pentland ANALYTICS

Reputation Risk in the Cyber Age

THE IMPACT ON SHAREHOLDER VALUE

AON

Foreword

Reputation risk is a formidable challenge for companies worldwide. Although risk management awareness and tools have evolved, reputation risk continues to weigh on corporate executives as one of their leading concerns. For the past 10 years, reputation risk has occupied one of the top spots on Aon's bi-annual Global Risk Management Survey. Aon is delighted to collaborate with longtime partner Dr Deborah Pretty from Pentland Analytics to take a closer look at how reputation risk has changed in an age of instant communication and connectivity.

Reputation risk events can result from many different sources, such as supply chain disruption, cyberattack, product failure, executive malfeasance or adverse social media. Advancing technology has changed the speed and channels of information flow, which now operate in a global, 24-hour news cycle. Our research suggests that widespread use of social media increases the impact of reputation events and significantly elevates a company's reputation risk.

Reputation events, such as cyberattacks, can have a material impact on shareholder value. Research shows that the impact on value is greatly influenced by three factors:

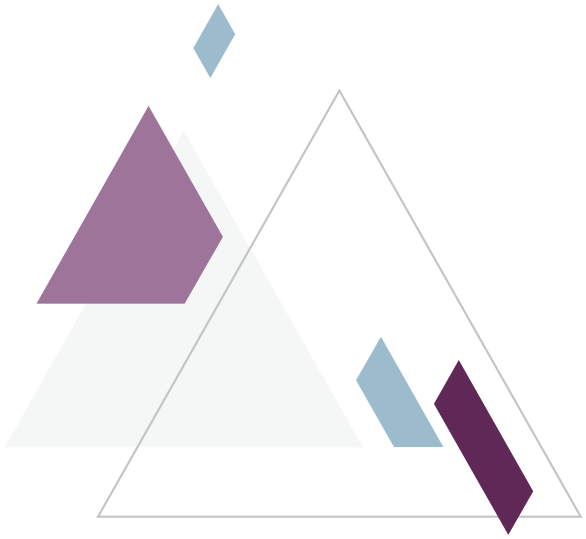
1. The ability to produce instant and global crisis communications
2. Perceptions of honesty and transparency
3. A program of active social responsibility

Using risk management frameworks, including assess, test, mitigate and manage, can prepare organizations to survive and thrive from reputation events. In fact, companies that navigate reputation events successfully often see a net gain in value.

We invite you to read the 2018 Reputation Risk in the Cyber Age Report and use it as a catalyst for conversations inside your organization. The return on investment for active, engaged risk management has never been higher.

Randy L Nornes
Enterprise Client Leader
Aon

Preface



I am delighted to share my latest research into the shareholder value effects of disruptive events. This work represents a comprehensive update and extension of my original study[1]. Far from dissipating over the last twenty-five years, the impact of critical risk events on financial performance remains as relevant today as ever.

Natural disasters, politico-economic turmoil, reputation crises, and the otherwise sudden and unexpected continue to challenge executive managers around the world. This report summarises my research results to date, and presents new evidence on the effects of social media and cyber risk, on shareholder value impact and recovery.

Back in 1993, my early work focused on corporate catastrophes occurring primarily in the oil, gas and petrochemical sectors. BP had taken the decision to self-insure its catastrophe exposure, in the belief that its balance sheet provided greater strength than that of the insurance industry combined. It was an interesting time, and piqued my curiosity as to the dynamic between loss and impact. Without the luxury of electronic data access, the first study portfolio contained just fifteen losses occurring since 1980, with daily share prices and market data collated (laboriously!) from the back pages of the financial press. Nonetheless, the results are striking.

1993 study results

- The market makes a rapid judgement and, initially, all companies suffer a fall in value.
- However, some firms demonstrate that it is possible to create value from a crisis.
- The human death toll from a catastrophe amplifies the value impact.
- The presence of traditional insurance cover is not the key to assuring value recovery.
- Managerial responsibility for the loss determines the trajectory of value recovery.

[1] *The Impact of Corporate Catastrophes on Shareholder Value* (1993), by D. J. Pretty, Energy Insurance Review.
[2] *Reputation at Risk* (2000), by D. J. Pretty, Global Reinsurance.

