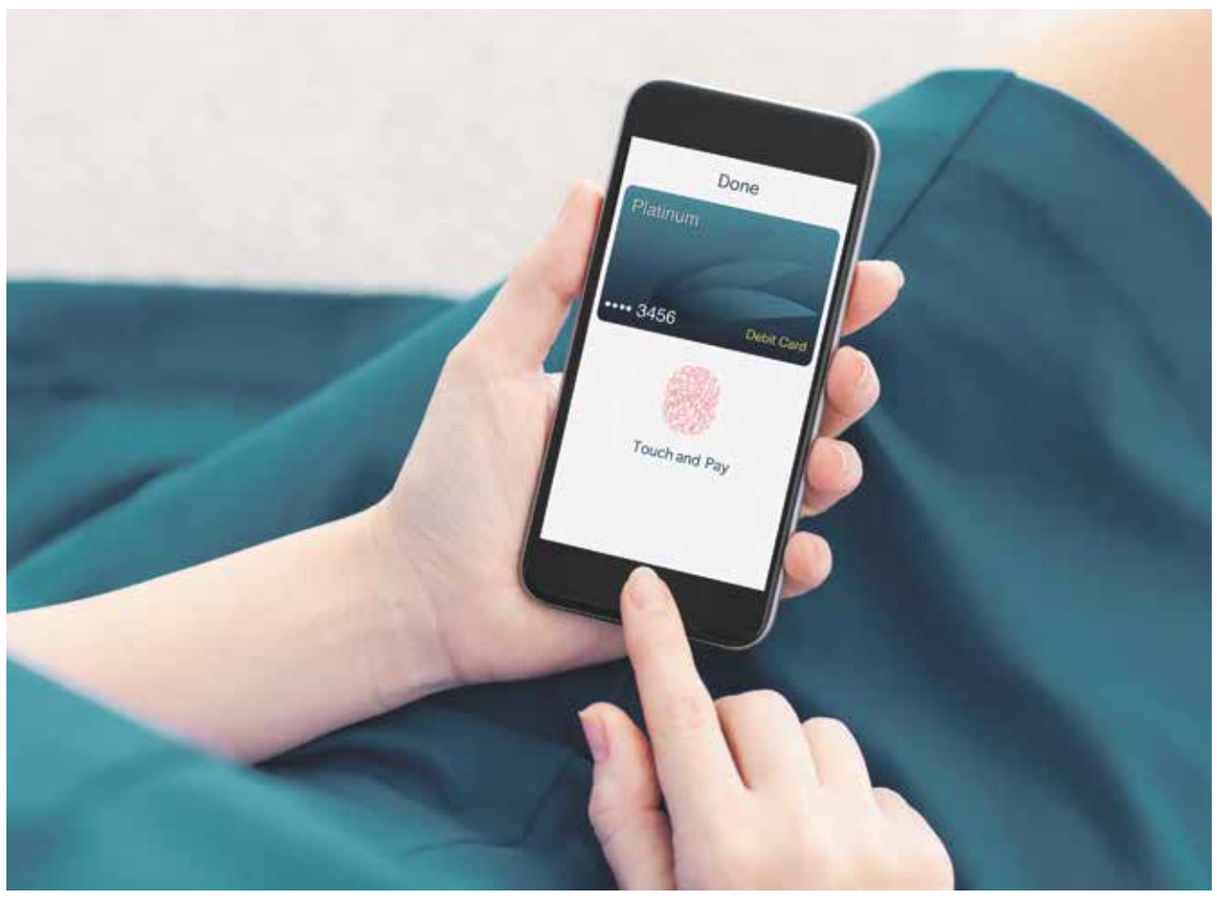
Digital intelligence and the concept of digital identities in particular, is still relatively unknown among the general public. Without the knowledge to understand how this technology works and what the benefits can be, some consumers are suspicious of the process.

"We have a responsibility to educate consumers and make them aware of the threats online," says Dr Topliss. "A lot of the tension over the last couple of years has been placed on marketing companies using digital data to track consumers to learn their spending habits online and then generate targeted adverts for them. This has influenced public opinion negatively around the use of digital data."

"It's important for consumers to realise a combination of this digital data, together with traditional identity data, can also be used effectively to combat identity fraud in the digital space and that their favourite shopping sites, services and social media networks are often making use of this type of fraud prevention services. This can help customers make a more informed decision around what data to share, or permissions to allow to a website, to help provide a safer and more secure online environment to transact in."

"The route to success is providing added security and identity assurance without harming the user experience"

1. *Gemalto's Breach Level Index*



HOW WILL NEW IDENTITY TECHNOLOGY IMPACT OUR LIVES?

My health

A modernised and sustainable health service that fits around you

You are able to securely access a qualified GP online, in minutes. With advancements in identity technology you can be securely authenticated by the system and have your medical records linked to you, allowing the GP to provide tailored medical advice, without the fear of your data and records being at risk.

My finances

Faster access to your finances, without compromising on security

You access your bank account from your mobile and the system uses a combination of biometrics and device identifiers to authenticate you, whenever and wherever you are. Not only is this more convenient but it also dramatically improves security.

My travel

Speed up airport checks without the need for paper documents or lengthy queues

You authenticate for flights, well ahead of travel, so that when you arrive at the airport, there's no need to carry out passport checks. New technology, including facial recognition, knows who you are and allows a smooth flow through baggage drop, security and flight on-boarding.

My shopping

Online shopping at a click without the need to be redirected for additional verification

You click to make an online purchase without the need to complete forms and you can do this across many online shops. You authorise a payment using your Digital ID and send your usual delivery address information quickly and securely.

Attack vectors evolve as fraudsters move to mobile

New research has exposed just how vulnerable the financial services, ecommerce and media industries, and more importantly their customers, are in the digital age, with cybercrime shifting towards cross-organisational fraud and mobile-first attacks

Companies across sectors that enjoy the most engagement with consumers online are struggling to keep up with fast-evolving attack patterns from fraudsters and the ever-growing networked footprint of cybercrime. ThreatMetrix, a LexisNexis Risk Solutions company, recorded 244 million human-initiated attacks and three billion bot attacks in the second half of 2018, according to its biannual Cybercrime Report. This included 189 million mobile bot attacks, a 12 per cent increase on the first half of 2018.

While new account creations have the highest attack rate of all use-cases analysed by ThreatMetrix, with one in eight rejected as fraudulent, the most noticeable growth in mobile attacks is on account logins. Attempts by fraudsters to infiltrate user accounts by brute force, with mobile bots, or stealth, using mobile remote access attacks, contributed to 107 per cent growth in mobile account takeovers in the period examined.

"Businesses must be able to piece together digital identity intelligence on a per-user basis so departures from trusted customer behaviour can be identified in near-real time"

With consumers increasingly opting to bank online and using mobile apps, financial services firms are under pressure to ensure integrated and low-friction digital authentication capabilities form part of the customer experience. Aligning security with the online experience that customers expect is crucial for the sector to advance.

Ecommerce is another industry where achieving that alignment is important while also maintaining effective fraud control, particularly during busy shopping periods such as Black Friday. This might mean accepting a higher percentage of fraudulent transactions to accept more genuine orders from good customers, which is a difficult decision to make.

ThreatMetrix detected and stopped 2.1 billion bot attacks on ecommerce merchants in the second half of last year, 142 per cent growth compared with the previous year. Although sophisticated attacks dropped, the impact of high-volume bot traffic continues to disrupt the sector. Identity-testing bot attacks often make up considerably more of an ecommerce merchant's daily transaction volume than good traffic, making a low-friction experience for trusted customers all the more challenging for merchants.

The media industry, which includes social networks as well as streaming, gaming and gambling sites, sees the highest penetration of new account creation attacks of all sectors, with one in six found to be fraudulent. Low barriers to creating and accessing accounts, along with less-stringent security measures, have made media a prime target for testing identities, so companies must be extra vigilant against fraudulent attacks.

In the period analysed, ThreatMetrix found the media industry was hit by 211 million bot attacks, 16 per cent growth compared with the first half of last year. The sector also saw 7 per cent growth in mobile new account creation attacks year on year, as well as an increase of 24 per cent on mobile payments transactions.

Fraudsters are master manipulators, with constantly shifting tactics, according to Alisdair Faulkner, chief identity officer at LexisNexis Risk Solutions. "They adapt their attack patterns and modus operandi to take advantage of shifting customer trends, evolving regulations and technological changes, always attempting to stay one pace ahead of businesses," he says.

"We see this through the way in which attack patterns evolve and morph over time. Businesses must be able to piece together digital identity intelligence on a per-user basis so departures from trusted customer behaviour can be identified in near-real time, before a transaction is processed and before fraudsters can operationalise new attack methods."

ThreatMetrix detected and stopped...

2.1bn

bot attacks on ecommerce merchants in the second half of last year...

142%

growth compared with the previous year. Although sophisticated attacks dropped, the impact of high-volume bot traffic continues to disrupt the sector.

For more information please visit risk.lexisnexis.co.uk

LexisNexis® RISK SOLUTIONS

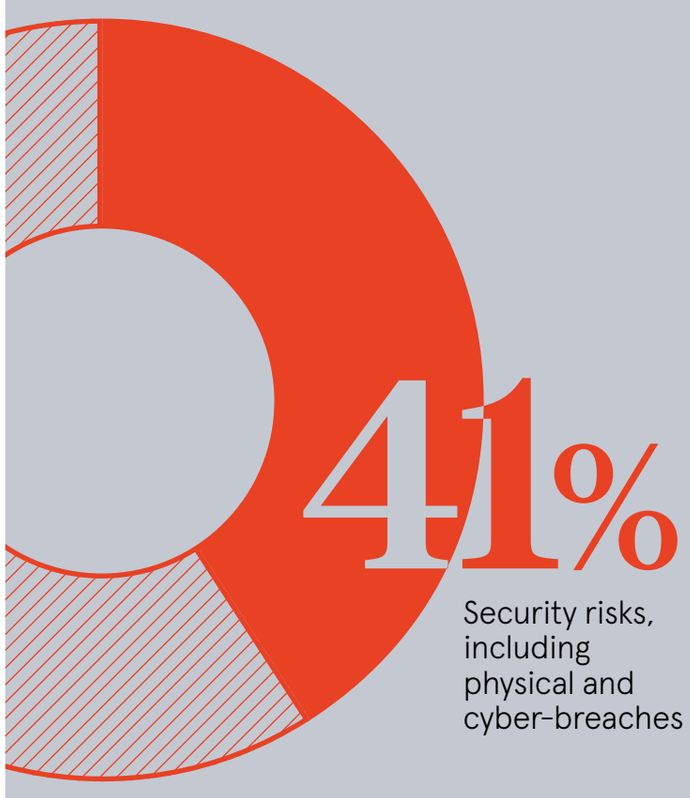
RISKY BUSINESS

THE IMPORTANCE OF REPUTATION

Warren Buffett famously said that a business's reputation takes twenty years to build but five minutes to ruin. In an age of hyper-connectivity and global suppliers, navigating reputational risk is now a multi-faceted challenge that stretches across all aspects of an organisation

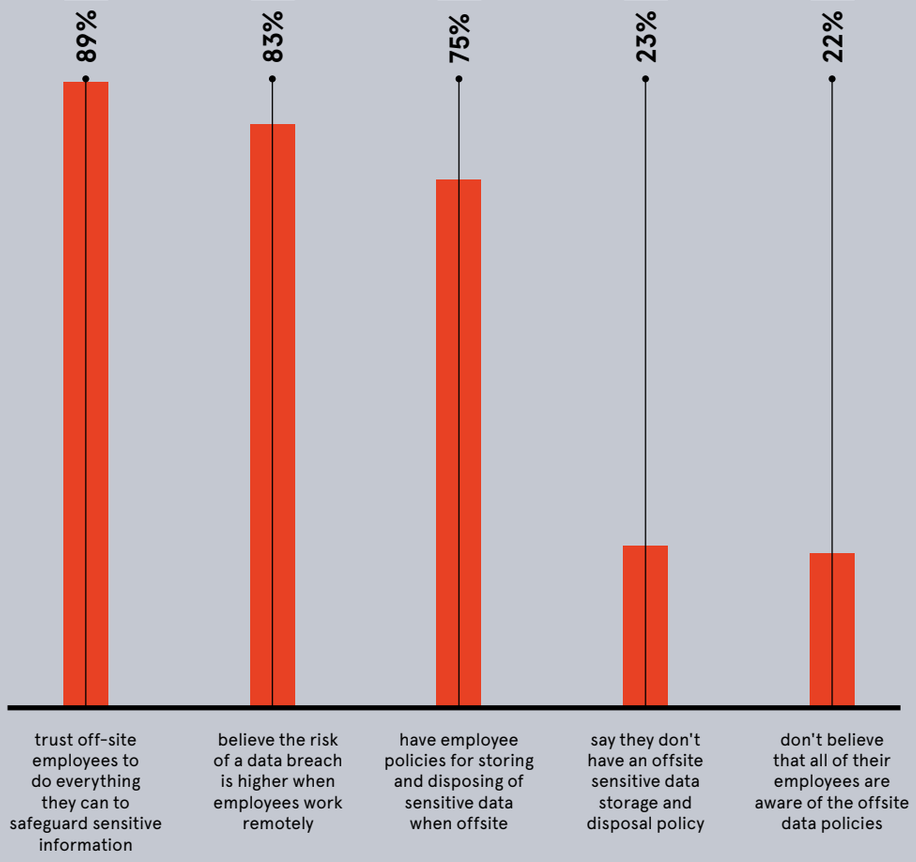
GREATEST REPUTATIONAL THREATS TO BUSINESSES OVER THE NEXT 12 MONTHS

According to a survey of chief executives



HOW C-SUITES VIEW THE RISKS OF REMOTE WORKING

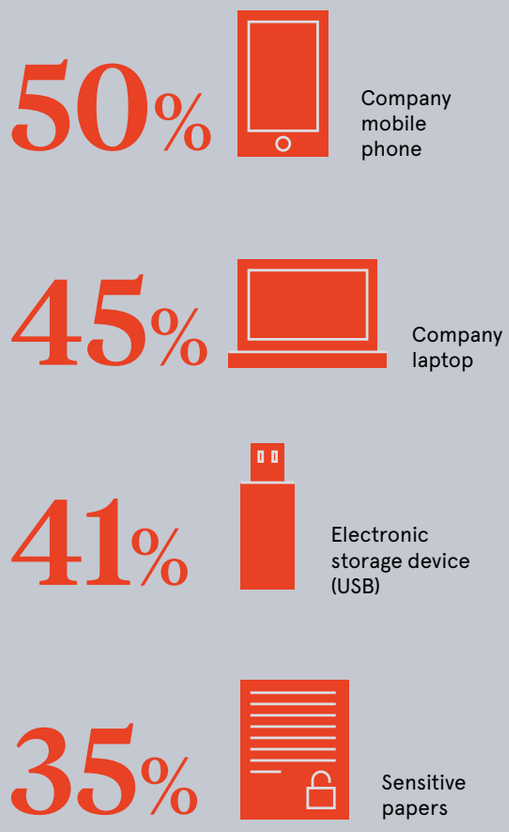
As more employees work remotely, an increasing amount of sensitive data is taken offsite, exposing organisations to risk. The following survey questioned C-suites about their strategies when it comes to remote working