By 2000, a fascinating emerging risk had established itself: reputation impact in the absence of physical loss. In 1999, 100 Belgian schoolchildren were taken ill following the consumption of Coke. As it transpired, it was a mass psychosomatic reaction and there was nothing wrong with the product. Over the following year, USD70 billion was wiped off the value of Coca Cola's shares; approximately 40% of market capitalisation. My next study focused on twenty-five reputation crises and the determinants of value recovery. Previous results are confirmed and new lessons learned.

2000 study results

- The roles of context and perception are critical in determining value impact.
- Strong leadership from the CEO is essential to inspiring confidence and value recovery.
- Swift corporate action fosters managerial credibility across stakeholders.
- Accurate and well-coordinated communications help to protect against value loss.
- Understanding of the need to restore trust accelerates the recovery of value.

> Cyber risk has arrived, sometimes with a vengeance, sometimes not.

Twenty-five years after my original work, and we are in 2018. Big data and technology dominate. No more the heroics required simply to find data, and the constraints of analytics or technology. Here we examine a portfolio of 125 reputation crises occurring over the last ten years. The context has changed considerably. Technology stocks ride high in the markets. Cyber risk has arrived, sometimes with a vengeance, sometimes not. The ability to make and disseminate news instantly and globally is the norm.

I hope that you will find this latest research of interest, as you strengthen your firms' resilience to the sudden and unexpected. I am very grateful to Aon, a leading global professional services firm, for their support of this work.

Dr Deborah Pretty
Director
Pentland Analytics

Executive Summary

The aim of this briefing is to take a fresh look at reputation risk and its dynamic with shareholder value in the advancing cyber age. Relentless technological innovation has provided us with tremendous opportunities. As with all opportunities before them, the attendant risks require active management if companies are to thrive and prosper.

The study portfolio on which this briefing is based includes 125 reputation crises occurring over the last decade, measures their impact on shareholder value and identifies the key drivers of recovery. Special attention is given to both the growth in social media and the value impact of cyberattack. The results complement those summarised in the Preface, and build a richer, more current profile of the dynamic between risk, reputation and value.

> Advancing technology has transformed the risk management landscape.

2018 study results

- The value impact of reputation events has doubled since the advent of social media.
- Crisis communications must be instant and global to spur a recovery in value.
- Active, social responsibility is a critical element of a value-creating response.
- New evidence explodes the myth that cyberattacks have no impact on share price.
- Neither firm size nor reputation premium offers any protection against value loss.

> Demands for greater social responsibility to be demonstrated by firms have intensified.

To place the results in context, this briefing first reviews the latest revolution in technology, the introduction of social media and the threat of cyberattack. Next, is presented new evidence of the impact of reputation crises on shareholder value and, in particular, the effects of social media and cyberattack. Finally, the consequences for reputation risk management by senior managers and corporate boards are outlined. Punctuating the analysis are four case profiles to highlight selected themes: the Samsung Galaxy Note7 recall (a failure in technology), the emissions software devices used by Volkswagen (an exploitation of technology), and the cyberattack to each of TalkTalk and Home Depot.

Advancing technology has transformed the risk management landscape. Many of the older dynamics and risk solutions remain, and apply equally to relatively new exposures such as cyber risk. However, new technologies continue to emerge (robotics, artificial intelligence and bionics, for example) requiring constant vigilance. Communications have changed - both the opportunity for error, punished by social media, and the accelerated response times that are now assumed. Demands for greater social responsibility to be demonstrated by firms have intensified. Or perhaps simply they return us to the early days of capitalism when such behaviour by firms was pioneered.

The portrait that emerges of reputation risk in the cyber age is one of exciting possibility and sobering concern. Corporate managers and boards seeking to exploit the opportunity and protect their firms against disruption will heed the lessons.

1 The Rise of Technology

The World Economic Forum[3] calls it the Fourth Industrial Revolution (4IR) – that is, the "fusion of technologies that is blurring the lines between the physical, digital and biological spheres". A new revolution that is distinct from the Third (digital) revolution in its sheer "velocity, scope and systems impact".

What is clear is that the business and risk landscape is shifting fundamentally, as the digital and physical worlds continue to connect and converge. Driving this change is unprecedented investment and innovation in technology.