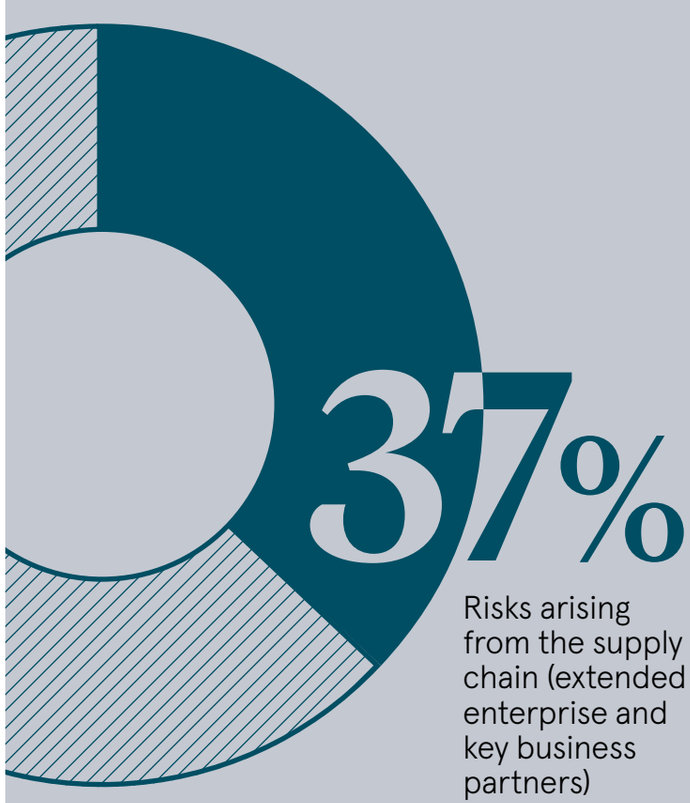
Shred-it 2018

SENSITIVE ITEMS MOST LIKELY TO BE LOST OR STOLEN WHEN EMPLOYEES WORK OFFSITE

According to a survey of C-suites

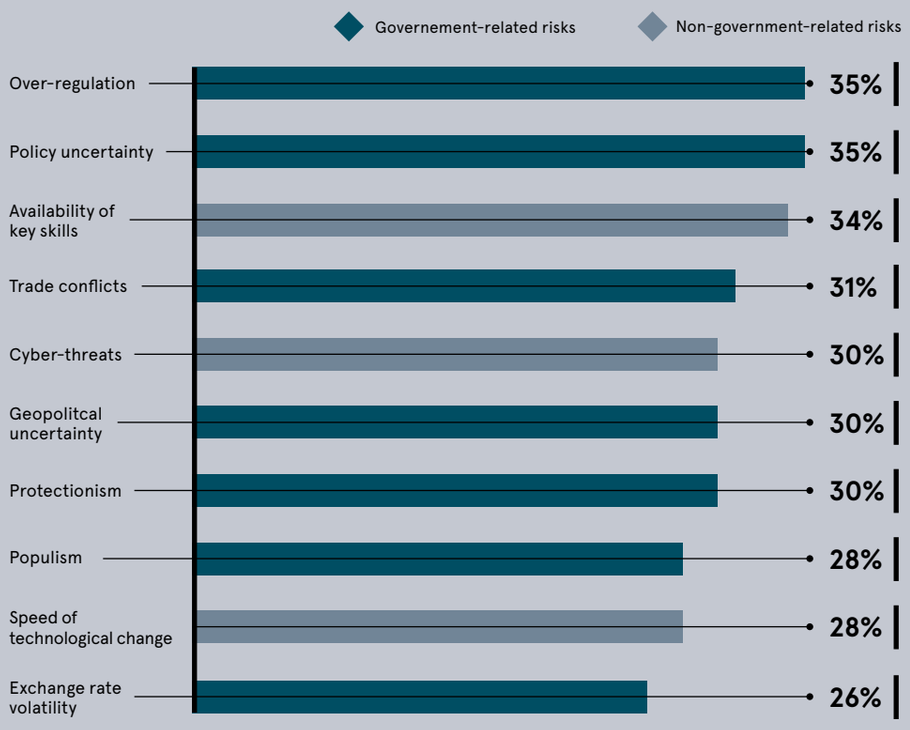


Shred-it 2018



TOP CONCERNS FOR CHIEF EXECUTIVES IN 2019

Governent-related risks such as protectionism, populism and trade conflicts are dominating concerns and forcing a rethink of sourcing throughout the supply chain



PWC 2019

BREXIT BORDER DELAYS CAUSING SUPPLY CHAIN RISKS

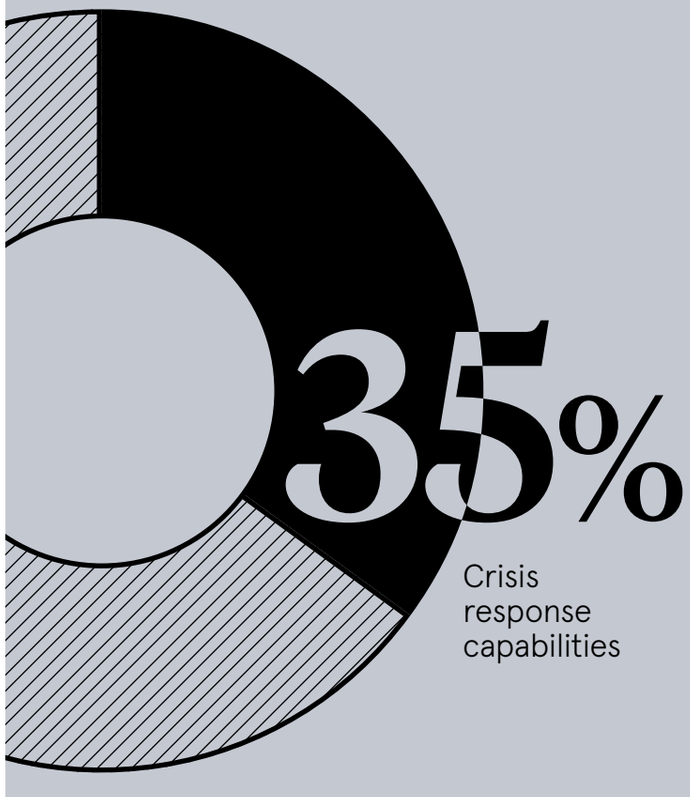
In the event of a no-deal Brexit, supply chain impacts could have a far-reaching and lasting effect on UK businesses

1 in 10 UK exporters could have contracts cancelled if there are border delays

2 in 10 EU businesses will expect a discount from UK suppliers if border delays persist for just one day

4 in 10 UK businesses would be able to export to the EU in the event of no deal as a result of EU customs requirements

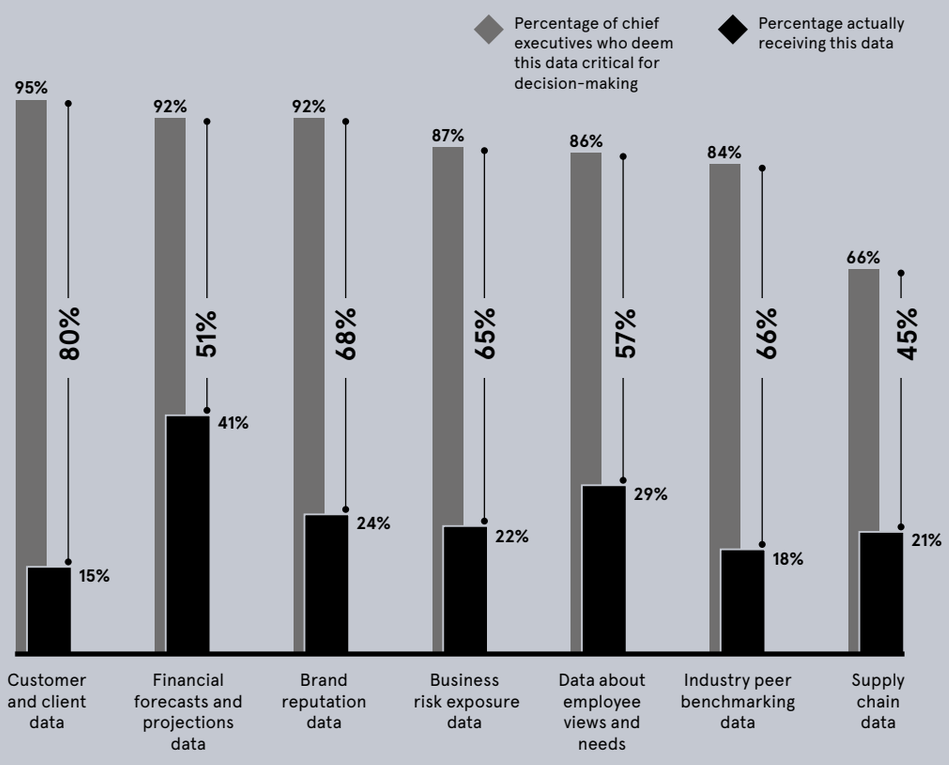
Chartered Institute of Procurement & Supply 2019



Deloitte 2018

CRISIS MANAGEMENT: VIEW FROM THE BOARDROOM

When it comes to crisis management, having access to the necessary data is vital for an effective response. Yet there is a significant gap between the data chief executives need and the data they have access to



PwC 2019

IMPACT OF CRISIS: BA DATA BREACH 2018

When British Airways announced their second data breach of the year in September 2018, the business impacts were instant and severe

Aug 21 - Sept 5 Breach occurred

380,000 customers affected

4% drop in share price when markets opened on September 7

£500m+ knocked off the airline group's market value

£488m potential maximum fine from regulators

£1,250 potentially avaliable in compensation to each customer claimant

Sept 7 Breach announced

Sky News 2018/SPG Law 2018

Commercial feature

Fighting financial crime with innovation and collaboration

A rapidly evolving regulatory environment and growing sophistication among criminals has elevated the cost of financial crime on both industry and society at large. Tackling the issue requires more innovative approaches and technology, but also greater collaboration

Financial crime has evolved. Anti-money laundering and counter-terrorist financing legislation is considerably stricter and the application of those laws has been extended to include designated non-financial businesses such as lawyers, accountants and real estate brokers. This means a broader set of organisations are obliged to conduct more intensive due diligence around their customers and the amount of work required to comply is increasing.

Other new regulations are mandating enhanced consumer privacy and protection, while consumers are demanding more choice and flexibility across digital channels, and technology advances are enabling new entrants in the banking sector with low barriers to entry. Amid these challenges, the digital identity revolution is gaining momentum as the need to protect against sophisticated financial criminals grows.

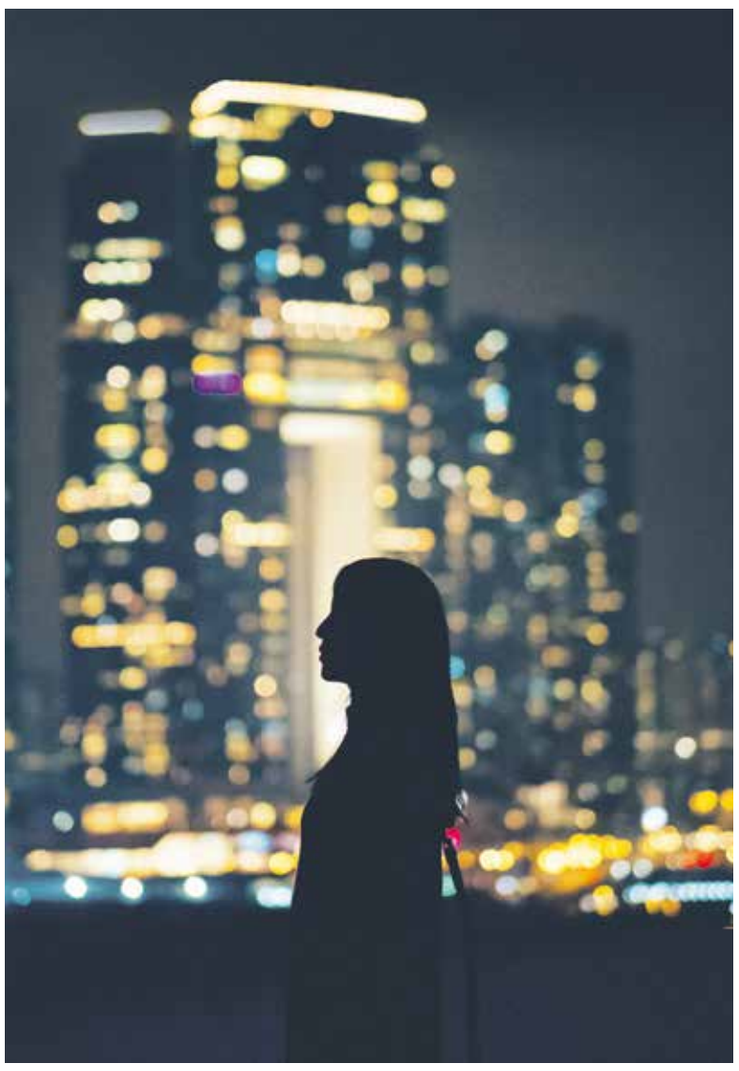
The True Cost of Financial Crime report released last year by Refinitiv, a global provider of financial technology and risk solutions, estimates that the loss of annual turnover from financial crime now totals around $1.45 trillion, equal to about 3.5 per cent of annual turnover. Companies spend more than 3 per cent of their turnover combating financial crime, according to the report which quizzed over 2,000 firms across 19 countries.

"When you look at the combined loss, it's huge and is getting bigger," says James Mirfin, global head of digital identity and financial crime at Refinitiv. "We're also seeing unintended costs from regulation. As banks start to perform more robust due diligence and seek to derisk their portfolios, there can be unexpected consequences, such as potentially putting customers at risk of losing access to financial services. We've all seen the headlines about money laundering and the impact of getting this wrong is significant, both financially, with the fines levied, and in relation to reputation too."

Massive amounts of data are created every day, but if banks and financial institutions don't have confidence in the data they're using, they're more likely to avoid higher-risk activities or customers and therefore withdraw products and services. This situation can be avoided by structuring and bringing together datasets and sources of data and solutions from companies such as Refinitiv to help organisations make more-informed decisions.

Moving away from traditional paper-based identity verification to embrace digital equivalents transcends geographies, and enhances both speed and efficiency. This in turn boosts productivity and means potential financial crime-related risk can be detected with greater accuracy.

There is growing recognition that approaches to financial crime mitigation are not working. While regulations have the right intentions, they don't necessarily have the intended effects. Europol estimates that just 1 per cent of financial crime proceeds in the European Union are actually confiscated. The number of suspicious activity reports flagged is soaring, but only 0.5 per cent lead into any meaningful investigation by law enforcement agencies.



> **We are committed to finding better ways to fight financial crime with the industry participants, providers, regulators and governments working together**

Greater collaboration in the form of public-private partnerships is helping to lead the line in finding better ways to tackle financial crime. The UK's Joint Money Laundering Intelligence Taskforce has seen major banks and law enforcement share and analyse information since its launch three years ago, while similar efforts now exist in Australia, Singapore, the United States and Hong Kong.

"You need to have the industry participants, providers, regulators and governments working together," says Mr Mirfin. "These partnerships are starting to work well, though they are still largely built around law enforcement and major financial institutions. The impact of financial crime is felt much more broadly, so there is an opportunity for wider involvement. The private sector needs to play a bigger role, contributing valuable expertise in areas such as artificial intelligence and data analytics to support compliance processes, but it's really a case of working together because when only 1 per cent of funds are being stopped, something's not working."

Last year, Refinitiv launched a global coalition to fight financial crime in partnership with Europol and the World Economic Forum. The coalition aims to improve awareness of the extent of financial crime, promote more effective information-sharing and establish enhanced processes to share best practice.

There is a common misconception that financial crime is victimless, but over 40 million people are trapped in modern slavery, more than ever before, with 25 million in forced labour and 15 million in forced marriage, according to the International Labour Organization and Walk Free Foundation. The proceeds of these crimes are often laundered through the financial system.

The United Nations Office on Drugs and Crime estimates the scope of money laundering is between 2 and 5 per cent of global GDP, which equates to between $800 billion and $2 trillion. It's clear that financial crime has many different victims, and the proceeds from bribery, corruption, human trafficking, drugs and fraud are hugely significant.

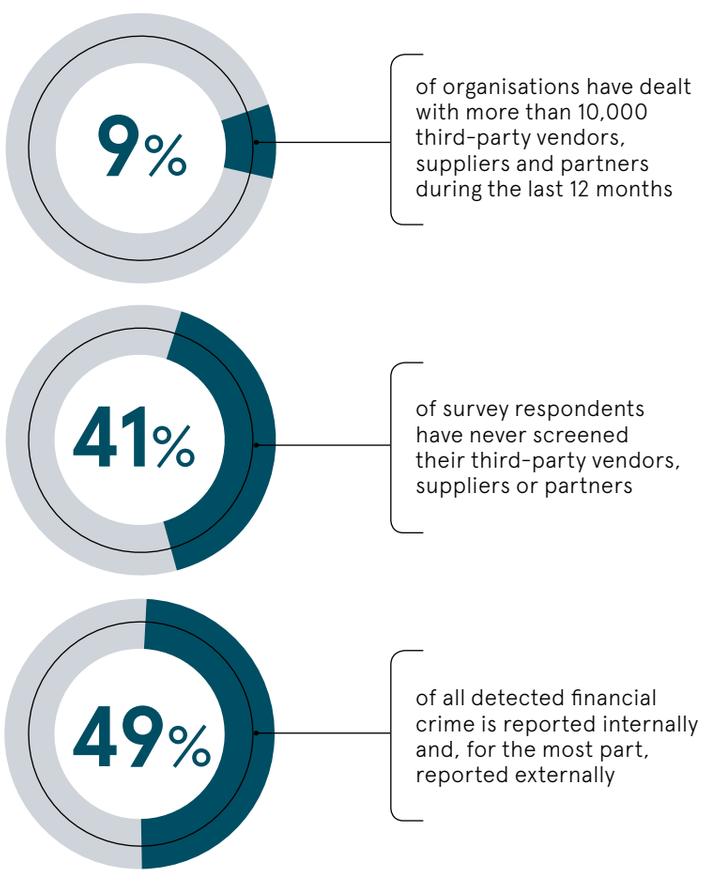
"Financial crime has very serious economic costs and very serious social costs as well," says Mr Mirfin. "It's causing massive harm and it's one of the reasons we're so focused on helping to fight this. As well as helping the financial institutions to meet with their regulatory obligations, it can have a real impact on people around the world.

"We're committed to finding better ways to fight financial crime, and that means continuing to invest in our products and solutions, including our multi award-winning World-Check One platform, but also participating in more industry forums and leading further cross-industry dialogue to ensure it gets the level of focus it needs. We help companies make better decisions around the types of customers and third parties they can support, and enable them to continue to offer services to legitimate customers so they have confidence about who they're dealing with."

For more information please visit refinitiv.com

REFINITIV™

HIGHLIGHTS FROM THE TRUE COST OF FINANCIAL CRIME REPORT BY REFINITIV



CRISIS MANAGEMENT

Keeping a lid on an explosive crisis

In the event of a crisis, business leaders must communicate effectively, with speed, honesty and compassion, in a bid to limit damage to their company

Nick Easen

The aftermath of a global corporate scandal is a very messy affair. Firstly, there's the breaking news, then the media frenzy, the plummeting share price, the evaporating confidence, the damage-limitation exercises and finally the grovelling executives. We live in a super-charged, hyper-connected environment, answerable to the 24-hour "churnalism" cycle and social media chatterati.

Boeing, Uber, Nissan, Huawei, Airbus or Purdue Pharma, to name but a recent few, have all had to step up like Winston Churchill to their darkest hour. "Crisis management can be like dealing with an explosion," explains Jo Willaert, president of the Federation of European Risk Management Associations.

And with any explosion, corporate or otherwise, everyone ducks away from the line of fire for fear of getting hit. Damage limitation can trump open communication. Slow and myopic group-think can stymy a crystal clear, crisis management plan because the stakes can be excruciatingly high and the fallout unthinkable. No one really wants to spark the next Lehman or Enron crisis. It would be career suicide.

"Be quick, honest, open and, in such circumstances, be compassionate in communications, these are the key principles of crisis management," says Julia Graham, deputy chief executive of Airmic, the UK's risk management body.

Yet time and again these messages don't seem to permeate the rarefied air of boardrooms or the upper corporate classes, and it shows. Whether it's Boeing's chief executive taking a week to respond to the fatal Ethiopian Airlines crash or BP's boss Tony Hayward making a quip during the Gulf of Mexico oil spill saying he "wanted his life back". The rapid, heartfelt response to an incident is as crucial today as it was ten years ago.

"An actual crisis is a pressure cooker and no time to start working out roles, responsibilities and processes for your management team. Yes, Mr Hayward apologised quickly, yet the damage was done and here we are almost a decade later still talking about it," says Marc Cornelius, founder of 8020 Communications, a specialist public relations consultancy.

At the heart of every response is an effective crisis response plan. Businesses are most resilient when they've already considered what to do if the worst happens and if all executives understand the roles they need to play. A risk manager coordinates decision-making teams that need to be multi-disciplinary, with all business functions represented, since they see situations from diverse angles.

"For instance, a classic tension can exist between legal and marketing perspectives: saying very little might theoretically limit your potential liability, but will the consequent damage to your brand end up costing you more long term? You can bet those functional tensions would have been going on recently within Boeing," says Mr Cornelius.

Time and again though companies are caught up in a crisis storm that is hard to weather. Facebook had its Cambridge Analytica moment, while Monsanto had to deal with a customer allegedly contracting cancer from its weedkiller, then there was Exxon's reaction to the Alaskan oil spill, the list goes on. The lessons that can be learnt are legion. Each event is unique and complex.

Rupert Younger, director of the Oxford University Centre for Corporate Reputation, thinks we need to go beyond our preparation manuals, rehearsals, box-ticking exercises and well-documented management plans, and instead create more of a wider culture of being able to respond to crises.

"Smart companies should spend as much time listening as talking, empathy and humanity are crucial. Each stakeholder has to feel well informed and properly looked after at all times, and internal teams need to be organised and focused on this," says Mr Younger.

One thing that a lot of crisis experts agree on is the crucial role that the executive leadership play in dealing with a crisis. Like the logjam over Brexit, markets and corporations look for certainty, any perceived loss of control, lack of solutions or uncertainty can cause real harm, especially in the early stages of an incident, and a lot of direction comes from the top.

A responsive C-suite is the new imperative, especially when key executives are increasingly being held accountable if their company is not able to respond to a crisis. Look at various governments' response to the live-streamed mosque attacks in New Zealand and their crackdown on social media companies for showing harmful content, from Australia to the European Union, including the UK.

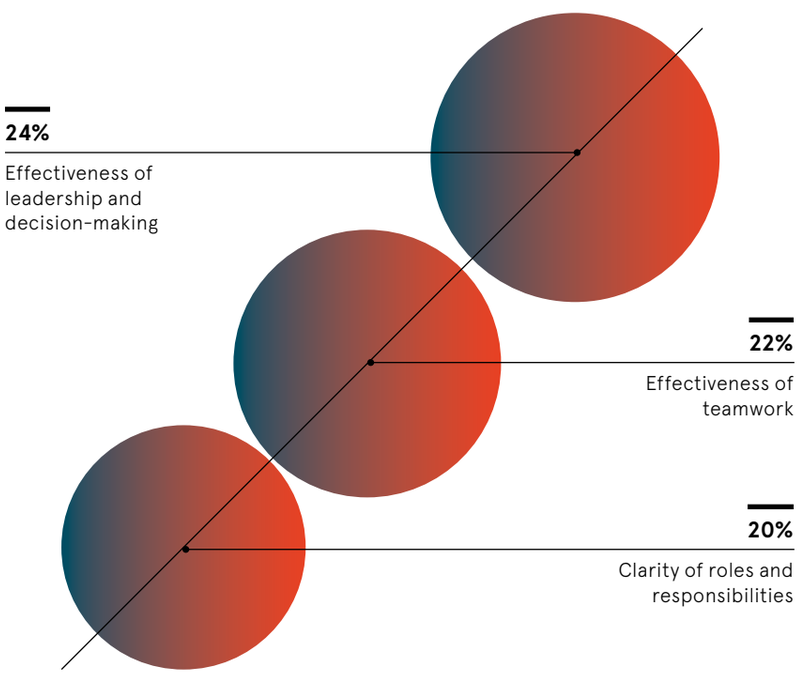
When management could be personally liable for these crises and fines could reach as high as 4 per cent of global turnover, as is the case under the EU's General Data Protection Regulation, it's enough to make any corporate board, from Twitter to YouTube, rewrite their crisis management plans and think twice about how they respond.

"Yet events usually outpace responses and without preparations or expertise at the table, leadership can find themselves frozen as they watch things unfold. The organisation needs to be clear on who takes the lead in efforts to restore the confidence of the public, clients, employees and investors," says Erik Petersen, head of crisis management consulting in Europe at Control Risks.

"The issue is that leaders will often be required to make decisions with insufficient information. It can take days or

EFFECTIVELY RESPONDING TO A CRISIS

Organisations believe the top three significant challenges to an effective crisis response are



Deloitte 2018

Five top tips when a crisis hits

01 Take ownership

Don't wait for the crisis to take hold. Look at your company right now and determine if the response capability is fit for purpose. Risk management is the mother of crisis management. Also take ownership of a crisis when it occurs, otherwise the vacuum will be filled by speculation.

Marco Restivo/Getty Images

sometimes longer to get facts or understand the nature of the problem, while stakeholders will demand immediate answers and a response."

The fact is most of us trust corporations around the globe without knowing what kinds of systems they have in place to deal with risk, safety and incidents that involve people's lives, health and wealth. We eat, fly, drink, drive and consume various products from countless companies that we put our utmost faith in. The question is, can we really trust them?