Figure 1 shows the performance of the Nasdaq Composite Index over twenty years from the end of 1997 to the end of 2017. The so-called internet bubble and subsequent Dotcom Crash from 10 March 2000 to 2002 are conspicuous, and make the performance through the 2007-2008 Financial Crisis seem tame by comparison. Since then, technology stocks have soared. In the opening session of 2018, Nasdaq closed above 7,000 for the first time.

FIGURE 1
Twenty years of performance

On the facing page, is depicted a timeline of selected social media launches. There is a clear cluster in 2002-2006 and then again in 2009-2011, as social networking becomes ever more visual and compressed. Also illustrated is a selective timeline of milestones in the development of wireless, wearable and hearable technology.

[3] *The Fourth Industrial Revolution* (2016), by K. Schwab, World Economic Forum.

Social Media		Wireless/Wearable Technology
	1997	WiFi
	1998	
Blogger/Friends Reunited	1999	
	2000	Bluetooth headset, Blackberry, Microsoft Tablet
	2001	
MySpace	2002	Cloud technology, Nokia/Sanyo camera ‘phones
Skype, LinkedIn	2003	BlackBerry’s integrated ‘phone
Facebook, Flickr	2004	
YouTube, Bebo	2005	
Twitter	2006	
	2007	iPhone
	2008	First 3G ‘phone, Fitbit
Tumblr, WhatsApp	2009	
Instagram, Pinterest	2010	iPad, first 4G ‘phone
Snapchat, WeChat	2011	BYOD becomes mainstream, Siri
	2012	
	2013	Google Glass, Samsung Galaxy Wear
	2014	Alexa
	2015	Apple Watch, Ringly
	2016	Oculus Rift
	2017	Pilot hearables

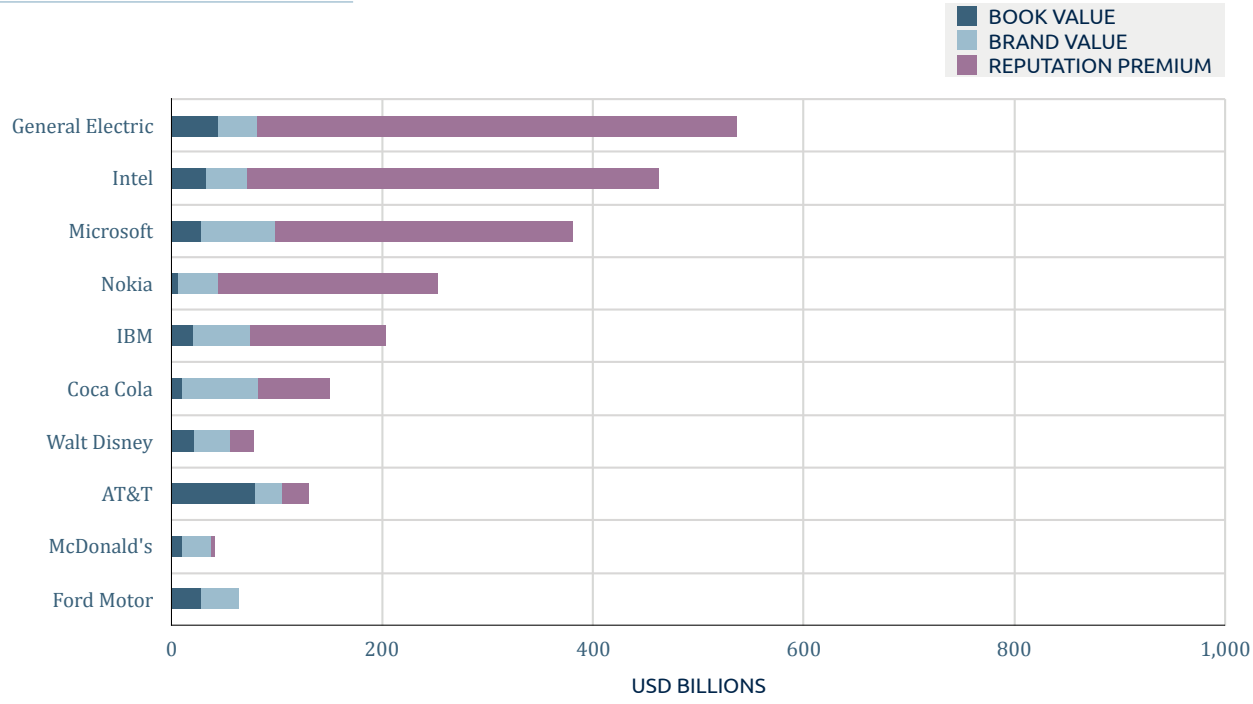
The combination of social media and wearable technology has had a pivotal effect on reputation risk (personal or corporate). People now have both the environment and the means, to capture and disseminate information, globally and instantly - information which may or may not be accurate.