"Companies that manage risk well tend not to face crises of their own making," says Sandra Sucher, professor of management practice at Harvard Business School. "In my research, I've found a close association between sound risk management and being trusted. Risky actions lead to mistakes of many kinds, and we mistrust, with good reason, companies which don't seem to appreciate the consequences of their mistakes and fail to anticipate the risks that things could go wrong."

> **Be quick, honest, open and, in such circumstances, be compassionate in communications, these are the key principles of crisis management**

Another aspect that's crucial is crisis communication and the language used. "It is arguably becoming one of the most important elements of damage limitation in an era where harm to brand and reputation is the greatest part of the impact," says Mr Petersen.

Increasingly, big corporations value the role of crisis communications, they also understand that it's a specialised skill either to be cultivated in-house or via an outside consultant who knows the business well and is on call. "Those organisations that don't value communications, do so at significant risk," says Kelli Matthews, senior instructor at the School of Journalism and Communications, University of Oregon.

Many crises that whip through the media are hardly binary affairs, they are infinitely complex. The key is to make these issues simple and communicate in plain, unambiguous language. "This can be really challenging," says John Martin McDonald, founder of Caeli Communications. "As Mark Twain once said: 'I didn't have time to write you a short letter'. But you must make the effort and do it throughout the crisis."

All this underplays the role of the risk manager, yet they are a crucial go-to person in any crisis. They have a pivotal role to play, since the impact of a crisis can touch many facets of a business from customers to shareholders, affected communities to supply chains.

"The professional risk manager serves as a co-ordinator across many functions that need to be involved in a situation like this, both for the manufacturer and the airlines in the case of the Boeing crisis," says Typhaine Beaupérin, chief executive of the Federation of European Risk Management Associations. "The risk professional will also play an important role in managing the complex insurance issues that will inevitably arise as a result of a crisis."

It's not all doom and gloom. Many businesses can be resuscitated over time. "A company's reputation is not earned over night and, usually, not lost over night," says Marc Szepan, lecturer at the University of Oxford Saïd Business School.

But beware, a recent study by *The Economist* of the eight most notable corporate crises since 2010, including those at Uber and Wells Fargo, found that the median firm was worth 30 per cent less today than it would have been had the scandals not occurred. Ouch.

Crashing into a crisis

In the grip of a global crisis, following two major air disasters, Boeing is grappling with how to recover public confidence and restore its reputation

Not a week goes by when there isn't fresh news on the crisis that is engulfing Boeing, one of the world's largest aerospace companies. With it's top-selling aircraft grounded globally after two disasters, one in Ethiopia and the other in Indonesia, which left 346 dead, the fallout continues. The incident is played out in the press, on TV and web pages as the chain of events is scrutinised.

Lawsuits are now in the offing, accusing Boeing of putting "profits over safety", and software problems have been identified while the media attention has badly shaken the public's confidence in the safety of the 737 MAX aircraft, a workhorse of the global aviation industry.

"It is highly unlikely that Boeing will be put out of business by the fatal crashes. But that doesn't mean it will be trusted in the same way as it was before," says Sandra Sucher, professor of management practice at Harvard Business School.

Already analysts and risk consultants are weighing in on how Boeing initially reacted to this complex incident that involves the US Federal Aviation Administration, crew and technology interactions, as well as stalled responses to the Ethiopian Airlines crash from the offset. It does not help that the actual root causes are only just beginning to surface, weeks after the event.

"The company was too slow and too focused on themselves. It's hard to regain the public relations initiative if the start has been handled badly," explains Rupert Younger, director of the Oxford University Centre for Corporate Reputation. "Their first response was legalistic and engineering-based rather than focused on the tragedy and loss of life. There was no empathy, a lack of humanity and an inappropriate internally focused response."

How Boeing then handled the unfolding crisis gives some insight into the internal workings of the company. It raises questions on many fronts, including how it handles risk, implements crisis management plans, action from leadership and a co-ordinated response to stakeholders.

"These events portray a picture of corporate confusion and absence of cohesive crisis leadership. Boeing's response created a communications chasm that was filled with negativity," says Julia Graham, deputy chief executive and technical director of Airmic, the UK's risk management association. "The company was seen as uncaring and more interested in their business than the people their aircraft carried around the world, despite the high regard globally for Boeing's engineering community."

> **The company was seen as uncaring and more interested in their business than the people their aircraft carried around the world**

Whatever inquiries reveal over the coming months, corporate trust has been lost and reputation has been damaged. At some point Boeing will have the opportunity to state clearly what happened and what they will do about the 737 MAX aircraft to regain business confidence.

Let's not forget the 737 has been in the air more than 50 years in some iteration. The aviation company still holds an immense, multi-billion-dollar order book for this new version. Boeing will need to do something. "This will be a critical credibility moment for the company and its senior management team. Handling this well will be a major test for the leadership team," says Mr Younger.

If you think it's nearly over, think again. Share prices have taken a hit, yet Boeing is not a business-to-consumer business. You and I don't buy planes, but we are passengers on flights. Ignore the end-consumers at your peril.

"The Lion Air and Ethiopian accidents carry the risk that the 737 MAX becomes like the DC-10 of the 1970s, which was so associated with disaster that the public would actively avoid it. For Boeing, therefore, the general public is also now a core constituency," says Marc Cornelius, founder of 8020 Communications. "The 737 MAX is probably the most well-known aircraft in the world right now and Boeing doesn't want it following the DC-10."

We all take it on trust that our chosen airline will be flying a safe aircraft. Boeing take heed. "I flew today and the gentleman behind me made a comment to the effect of 'well at least we're not flying on a 737 MAX'. That's a problem for the company," says Kelli Matthews, senior instructor at the School of Journalism and Communication, University of Oregon. And so the saga continues.

Andrey Larin/Unsplash

02 Put people first

A crisis generally means someone's life has been affected. Being compassionate, empathetic and genuine in all your corporate actions and responses is crucial. Be as interested in listening as in talking. No company wants to be branded as uncaring, putting profits and business before peoples' lives.

03 Communicate

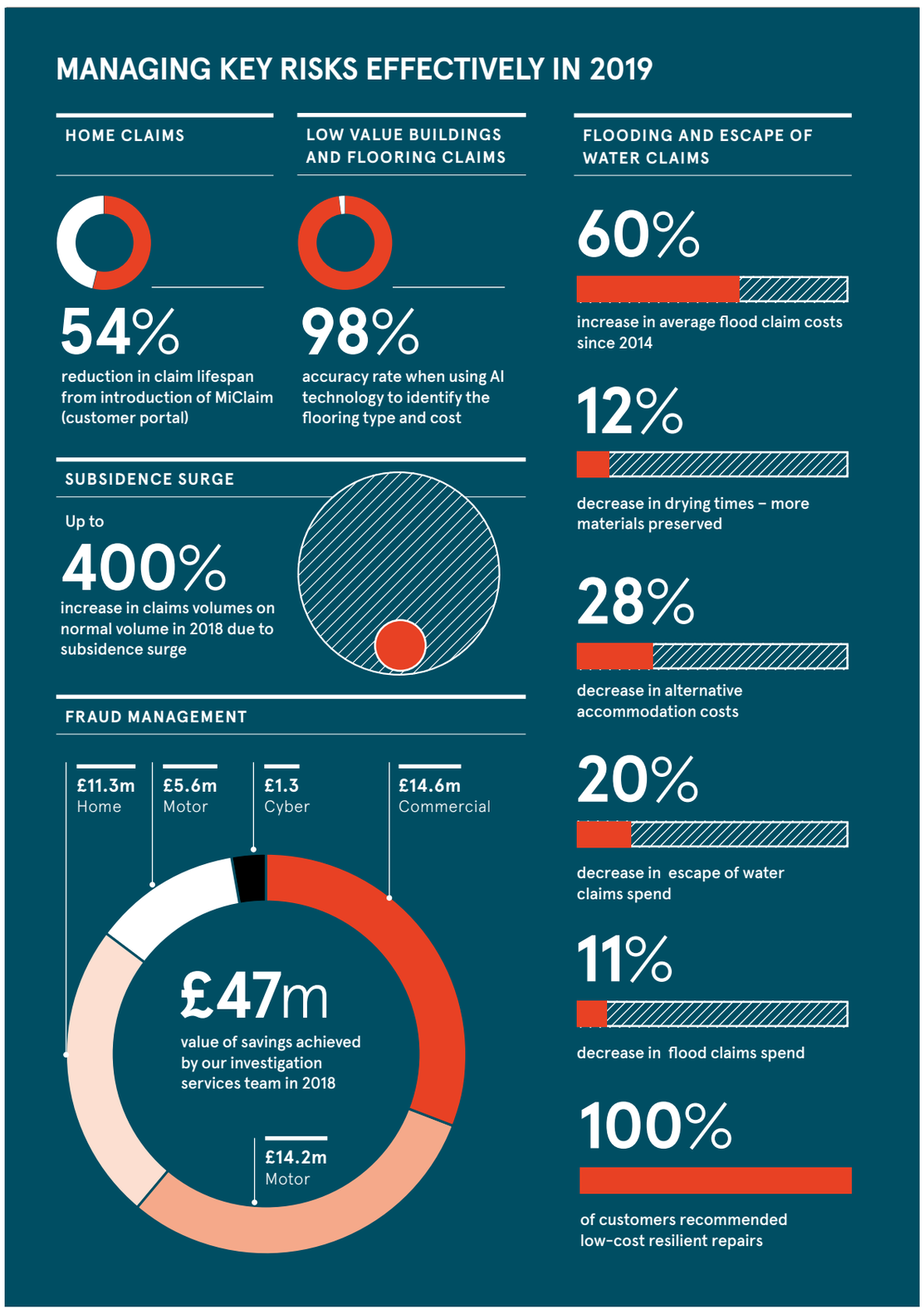
No one expects a perfect response, but they do expect action. There are many ways to respond effectively without having all the answers in a crisis, if only to demand action as a corporation; don't let lawyers slow a response down. People need to know you care before they care what you know.

04 Respond immediately

In today's social media frenzy and 24/7 news cycle, bad news travels around the globe in a matter of seconds. Reputations can be sullied within seconds. Confusion and misinformation can take hold quickly and be amplified. Responses must be immediate.

05 Invest

The cost of crises can now be regularly measured in the billions of dollars or pounds. Some companies or brands have ceased to exist following a scandal. If you are, say, spending £25,000 a year on crisis management capability, it's worth considering whether this is appropriate.



Facing business risk in an interconnected world

The seemingly unstoppable rise of globalisation has opened up countless new markets for businesses and unlocked highly profitable economies of scale. But this interconnected world also exposes companies to a multitude of risks that threaten their ability to do business

Cyber-risks may have been around for many years, but they remain a constant danger for firms of all sizes with ransomware, phishing, data loss and hacking having the power to bring operations to a standstill.

"Cyber-related business challenges have grown considerably over the past decade," says Stewart Steel, chief executive of Sedgwick UK, a leading global provider of technology-enabled claims and productivity management solutions. "It's clearly something that's here to stay, as many major businesses are suffering from repeated cyberattacks on practically a daily basis."

Complex supply chains, the impact of Brexit and climate change are requiring companies to adopt the most effective solutions to mitigate and reduce risk, with having the right management team in place to combat these challenges quickly and effectively being vital.

It's more important than ever to make sure that larger organisations have a talented risk management team in the business, which are able to not just moderate risks, but also ensure there is a comprehensive plan in place to deal with the immediate aftermath of loss.

"Beyond the internal resources, a trusted global broker who is able to explain the risks and challenges that are likely to be faced in certain territories is key as they will likely have more knowledge in this area than you, as the policyholder, might," says Mr Steel.

By nominating loss adjusters to global programmes as early as possible and allowing them to work with the risk management team to plan loss, relationships can be built that ensure if loss happens a robust business continuity programme can be implemented.

Mr Steel believes that to prepare for threats around reputational risk, alongside enterprise risk management, it's important to line up other talented partners who have global penetrations, including a PR firm, which may prove vital around cyber data-breach risks.

"A competent law firm is usually required because fundamentally there's often a legal aspect to the possibility of recovering outlays from another party," adds Mr Steel.

Artificial intelligence (AI) and machine-learning solutions, too, are beginning to speed up the claims process for policyholders, and help them to self-serve and handle their claims at a time that suits them, rather than having to wait until the various insurance and supplier offices are open.

Being able to take cost out and reduce unnecessary customer service costs for insurance companies would, in turn, have a beneficial effect on the premiums the policyholders pay. Perhaps most importantly for businesses, the power of AI to process claims quickly will enable them to move on immediately from the impact of a risk that damaged the firm.

"If you look at the way many insurance companies are set up, quite a few are already using AI to handle claims. A few of the insurers we have dealt with have said claims of less than £2,500 may soon go through the claims process with no human intervention at all. From a supplier perspective, we are building processes and systems that mirror and match the AI process," says Mr Steel.

> **Thanks to our extensive global network, we have at our fingertips practically all the expertise that any global corporate would want or need when facing pressing business risks**

It's getting more difficult for insurers to keep pace with the rate of digitalisation, due to the significant cost involved and lack of adequately skilled technology professionals.

"There are some smaller insurers that are already considering either getting out of the market completely or looking towards companies like Sedgwick to offer a faster better, slicker, more customer-focused experience to enable them to grow in the sector, which otherwise would be risky for them to do with their own capital," says Mr Steel.

As the world's largest loss adjusting and claims management company, Sedgwick's 21,000 staff in 65 countries are well placed to offer their technical expertise and vast practical experience to benefit their clients at every stage of the risk management process.

Sedgwick has been involved in dealing with the majority of major global catastrophes, allowing them to bring a considerable amount of post-loss expertise to help organisations plan for the worst-case scenario.

"Within the Sedgwick organisation we have a forensic accountancy business, which is beneficial if you're looking at mitigating losses from interruption risk that may flow from outside your business and involve, for example, a supplier," says Mr Steel.

Emerging risks, including extreme weather-related problems and the rise of terrorism, will continue to challenge how many global businesses operate. Even moderate weather events may require preparation to ensure there are no issues in continually operating.

"In this situation it could just be something as simple as getting your senior management together and considering what could happen in the worse circumstances, and then creating what we call a 'grab bag'," says Mr Steel.

A grab bag should hold all the information that is needed to get out of the office as quickly as possible and then put steps in place to start the process of recovering the business, including preparing back-up facilities, so the company can still provide a fundamental service for customers.

Forward-thinking businesses need to be considering how they would manage complex situations that require skills and expertise not available in their own company.

"Thanks to our extensive global network, we have at our fingertips practically all the expertise that any global corporate would want or need when facing pressing business risks," Mr Steel concludes.

For more information please visit www.sedgwick.com/uk

sedgwick®

Commercial feature

CULTURE

Why CEOs need to be chief culture officers and lead from the front

Chief executives must be flag bearers of brand reputation in the face of potentially damaging cultural risks

Karam Filfilan

A toxic culture creates a variety of risks for a business. From reputational damage brought on by revelations about employee conduct to the corrosive influence of issues around discrimination and employee wellbeing, a poor culture can rapidly sink a brand, particularly in an age when social media amplifiies every misstep.

Despite this, businesses are failing to read the warning signs. A 2018 survey of 400 US chief executives by Deloitte found that while leaders were focused on the risks of technological disruption and digital transformation, fewer than half (42 per cent) had discussed risks to brand reputation in the previous year and 53 per cent couldn't even identify what those risks were.

It's time for chief executives to step up and embody the culture they want their business to have. By leading from the front, and crucially creating a culture that fits their business, they can mitigate cultural risks and create a more resilient and engaged workforce. But what are the challenges?

No culture, no strategy

It may have become a cliche, but the late Peter Drucker's famous quote "culture eats strategy for breakfast" still applies. If not enough time is invested in researching, creating and implementing a culture that fits a business, then all subsequent strategising is at risk.

"Cultural questions are as essential to strategy-shaping, planning and execution as the business case," says Jan Tregelles, chief executive of UK learning disability charity Mencap.

On taking over in 2014, Ms Tregelles and her leadership team identified the culture they wanted their people to demonstrate at the same time as building the strategic aims of the charity. Culture change was a big part of setting the charity on a new strategic direction.

She says her leadership team chose to define the organisation's culture by prioritising two capabilities – customer connectivity and collaboration – that were considered essential to future strategies. Then, it was up to them to lead by example.

"No one individual defines and leads the culture of an organisation; it develops through all its people. Trying to create one homogenous culture that everyone sticks to is futile. What you can do is encourage people to coalesce around some key principles," she adds.

Mental health is a corporate risk

Research by mental health charity Mind found that 48 per cent of people have experienced a mental health problem in their current job, while figures from the Health and Safety Executive suggest 15.4 million working days were lost to issues around stress, depression and anxiety between 2017 and 2018. This is the first time work-related stress and anxiety has accounted for more than half of all absences.

"As businesses, it's our responsibility to admit that the way mental health is spoken about is wrong and we must be active in changing it. It's a business issue in that we're wasting a group of talented people who feel businesses aren't supporting them," says Josh Krichefski, chief executive at MediaCom UK.

To counter this, MediaCom has appointed more than 160 mental health allies, who are trained in dealing with mental health issues. They are identified by green lanyards and name badges, and are there to listen to any concerns colleagues may have.

"As a leadership team, we know it's important to lead the way. One of our first initiatives was to ask our employees to openly share experiences they've had with mental health. I shared my own story and many in the leadership team did too. It felt like a barrier had been lifted," says Mr Krichefski.

Identifying diversity differences

Analysis of the recent gender pay figures released in April shows that fewer than half of employers surveyed have reduced their gender pay gap in the last 12 months. In fact, 45 per cent of the 10,428 companies that submitted figures actually saw an increase in the pay difference between men and women.

It's not just equality of pay between men and women where boardrooms face diversity issues. At its current rate, the UK's FTSE 100 will take until 2066 to meet a government-backed target of having a least one BAME board member when the initial target was 2021, while a 2018 report by LGBT rights charity Stonewall revealed that 35 per cent of members don't feel included at work.

Put simply, very few of our businesses accurately represent the customer base they're trying to attract. This can only be dangerous for the future.

"I do believe the government's gender pay gap legislation will help with gender equality, but there is a bigger cultural issue that needs addressing," says MediaCom UK's Mr Krichefski.

"We can put all manner of targets and legislation in place, but if the attitudes, beliefs and behaviours of a business and its people don't change, we'll never be open to all. Leaders cannot be distant and hierarchical if we want to establish a culture that empowers our people to deliver the best work they can," he says.

Need for 'glocalisation'

"It isn't easy to define culture, but in the globalised economy in which we now live, what is common and accepted in the UK could be very different for a colleague and customer in Singapore or India," says Porteur Keene, founder of executive search firm The Art of Talent.

Failing to adapt global business models to local markets is a common error that affects all businesses, no matter how large they may be. Consider the case of Uber in the Middle East market. Despite its dominance elsewhere, Uber found its market share there eaten up by local ride-hailing app Careem. The difference? Careem continually updated its product based on local considerations, such as call-masking passengers' phone numbers from drivers, introducing cash payments and allowing pre-scheduled bookings years before Uber implemented the feature. The outcome? Uber spent $3.1 billion buying Careem earlier this year.

To mitigate the expensive risk involved in moving into new territories, chief executives must abandon the one-size-fits-all approach to business and instead focus on a "glocal" mindset, a hybrid of global and localised approaches. The starting point should always be the needs of the local market, backed up by allowing local hires to implement a culture appropriate to the region with the support of the leadership team.

Risk of stagnation

According to a 2017 study by the Yale School of Management, the average lifespan of an S&P company in the United States has fallen from 67 years in the 1920s to just 15 today. In an increasingly volatile and complex world, the biggest risk most companies face is failing to adapt to change and stagnating.

For chief executives, this is often about embodying a culture that is open to change. Here, much can be learnt from the agility and resilience startups show.

"A startup is there to constantly evolve and figure out what the team should create for a happy customer, and that culture of questioning and innovation runs deep," says Dan Murray-Serter, serial entrepreneur and co-founder of Dawn, a "human potential company", which provides content, community and products geared towards optimising cognitive performance.

"If you empower smart people with a mission, make it clear why the goals are there, what the timeframes are and that you don't know all the answers, but value their input, it's hard to go wrong," he adds.

Leaders of larger businesses can start by understanding that strategy delivery is just as important as strategy design. By taking ownership and being accountable for the implementation of new ideas, chief executives can demonstrate that innovation is central to the company's mission. For many organisations, this can be the difference between mere survival and actual growth.

ENVIRONMENT

Business as usual is no longer enough

As the effects of climate change increasingly make themselves felt, successful companies will future-proof their business and limit further environmental damage

Jim McClelland

From Hurricane Katrina to bee-colony collapse, or city smog to ocean plastic, the environment keeps making the wrong kind of headlines. The impact is sometimes sadly fatal, often irreparably harmful, but always bad for business.

"Climate change, biodiversity loss and natural-capital degradation pose new, often unquantified, risks for businesses, as well as systemic risk to the economy," says James MacGregor, environmental economist at Ramboll.

As evidenced by rising momentum behind the Task Force on Climate-related Financial Disclosures, institutions and corporations are increasingly aware of these risks. There is also growing demand for environmental, social and governance investment criteria from creditors, customers and shareholders.

The risk is real and recognised as such. In the World Economic Forum *Global Risks Report 2019*, environmental concerns dominated results of the *Global Risk Perception Survey* for the third consecutive year. They accounted for three of the top five risks by likelihood and half of the top ten by impact, with extreme weather not surprisingly ranking highest.

Some sectors are already realising the reward-potential inherent in this redirection, says Trevor Hutchings, director of strategy and communications at Gemserv. "Climate change and environmental drivers are transforming markets," he says. "The debate has moved on from mitigating business risk to seizing opportunities that come from disruption."

In the transition to electric vehicles, for instance, Mr Hutchings sees innovative companies such as Zap Map and Charge Master entering this space, as well as more traditional companies upending their businesses models.

Working together to tackle structural issues is also increasingly popular. Gemserv has launched proposals for an industry-led electric vehicle governance framework to enable cross-sector collaboration and a co-ordinated market-led approach to the challenges.

Ultimately, though, it is adapt or die, says Mr Hutchings. "If businesses are not willing to change, they may not be able to participate in the market to the same extent," he says. "Any lack of data, metrics and tools is not an acceptable excuse for inaction."

The do-nothing option is essentially being eliminated in favour of embracing change that can positively affect the environment, while successfully managing risks, argues Rowena Sellens, chief executive of Econic Technologies. "In the past year, we have seen the balance of decision-making shift, with sustainability impact now more of an equal driver alongside pure economics," says Dr Sellens.

The turning tide of public opinion has been influential. She adds: "Businesses, large or small, are made up of people who'll have read the shocking news reports, seen the images on the television and heard the warnings of scientists.

"Businesses are not divorced from the concerns of the population as a whole; they will be riding the green wave because the shareholders, managers and employees care about the planet. It's a natural, organic shift in attitude."

As a result, innovation is rife. Developments in catalytic science, for instance, now make it possible for Econic to create a range of better-performing and more biodegradable plastic products out of CO_2, while also reducing emissions and costs.

What Econic is doing with chemicals and plastics, innovators such as Deep Branch Biotechnology are developing elsewhere for the feed industry. Their single-cell protein uses carbon dioxide from industrial waste gas to provide sustainable alternatives to soy and fishmeal.

Tackling textiles waste to landfill is another risk-to-opportunity scenario, at the forefront of a circular-economy awakening, says Cyndi Rhoades, founder and chief executive of Worn Again Technologies.

"The game-changers on the horizon will be the new wave of chemical-recycling technologies. These take low-value, non-reusable products and turn them back into virgin-equivalent raw materials at the same price, if not less," she says.

Almost by definition, of course, entrepreneurs are problem-solvers and risk-takers. The new breed, though, have grown up with the environmental legacy of previous generations and know we cannot continue with the status quo, says Steven Hess, trustee and programme lead at The Startup Leadership Program. "The next generation of entrepreneurs combine purpose, profit and people into exciting and world-changing ventures," he says. "In the 21st century, you cannot separate the three."

Pioneers include Taste of Kenya that owns its entire supply chain in sustainable tea and coffee or Made in Britain champions Naturally Tribal, a chemical-free skincare brand, which sources ingredients direct from Africa.

For this burgeoning startup ecosystem, bringing with it a paradigm cultural shift towards the environment and sustainable, transparency will be key, says Mr Hess. "As the digital revolution continues to open the bonnet on all business activities, consumers, shareholders, the media and activists are able to hold companies to account," he says. "Every sector, from energy to finance, transportation, media, technology and tourism, is being disrupted."

The same digital analytics, insights and data also support more comprehensive and conclusive decision-making, in general and on sustainability matters, says Andrew Frost, executive director at compliance and regulatory experts Lawson Conner. "Technology and software has drastically improved the ability to manage business risk," he says. "This allows firms to account for important and potentially unforeseen environmental considerations."

But this step-change in what all parties can affordably know and measure means no going back, says Ramboll's Mr MacGregor. "The current changes herald 'the end of greenwash', as more informed consumers challenge company and government decisions with evidence that is easier to obtain digitally," he says.

"For many businesses, though, truly transforming and disrupting is a big ask, solely from climate risks. And there will be losers. Companies and business models that can't adapt, won't adapt."

However, there will be winners, notably the planet, concludes Jeffrey Milder, director of global programmes at the Rainforest Alliance. "Our food system used to be based on endless expansion, but that no longer works," he says. "The world's remaining forests, grasslands and wetlands are needed to protect biodiversity, store carbon and support local communities.

"Major food and agribusiness companies now recognise this and are leading a profound shift to freeze the footprint of food. There is new hope that responsible business can help protect the world's last great biomes, such as the Brazilian Cerrado."

Survival is the prize, not just in the natural world, but the business one too: "business as usual" is an endangered species.

> **Businesses will be riding the green wave because the shareholders, managers and employees care about the planet**


Daniela Dirscherl/Getty Images

UK CORPORATES' ATTITUDES TOWARDS CLIMATE CHANGE REPORTING AS A REPUTATION DRIVER

72% believe climate-related reporting will increase brand value

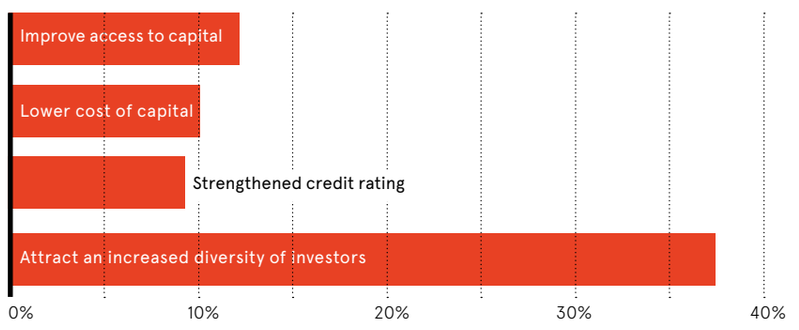
67% will disclose climate-related risks and opportunities in their 2019 annual reporting

37% believe improved climate-related reporting will reduce shareholder pressure and/or activism

21% think that improved climate change reporting will increase company valuation

Carbon Trust/Ipsos MORI 2019

PERCEIVED FINANCIAL BENEFITS OF CLIMATE CHANGE REPORTING BY UK CORPORATES



Carbon Trust/Ipsos MORI 2019

ROUNDTABLE

Risk roundtable: what the experts say

Thought leaders from across the sector and academia discuss risk management and resilience in a fast-moving digital age when board members need to keep pace with business transformation

David Denyer
Professor of leadership and organisational change
Cranfield School of Management

Julia Graham
Technical director
Airmic

John Ludlow
Chief executive
Airmic

Mary O'Connor
Chief risk officer
KPMG UK

Chyono Flynn
Vice president of enterprise risk management
Pearson

Tim Murray
Group director enterprise risk
Serco Group

Q How is the digital revolution changing the way boards talk about risk?