> Social media and wearable technology have had a pivotal effect on reputation risk.

Presented in Figures 2 and 3 are the top ten corporate brands of 2000 and 2018, respectively[4] . Reputation premium in this context is defined simply as the excess of market capitalisation over the company's book value and brand value[5]. Reputation premium, therefore, reflects the earning power of the firm that is valued by investors but not captured in either the brand or net assets. In each case, the ten brands are ranked by their combined brand value and reputation premium, effectively their 'reputation at risk' [6].

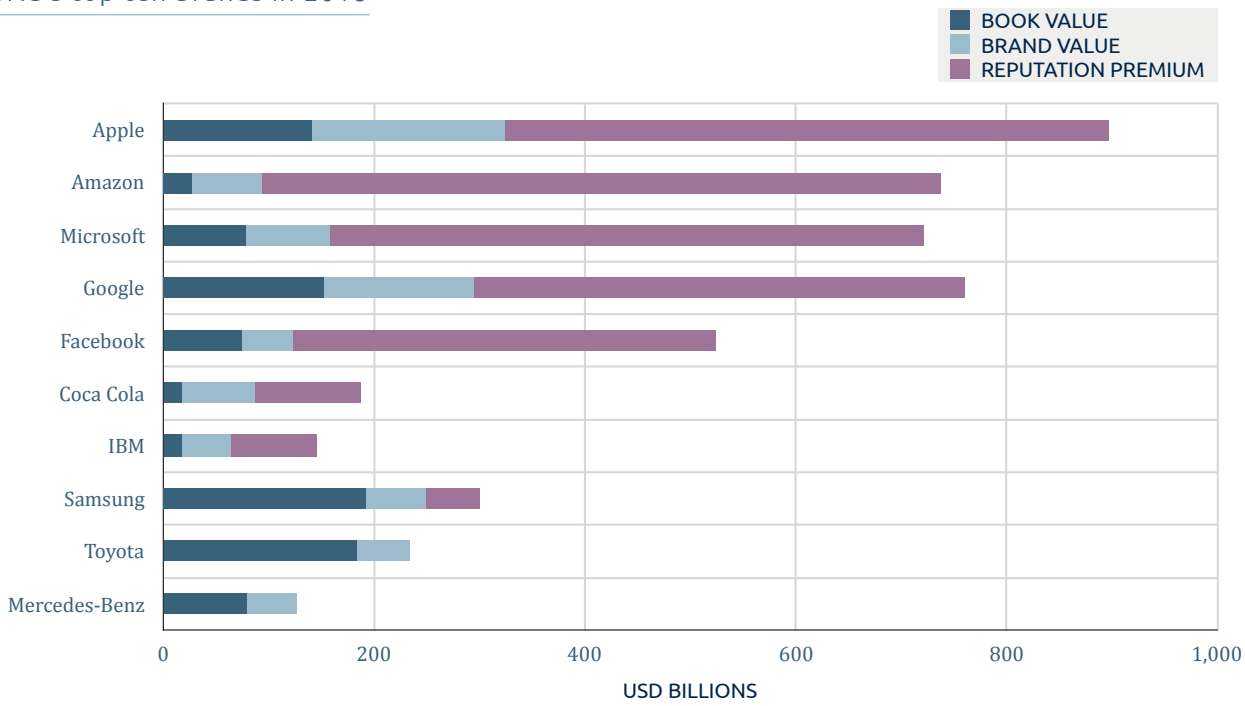
The difference in composition of the rankings is apparent, with technology firms occupying the majority of places in 2018 and Apple well on the way to becoming the world's first trillion-dollar company. Companies from the United States (US) dominate in both years and two new entrants appear from Asia in 2018: South Korean conglomerate Samsung and Japanese automotive company Toyota. Only three companies appear in both rankings: Microsoft, Coca Cola and IBM.