CF In the past, you had maybe two years' warning before big changes such as new regulations. But with digital transformation, disruptive technologies, you're having to react month to month. Our biggest digital transformation programmes are on every single audit committee agenda which are well attended by our board members.

MO There is an enormous amount of execution risk. How do you deal with that? It's a very difficult thing for boards to measure because you have to get quite granular to really appreciate what's happening. If you're not a technological, transformation expert, it's actually very hard to do that.

JG I agree. You would never in days gone by consider having a director who didn't have financial literacy. I think it's getting to the stage where you wouldn't consider having a director unless they also have a degree of technology literacy. Otherwise, how do you ask the questions? How do you exercise oversight and governance if you don't understand that part of what you're governing?

I don't think oversight of digital is something you can pin on one individual on a board, which I think some organisations have tried to do, albeit expert capability can be a good thing to have in addition, especially in technology-oriented sectors.

TM But it's not just digital transformation. Digital transformation shows the need for new and emerging ways of thinking; the need to understand the connectivity of risk. It should be a catalyst for a change in thinking.

JL The board needs to make sure it has a much better relationship with all its stakeholders so if something goes wrong, they're not calling on an empty relationship. So I think the whole technology agenda feeds into the trust agenda.

DD I think for all these things – artificial intelligence, automation, machine-learning – the future is uncertain and I think that creates quite often a defensive mindset in organisations. The level of uncertainty and risk aren't known, so although they talk the language of digital, they can't really understand the ramifications of some of the changes that are coming.

> **Pure data will not do it; you have to provide a summary and translate it into usable information**

I used to have conversations with people responsible for risk who would tell me there was a group or committee with responsibility for cybersecurity or information security. Now I'm seeing much more of an enterprise-wide conversation; it's about the whole organisation. I think we should use language more around resilience than just risk management, not only stopping things from happening, but looking at the ability of the organisation to anticipate some of these changes, prepare for them, adapt and to respond.

Q Can boards be bolder if they have a better grasp of digital transformation risk?

CF At Pearson, the shift in the conversation about digital is that risk isn't necessarily about avoiding something bad, it's also about maximising opportunity.

DD I've recently seen much more of a strategic-level conversation that's not just about prevention, but more "How do we leverage the opportunities?" But equally, there's a lot of discussion around impact tolerance and risk appetite. What if your IT system goes down and you have people caught in the forecourt of a garage unable to pay? How quickly do you need to get that up and running? What's the damage to the customer, to the brand, to our reputation from an event like that?

MO You have to assume you're not going to get it 100 per cent right, because you're doing something by nature that no one's done before. So you're going to make mistakes. The key is communication and fixing them.

Q What's the best approach when risk professionals talk to the board? Should they talk about return on investment or storytelling?

MO I think you need to do both.

JG It's about taking academic excellence and topping it up with strategic, horizon-scanning and storytelling skills, and becoming a true business partner because the worst thing you could do is go to a board meeting and produce all these colourful risk heatmaps, which you think are wonderful, but the board get quickly bored with. They want to talk about what really matters and those are probably not things that you find on many heatmaps.

TM Yes. Pure data will not do it; you have to provide a summary and translate it into usable information.

CF Our board are engaged and will challenge me on risks in audit committee meetings. Individuals sometimes have specific risk interests and the more emotive risks can get more attention, so you have to go in prepared to tell the story on which risks they need to focus on.

JL Risk managers are dealing with a very tough subject. But the culture is that nobody wants to talk about it. Therefore they need to be ninja warriors in terms of getting board attention. It probably means seeking out individual directors, going to have breakfast with them, coffee with them, wherever they are; getting your point across long before you ever get to the boardroom.

TM As well as being a ninja, you need to get across that risk management is not a blocker, it's not a policing function, it's more of an enabler. The skillset requires persistence and diplomacy.

Q Is this a common problem? Are risk experts seen in the boardroom as whingers or people who don't "get" digital?

MO Good risk management is just good management, right? At the end of the day, companies that manage risk well are going to be more successful. You can't be a kind of observer or a pointer-outer of bad things. You need to be a leader. You need to drive the change.

TM That's probably one of the good things about the profession that there are so many touchpoints within the business it crosses many, many functions. And it crosses many horizontal and vertical levels. You have conversations at the top and the bottom and in-between.

JL I agree. You can be inside the business. You could be outside the business in the supply chain, in the wider ecosystem. It's a great way of actually getting the dark side of management information that nobody wants to give you.

Q Does it help to talk to the board about near-misses, serious problems that were narrowly averted?

MO Absolutely. Learn from these. If you don't have an open dialogue, you're potentially exposing the company.

DD The interesting thing about the near-misses is they often identify where someone has noticed, anticipated a problem and has usually intervened in the system in some way to fix it. They are really a window of opportunity to look up what's the positive human contribution to the system that's enabling us to manage those risks.

MO On the one hand, boards need to be firm. It's their job to hold executives to account, to make sure the rules get followed, to make sure all the processes are there. But at the same time, they need to make sure the culture is willing to make mistakes, embrace problems, embrace mistakes and make sure actions happen on the back of them. It's a really fine line.

JL I used to look after quite a lot of hotels around the world. And at every board meeting we published the serious incidents that had happened in the previous month or six weeks. We used to burst the bubble right at the start of every meeting. And it became their number-one read every month.

And once you do that over a long period of time, you build the trust of the company across the world. Hundreds of thousands of people know that it's OK to say, for instance, they saw a window cleaner with no harness on, 24 storeys up or whatever.

Q How big is the culture issue?

JL We used to celebrate people that managed crises well. For instance, when the Japanese triple disaster [the earthquake, tsunami and nuclear crisis of 2011] happened, we had a magnificent regional operator who managed a team right the way through that. We were the biggest hotelier in Japan, and we made a lot of people safe and carried on doing business. There was a huge celebration in the company, and part of the celebration was how did it go so well and what are the lessons for other leaders?

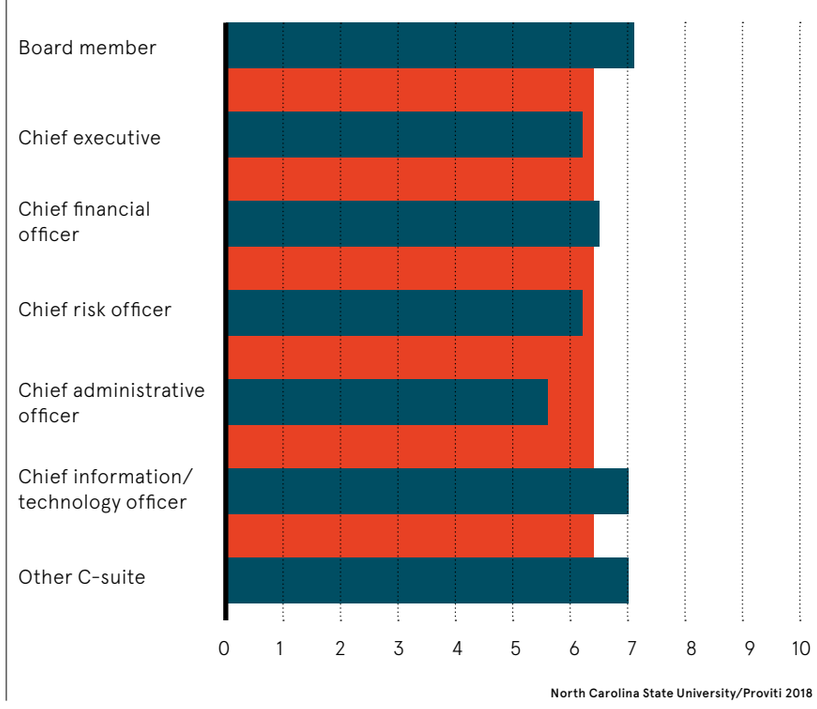
> **The board needs to make sure it has a much better relationship with all its stakeholders so if something goes wrong, they're not calling on an empty relationship**

CF And the other important thing is what you do with the lessons learnt. If you actually take action then the board can see you've done things differently next time.

Q Should you celebrate even if the crisis management wasn't 100 per cent perfect?

LIKELIHOOD OF INVESTING MORE RESOURCES IN RISK MANAGEMENT IN THE NEXT 12 MONTHS, BY JOB ROLE

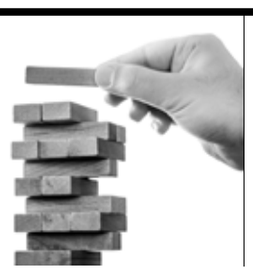
1 = Unlikely to make changes; 10 = Extremely likely to make changes



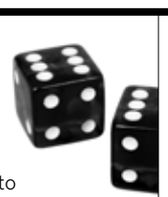
North Carolina State University/Proviti 2018

Growing need to manage cyber-risks

49%
of C-suite risk owners believe risk management is becoming more important to achieving strategic goals
Deloitte 2018



16%
of boards say they haven't discussed management plans to respond to a crisis
PwC 2018



1 in 2
chief executives say a cyberattack is now a case of when not if
KPMG 2018

90%
of FTSE 350 companies say their board is increasing spending on mitigation of cyber-risk
ICSA 2018

£900m
cost of downtime associated with DDoS cyberattacks to UK businesses in 2018
Netscout 2019

> **I think we need to change the discourse. Everyone says 'We've learnt our lessons', but have they actually done anything about it?**


Marc Sendra Martorell/Unsplash

JL Absolutely. You're dealing in chaos. But a robust leadership means that your business survives and thrives.

DD I think we need to change the discourse. Everyone says "We've learnt our lessons", but have they actually done anything about it? I've worked with one hospital that had six "never happen" events in six months, and after every one there was an investigation with recommendations and an action plan for implementation. It's almost like the organisation was going through the process in a very technical way without actually learning and doing something.

TM If you're not careful, the processes or the compliance side will overtake the actual substance, in other words the iterative understanding of what's really going on.

JG There's a tendency at the moment of saying hindsight is a bad thing and we have to look forward and extrapolate the future. But actually, you can learn so much from hindsight, we should never forget that.

Q How should boards be warned about more distant risks on the horizon?

CF You have to do more scenario-modelling; you have to do more horizon-scanning; you have to do more sensitivity analysis. And then, by the way, you have to keep doing it. It doesn't stop. You just have to because all the time your environment changes and your business is changing.

DD I did a piece of work which was for a manufacturing company that's been around for quite a long time, run by a traditional board. The chief executive, who I thought was one of the most enlightened I've encountered, asked us to run a programme taking 50 of their youngest, brightest people across the business. He told them, "We've run this company for the last 50 years. To ensure it's around for the next 50 years, we want you to be the eyes and ears, and really think about what the future risks are, what the future opportunities are."

If you give resources and support to people within the organisation, their collective intelligence is going to be much better at identifying some of these risks than the board would.

JG I've an anecdote that complements that. We ran an event last year with about 100 young risk managers and we asked what are the top-ten things that keep you awake at night? And then as a separate exercise, we said, "OK, put that to one side. Now write the headline that you would not want to see on the front page of the tabloid press tomorrow morning." And not one of them was in those top-ten risks.

Q One headline many companies didn't want to see was the Brexit referendum result in 2016. What have companies learnt about risk management from this tangled process?

DD It certainly showed you can have a disruptive event that no one saw coming. If you went back a period of time, five years ago, you would've said, "This is pretty implausible."

I remember working with one financial institution just after the referendum and I said to them, "What is your plan? What are you going to say to your customers?" And they hadn't got a plan, hadn't even gone through any of that process, which is remarkable.

Now we all know a plan doesn't usually survive the first engagement with the enemy, but the process of going through a planning process is what creates great value in the organisation.

JG It's like most potential crises. You plan for the worst and if it's not the worst, then lucky you.

This roundtable was arranged in partnership with Airmic, the association that represents UK risk and insurance managers. Its annual conference will take place June 3-5 in Harrogate.

Bursting the bubble

Q How can boards ensure they get an honest picture of risks to their business?

JL I think diversity is a big part of it. I think diversity of thought is an even bigger part of it. You wouldn't just go and talk to the IT department about IT; you need to talk to the people who use IT, the people who bend the rules in the field, the people who break it.

DD If the senior leader in the organisation's first response to something going wrong is "Who screwed up there?" you're immediately going to create a culture where people are not going to start admitting to mistakes. Just switching that question around, asking why it made sense to that individual to do what they did at that point in time, gets you immediately into a learning mindset.

JG The big issue for me is courage. Not everybody welcomes the conversation. But to have courage you need confidence and confidence is enhanced by having a grasp of what you're talking about.

MO But you need courage on both sides. The board needs the courage to ask questions even if they are not the experts and to have enough courage to admit it. And David Denyer is right to make the point that the board needs to be able to say "Hey, we might not have got this right" and to work together to reach solutions.

Part of the answer is proper management information. Sure, you want it easy to read, but sometimes more is actually better, so you can see trends and outliers. But also, information lock is a real problem for boards. If they are getting just one view of the world, it can be very problematic. So I think it's really important that boards can get out and about, and have different sources of information so they can sense-check things.

JG But don't you think there's a fine line? It's great for directors to walk the floor, but don't do too much. You're not the chief executive. One of our members wanted to know what the role of a director was during a crisis. We said their role is being on the board. They are not managing the crisis, but are there to make sure there is executive leadership who have a plan and a team, and that both have been tested.

Moving to the frontline

Risk management is moving out of the back office to become a business partner, says **Julia Graham**, deputy chief executive and technical director at Airmic

There has been a silent revolution going on and in the last three decades a remarkable transformation has taken place. The average value of companies has moved from a ratio of 90 per cent tangible assets and 10 per cent intangible assets, such as reputation, information and intellectual property, to 90 per cent intangible assets and 10 per cent tangible assets.

Concurrently, business transformation fuelled by technology is creating a world that is more connected and complex. Bring these two scenarios together and there is an explosive cocktail. The consequences are that the assessment and management of risk is harder and less certain. Traditional actuarial rules just don't apply to many modern risks and when companies think they have their arms around managing risk, the pace of change moves up a gear and the world spins away from their reach.

While the process of change is speeding up, the external and internal environments in which businesses operate are changing at different speeds. Changes to the external world are like a genie out of a bottle, they can't be put back and change will be exponential. On the other hand, sectors and businesses are typically moving at a slower pace than their external environment.

The increasing speed differential is creating a change lag. Speed of risk decision-making is essential, but this requires agility, new knowledge and enhanced skills.

In this context, the corporate governance functions of monitoring, strategy and legitimacy remain valid, but need to be enhanced and extended beyond traditional approaches. Governance of digitally transformed business models requires greater attention to the broader environment or ecosystem within which they operate.

Risk management is moving away from pure prevention to response. This requires a shift in the emphasis of risk management and risk management professionals.

First, there must be a better alignment with business priorities. Risk teams need to demonstrate strong commercial acumen, with the business language to communicate it persuasively, and engage more intensely with the company's strategic ambitions and major investments. This will sharpen their ability to develop valuable insights into emerging concerns and help scope innovative risk-mitigation solutions.

Second, the modern environment demands a more flexible deployment of resources. Revised analytical methodologies, including the introduction of new data science and automation techniques, should free up capacity in risk teams for more project-based, as opposed to routine, risk work and the provision of advice to business and functional leaders.

> **Speed of risk decision-making is essential, but this requires agility, new knowledge and enhanced skills**


Marc Sendra Martorell/Unsplash

Third, businesses and risk professionals should view emerging risk through a more creative lens. This will enable risk teams to engage with institutional and individual biases and blind spots, and help build an appreciation of threats for which evidence may be limited or conflicting.

As a final thought, it is often said that risk management is part science, part art. The arguments here demonstrate the risk profession needs to move more towards the latter, focusing on judgement, creativity and people skills. However, data-gathering and analytics will also grow in importance, while machine-learning and artificial intelligence will increasingly play a key role in managing risk. Technology will not take care of itself, and the risk community must enhance their knowledge and skills to be prepared.

Art of cultural leadership

Companies with a strong corporate culture generate better financial returns and enjoy higher staff retention rates. So, what's the secret to success?

A war for talent is raging across UK plc, driven by the lowest national unemployment rate in decades. For companies to attract the very best people, generous remuneration packages are no longer enough. For today's young career climbers, a positive corporate culture is at least as important. For many of the youngest new starters, it is their biggest consideration.

In a 2018 survey by consultancy group Deloitte, corporate culture was found to be the second most important factor for millennials in considering where they want to work.

Yet corporate culture can be a slippery concept to identify from the inside, let alone to improve. It is built on a company's long-term strategy, the way it communicates with staff and the outside world, the diversity of its workforce, and how it sets goals, rewards staff, embraces sensitivities and deals with misconduct.

Companies seeking to recruit the very best talent need to dedicate time and resources, nurturing their corporate culture, which demands a dose of introverted navel-gazing followed by a concerted and sustained drive to improve.

The Deloitte survey found that 52 per cent of millennials (born 1983 to 1994 in their analysis) thought that corporate culture was "very important" when choosing an employer, while 57 per cent of Generation Z (born 1995 to 1999) agreed, making culture their biggest consideration.

Staff benefits

Argo Group, a specialist commercial insurance business, is one of the growing number of global organisations investing in its corporate culture. The effort began by securing leadership from the top when responsibility for cultural development was allocated to a C-suite executive.

"Recruitment in our industry is now incredibly competitive," says Matt Harris, group head of international operations at Argo Group. "The talent war makes hiring the best people one of the biggest challenges confronting us.

"It is vital to present a clear vision and purpose, and articulate them to potential candidates. Delivering and reinforcing those messages is equally important from a retention perspective. It is critical that our people understand the role each of them plays in achieving our corporate vision."

Argo ensures this by aligning its corporate objectives with those of its workforce. It is equally important, Mr Harris says, to invest in employees' future careers, rather than just in training them for their current roles.

"If you can't explain how a person contributes to the corporate vision, or if you fail to compensate them appropriately or to contribute to their development, they will go elsewhere. But when you show people you care about their careers, you will benefit from improved levels of engagement within a positive workplace culture. When you get that right, you see people delivering consistently to the business and ultimately to its customers," he says.

> **As organisations expand globally, they must adopt a strong focus on culture**

Shareholder benefits

The rewards of a stronger corporate culture are not only reflected in happier, better quality staff. Shareholders also see a direct benefit in the form of improved financial performance: up to three times better for companies with the strongest corporate cultures. This finding led management consultants McKinsey & Co to conclude that corporate culture is "one of the most essential drivers of business performance".

The recognition of culture as a key financial driver is another reason why shareholders and investors are demanding companies do more. Businesses are responding by ensuring personal remuneration is linked increasingly closely to business outcomes. This helps to match up corporate objectives with personal ones.

"Across financial services, shareholders and boards are demanding that compensation packages are aligned with business results and corporate performance," Mr Harris explains. "Executive compensation has shifted over recent years, with a much heavier weighting on variable compensation relating to the delivery of specific business goals."

Cultural enrichment

As businesses grow and begin to operate in multiple international locations, maintaining a cohesive corporate culture can become increasingly difficult. Now based in London, Mr Harris has worked around the world, with stays in India, Indonesia, Malaysia, New Zealand and Singapore.

He says a truly global corporate culture, one that is inclusive and diverse, can only be achieved through the awareness of regional and cultural sensitivities. "As organisations expand globally, they must adopt a strong focus on culture," he says. "The behaviour and actions of the leadership group have the biggest influence on how you build that culture."

Argo's group head of international operations says organisations need to be welcoming of international regional sensitivities. Embracing them strengthens global brands by bringing local working approaches into line with global goals, targets and business strategy.

Merger planning

Interweaving cultural nuances is tricky when companies grow organically, but it is even more difficult with mergers and acquisitions (M&A). Organisations that fail to consider corporate cultures in detail before proceeding with M&A risk wasting considerable time and resources dealing with subsequent conflicts, which is a leading cause of value leakage in the aftermath of such deals.

Mr Harris has witnessed corporate culture consolidation many times during his career. The most successful outcomes were driven by management teams with clear ideas about their leadership objectives and clear communication throughout the newly merged business.

"When you bring two companies together, two separate cultures may co-exist for a period of time until the new cultural identity develops," he says. "So in an M&A situation, it is important to define the expectations early to everyone. The longer that takes, the longer you'll see two separate cultures and tribes working in isolation."

Personal touch

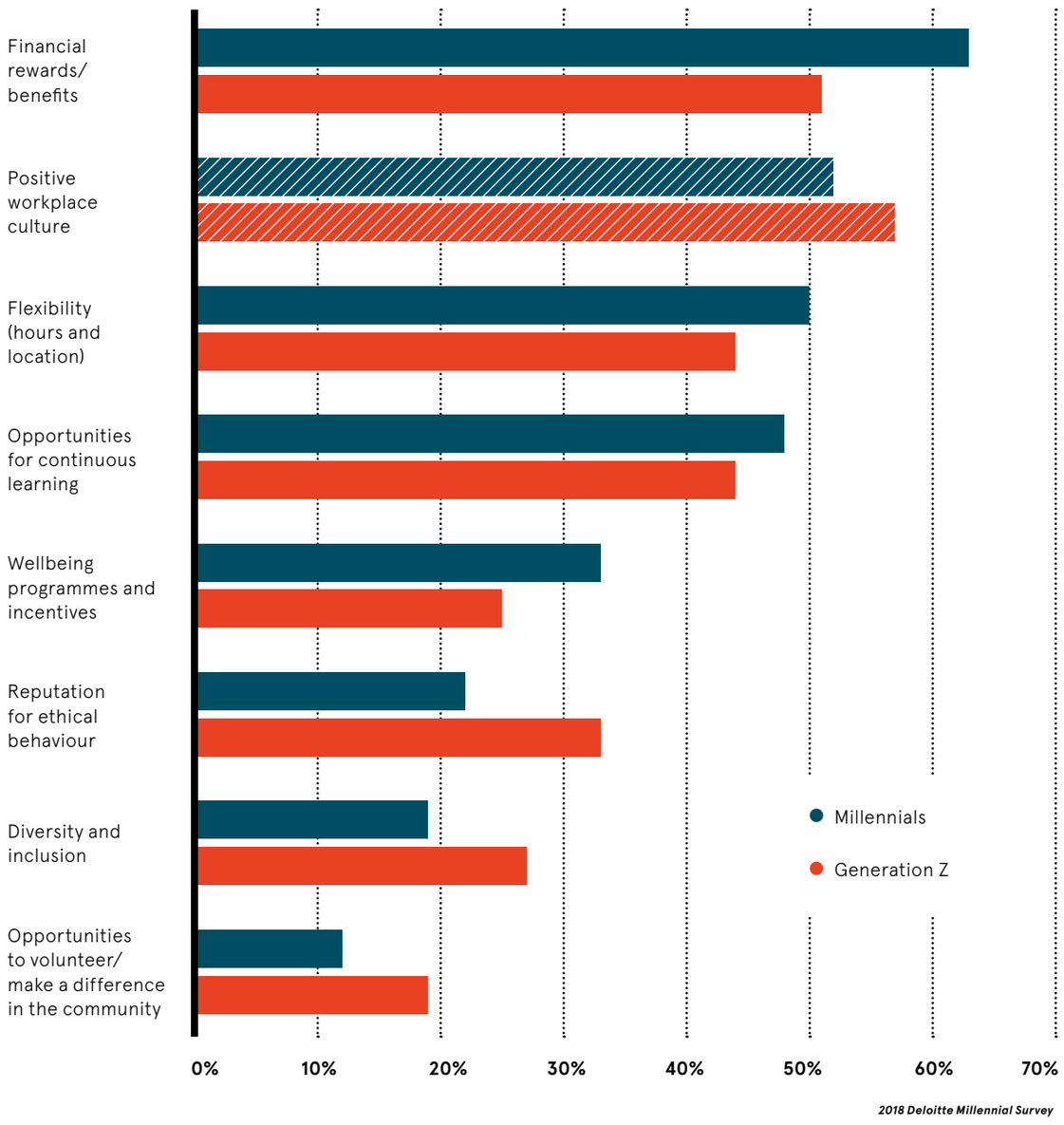
Rapid evolution of technology has focused many senior executives on the role it can play in shaping the behaviour of the workforce. However, while technology can assist with workflows, support training and enable flexible working, it cannot replace a key ingredient to building a culture: human interaction.

"The fundamental nature of the insurance industry is to take care of people after an unfortunate event," says Mr Harris. "To manage that effectively requires a whole lot of empathy. It is critical, therefore, that we have people in customer-facing roles with the skills that allow them to deal with our customers with empathy."

In the end, then, corporate culture is all about people. It must start form the top, and extend to every office and desk. When it is right, the rewards benefit everyone, from the shop floor to the boardroom to the shareholders' purse.

YOUNG WORKERS' WISH LIST: PAY AND POSITIVE WORKPLACE CULTURE

Percentage "very important" when choosing to work for an organisation



2018 Deloitte Millennial Survey

OVERSIGHT

Why digital oversight is so critical

When digital transformation projects are well underway, significant risks remain

Kate O'Flaherty

In a competitive business environment, companies are under increasing pressure to cut costs and improve efficiency. Over the last few years, this has resulted in a digital transformation drive with firms embracing technologies such as cloud, internet of things and artificial intelligence (AI).

Digital can boost a company's bottom line, but the area also comes with increased risks. While the European Union's General Data Protection Regulation has generally improved data governance, it's still a challenge for firms to manage their growing digital estates.

The issue lies in the fact that data managed by businesses is vast and disparate. Indeed, software-as-a-service applications intended to drive efficiency are being used across the organisation, often without IT's knowledge, and data can spiral out of control.

Amid this complex environment, there is a growing need for company-wide oversight in digital transformation. Visibility is an important first step; firms must identify which departments are most at risk and apply a policy across the business.

> **Create a culture of 'it's OK to make a mistake; let's learn from it' and that starts right at the top**

For example, developers can pose a big problem for organisations, according to Sarah Armstrong-Smith, head of continuity and resilience at Fujitsu UK and Ireland. "Their devices might not be as locked down as a typical user's. A system administrator might download products from the internet to have a play with, but they could lack the security controls on their devices required to have that level of access," she says.

Making things worse, companies often have no idea exactly how many apps are running throughout the business. "A company might think they are using 200 apps and services, but find after an analysis across their estate there are 4,000," says Ms Armstrong-Smith. "It is even possible that some applications are based on an older version of the same product, which opens backdoors to the estate for attackers to exploit."

To gain visibility, Karl Foster, legal director at Blake Morgan, advises firms to consider software solutions in a market segment dubbed regulatory tech or regtech. These products can help a business assess risk while managing and putting data in an understandable form. "It will take away some of the difficulties," he says. "It makes people think before they send out that email."

Strategic thinking taking the security risks into account should be in place from the start of any digital transformation project, says Carolyn Crandall, security consultant at Attivo Networks. "If it's not possible to secure a product through the vendor, are you confident you can do so in-house? It takes leading-edge thinking," she says.

Lisa Hamilton, Deloitte UK cyber associate director, concurs. She emphasises the importance of clear communication. "Educating teams and increasing awareness within the business is one way to help identify the associated digital risks," says Ms Hamilton.

As part of this, firms should try to understand users' motives. Ms Armstrong-Smith asks: "Is there a reason why they are downloading extra things from the internet? Are the corporate systems not good enough to do their jobs?

"Understand the business context of 'why', then see if there should be any lockdown on those devices. If you allow your developers different levels of accessibility, could you put that on a separate network? Understand the business need versus the risk."

It makes sense to implement a firm policy outlining who has access to what, says George Gerchow, chief security officer at Sumo Logic. He advises: "Create a culture of 'it's OK to make a mistake; let's learn from it' and that starts right at the top."

It's also important to note that fixing the issue isn't just the chief information officer's job, says Rob Lamb, chief technology officer at Dell EMC UK and Ireland. "The CIO is at the heart of it, but it's about engagement with all lines of the business, including the board," he says.

Better and more frequent communication with senior leadership is therefore important. "We know senior executives perceive security as a leading threat; more regular briefings will help better align the cybersecurity provision to business needs," says Paul Taylor, partner, cybersecurity, at KPMG UK.

A more measured approach to digital transformation can make a difference, but it will take time. Firms also need to take into account any challenges that might arise when implementing a risk management plan. For example, employees might be resistant to changing the way they use technology.

> **In an age of frequent and sophisticated cyberattacks, security must be at the forefront of any digital transformation project**

To avoid this, communication and careful planning is key, says Mr Lamb. "Inevitably with any large change or transformation there will be naysayers. Mandates and policies are an effective tool, but communication is important, so people understand," he says.

Mr Lamb advocates a programme including cultural and organisational change. "You have to tear down some cultural and operational barriers," he says. "Imbed skills and capabilities in teams that wouldn't normally be seen together."

In an age of frequent and sophisticated cyberattacks, security must be at the forefront of any digital transformation project. Getting this right will ultimately impact the bottom line, says Mr Foster. "In some industries, the growth of AI greatly improves customer service. That is why this technology is worth managing from a risk and security perspective," he concludes.

Three business functions with high levels of cyber-risk

As businesses strive to transform digitally, any part of the business can pose a risk. However, three key areas often create a surprising number of issues

01 Human resources
HR departments are among the most likely to use software-as-a-service (SaaS). If risk and security haven't been factored into this, it can lead to the exposure of employee data and be in breach of the General Data Protection Regulation (GDPR), says Rob Lamb at Dell EMC UK and Ireland.

People can take their eye off the ball when it comes to internal back-office platforms, such as SaaS payroll, says Sarah Armstrong-Smith at Fujitsu UK and Ireland. "Those HR systems are rife with personal data, including all the diversity and inclusion information which under GDPR is protected: disabilities, sexual orientation, it's really sensitive," she says. "It's easy to buy off-the-shelf products, but think about access controls and the security of these services, and how they are being managed."

02 Legal and commercial teams
Another area of potential risk is legal and commercial teams. These will often handle data on contracts or disputes that a firm would not want in the public domain. "If that's on an open email cloud platform, attackers might be able to access these types of documents," says Ms Armstrong-Smith.

03 Marketing
Marketing departments deal with vast amounts of data on a day-to-day basis, but it's easy for companies to lose control of this information, including marketing plans, trends and even intellectual property rights. If an attacker was able to access this data, they could try and sabotage a firm's approach, warns Ms Armstrong-Smith.

GEOPOLITICS

Safeguarding supply chains amid disruption

Global political events can impact world trade and supply chains in particular, so coping strategies are essential to limit disruption and maintain production

Dyson founder and chief engineer Sir James Dyson

Josie Cox

Ex-Army engineer Doug Johnson-Poensgen worked at BT and Barclays Bank before he took a leap of faith. Inspired by a desire to use technology to solve what he calls "real world problems", he set up Circulor.

The London-based company, of which he is chief executive, uses blockchain and artificial intelligence to track global supply chains, ensuring products are traceable from source to end-user.

"It's hard to know exactly where the cobalt that's mined in the Congo goes before it ends up in your car or the palm oil that's in your ice cream," says Mr Johnson-Poensgen. "And there's never been more pressure for companies to provide that transparency."

With a multitude of risks facing almost all major supply chains, from geopolitics to natural disasters and financial pressures, he says Circulor, established in 2017, is "making it harder to game the system".

Customer scrutiny of the practices of large corporations is increasing at a rapid clip. More than ever, there's pressure on retailers to reassure buyers that the tantalum used in their smartphones and laptops is not mined in war zones and sold to perpetuate conflict and bloodshed.

"Relying on self-certification is just no longer good enough," says Mr Johnson-Poensgen. "We need to do more."

Circulor has five large clients and several more in the pipeline, according to the chief executive. Demand for its services highlights the vast challenge of trust and accountability faced by corporations in a world where consumption is fuelling production at any cost.

But more generally, it underscores that businesses are being forced to be much more cognisant of their environment in an increasingly interconnected, yet deeply unpredictable, world.

The risks are omnipresent. Simmering trade tensions between global superpowers, a rise in international protectionism and uncertainty stemming from the UK's expected departure from the European Union mean companies are investing heavily to diversify their supply chains and minimise the risk of disruption. Each link in the chain raises a fresh slew of potential risks, but for many, US-China trade wars are the most prominent.

American clothing and footwear manufacturers have been shifting their production away from China to countries such as Vietnam and Indonesia for several years. In recent months the push has intensified in response to President Donald Trump imposing punishing tariffs.

Footwear maker Steven Madden and furniture group RH say they have offset cost increases by shifting some manufacturing operations away from China or negotiating discounts for their continued production in the country.

Others have ramped up shipments of imported goods, stockpiling in anticipation of President Trump's next move. For the first half of 2019, US ports are now expected to handle 10.7 million containers, a 4.1 per cent increase on the same period in 2018. This could lead to an uptick in warehousing costs and chip away at profit margins.

In Europe, meanwhile, Brexit is causing many corporations to reassess their strategies and supply chains, irrespective of political persuasion.

Sir James Dyson, a billionaire Brexit supporter best known for revolutionising vacuum cleaners, announced in January that his company was moving its head office from the UK to Singapore. He maintained that the shift was not driven by Brexit, but other companies, from Panasonic and Sony to P&O and Schaeffler, have cited the UK's departure from the bloc as a reason for shaking up their supply chain.

The Chartered Institute of Procurement & Supply (CIPS) estimates that a tenth of UK exporters could have contracts cancelled if there are delays at the border because of Brexit and one in five EU businesses will expect a discount from UK suppliers if border delays persist for a single day.

"The financial cost of Brexit indecision will not be paid in Whitehall, but by Britain's businesses," says John Glen, an economist at the CIPS.

Patrick Hogan, director in Rolls-Royce's global government relations team, says his company has built up additional inventory to manage a potential disruption or delay in supply on account of Brexit.

He adds, however, that the engineering company is less exposed than businesses operating in sectors with high-volume manufacturing, supported by so-called just-in-time supply chains, such as the automotive industry.

Like Circulor, tech giant Oracle is one of the companies that has recognised potential threats to global supply chains as an opportunity.

It has developed a product for customers to stress test their supply chains by simulating theoretical scenarios, such as a hard Brexit or an increase in US tariffs. Neil Sholay, Oracle's vice president of innovation for Europe, the Middle East and Africa, says the product was developed in response to businesses being increasingly fearful of the unknown and wary of who they can trust.

"Whether the risk is geopolitical, social or something else, there's a growing culture of responsibility in supply change management and businesses will have to keep up to remain competitive," he says.

Dubai-based port operator DP World is collaborating with Oracle to use microchips to ensure goods are not intercepted and a Dusseldorf-based shoemaker Cano is using blockchain to track the journey of its products, from cow to customer.

Cano's shoes are produced in Mexico and founders Lukas Pünder and Philipp Mayer say it's a priority for them to ensure working conditions are fair and that materials are sourced sustainably. Later this year they'll start offering their tracking technology to other apparel companies.

The founders say geopolitical pressures have so far not really affected Cano's supply chain, though they did have to halt production briefly in January amid a Mexican government crackdown on fuel theft. "Only a few places were able to get gas during that time," says Mr Mayer. "That was a huge problem for us."

Looking ahead, Rolls-Royce's Mr Hogan says that when it comes to assessing potential risks "the unknown unknowns are always out there".

29%

of chief executives believe global economic growth will decline over the next 12 months

PwC 2019

65%

of procurement leaders have limited or no supply chain visibility beyond their tier-one suppliers

Deloitte 2018

74%

of surveyed organisations faced a disruptive event with third parties in the last three years

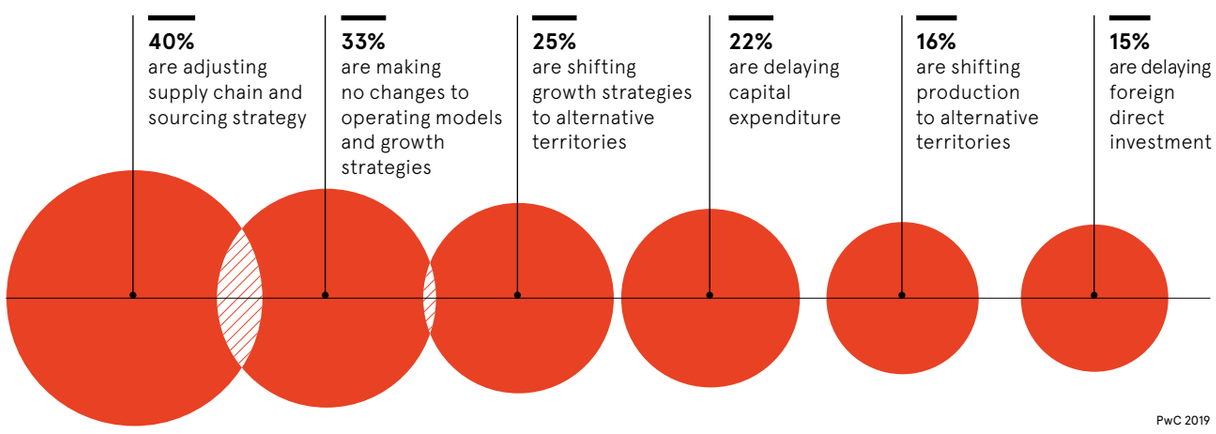
Deloitte 2018

> **Brexit is causing many corporations to reassess their strategies and supply chains, irrespective of political persuasion**

"Major disturbances can sometimes flare up from small-scale catalysts, triggering dramatic changes. We protect ourselves to the extent possible, by making prudent choices in the selection and location of suppliers, and by using a selection of forecasting and analysis tools and resources," he says. "It's not possible to eliminate geopolitical risk completely, but through these approaches we can minimise the impact on our supply chain and our business."

TRADE CONFLICTS ARE AFFECTING OPERATING MODELS AND GROWTH STRATEGIES

Survey of organisations "extremely concerned" about trade conflicts



PwC 2019

What can your business do to close the cybersecurity skills gap?

With 1.5 million cybersecurity roles estimated to be left unfilled by 2020, **Peter Kelly** of Computer Futures says more education and awareness is crucial to closing the skills gap

The threat to the cyber-landscape continues to evolve at a rapid pace. High-profile data breaches demonstrate not only the huge financial cost of being attacked, but also the considerable reputational damage. With hackers constantly moving the goal posts, cybersecurity is one of the top issues that keeps board directors awake at night.

Having the best cybersecurity skills to navigate the digital age safely has never been more important, yet the industry is facing a global shortage with 1.5 million unfilled roles predicted by 2020, according to Forbes. It's easy to assume the people simply don't exist, but while that may be true in some instances, what is actually fuelling the skills shortage is a lack of understanding around the skills required.

Our global team is dedicated to finding the best people in the security market for our customers and placing them in the right role. At Computer Futures we take the time to educate employers on how to write job descriptions, provide them with key market analysis and help them create environments that increase retention. Here are a few tips for business risk and cybersecurity employers to help address the skills gap.

$300bn

predicted global cybersecurity market in 2024

Global Market Insights

1.5m

unfilled security positions expected by 2020

Forbes

58%

of organisations report having unfilled cybersecurity positions

ISACA

01 Validate job descriptions against your peers

Job descriptions for cybersecurity roles often seek people that tick every box covering both technical and non-technical skills, but you'll rarely find that in one person. By validating and benchmarking job descriptions against the rest of the market, including looking at competitors' websites and job boards, employers can gain a better understanding of what they need and what they can realistically get.

02 Be flexible and offer progression

Companies should first look internally to see if there are existing employees who can be trained in cybersecurity. Most large organisations have considerable IT teams where many of the skills are transferable to cybersecurity roles and people in other departments may be interested too. You may identify loyal people who already know the business and culture, and contract resources are often valuable too.

Attracting the best people also means offering strong career progression from the outset, both in terms of training and future career opportunities. People desire employers that invest in their development and they want to be able to see their growth trajectory. Offering a training budget and involving security in business decisions will go far in both attracting good people and retaining their skills in the long term.

03 Truly care about security

One of the main things people want to know about the companies we recruit for is how seriously they take security. They don't want to feel like a side piece to the rest of the business or part of a tick-box exercise for compliance. It's their reputation at risk as well if the organisation is breached, so they often gauge the company's attitude to security by asking what part of the business security reports into or whether it is sponsored at executive level. Proving you care about cybersecurity will no doubt attract better people.

We all have a responsibility to help alleviate the skills gap and it's a core part of our company purpose in bringing skilled people together to build the future. At Computer Futures we're proud to run a series of events and awareness initiatives as part of our Secure Futures campaign. We're hoping it will have a positive impact, and the programme truly marks our commitment to educating people on exciting cybersecurity careers and increasing diversity within the industry.

For more information on Secure Futures or how we can help your business please email Peter at p.kelly@computerfutures.com or visit computerfutures.com

COMPUTERFUTURES