FIGURE 2
The world's top ten brands in 2000



[4] Source of brand values: *Interbrand Best Global Brands* (2000) and (2017).
[5] Market capitalisation and latest book values dated 21 July 2000 and 5 March 2018, respectively.
[6] Financial data for parent companies Alphabet and Daimler, respectively, are used for brands Google and Mercedes-Benz.

FIGURE 3
The world's top ten brands in 2018

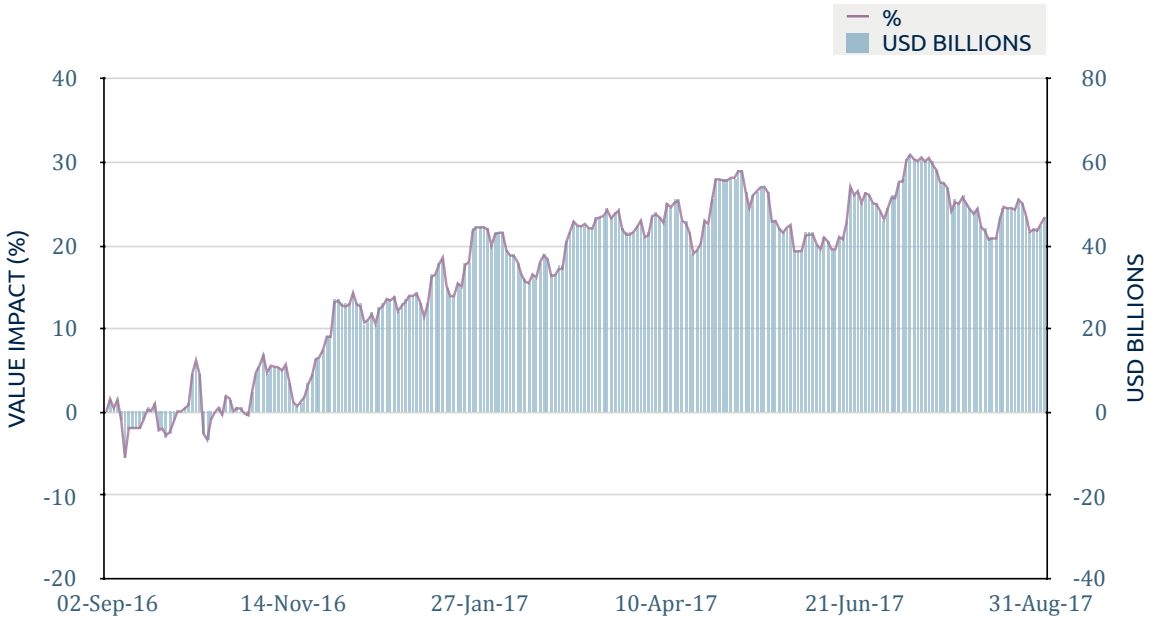


Innovation in technology is changing radically the world in which business operates. Simply keeping up with the pace of change (and the changing expectations of customers, suppliers and employees) is very challenging. New, disruptive technologies bring also new risks for companies to manage, exploit and guard against. The risk implications of connected, 'smart' devices through the Internet of Things (IOT), and developments in quantum computing, robotics, artificial intelligence and bionics have yet to become clear, while the risk of cyberattack is visible already. Algorithmic bias in these new technologies threatens not only the effectiveness of their application, but also the reputations of the companies that design and supply them.

> Technological developments heighten reputation risk by making it easier, cheaper and faster for people to spread news.

Personal technology has undergone an extraordinary transformation over the last twenty years. First, we didn't have it. Then we had to plug it in. Then we had to carry it. Now we have to wear it. Tomorrow, perhaps we implant it or apply it as graphene transfers. All of these technological developments heighten reputation risk by making it easier, cheaper and faster for people to spread news.

Samsung Galaxy Note7 recall



Lessons

Respond globally – rather than announce a series of national recalls, piecemeal, Samsung recognised that operating in a global market requires a global response.

Be decisive - the decision to halt production of the Note7 permanently contained the reputational fallout to a single device and curbed the damage from spreading too far across the brand.

Be open – beyond the contrite apology, Samsung disclosed precise details of the units affected and, in due course, of the technical flaws in the battery design and manufacturing.

Make amends – in this case, by committing to environmental stewardship and launching great new products.

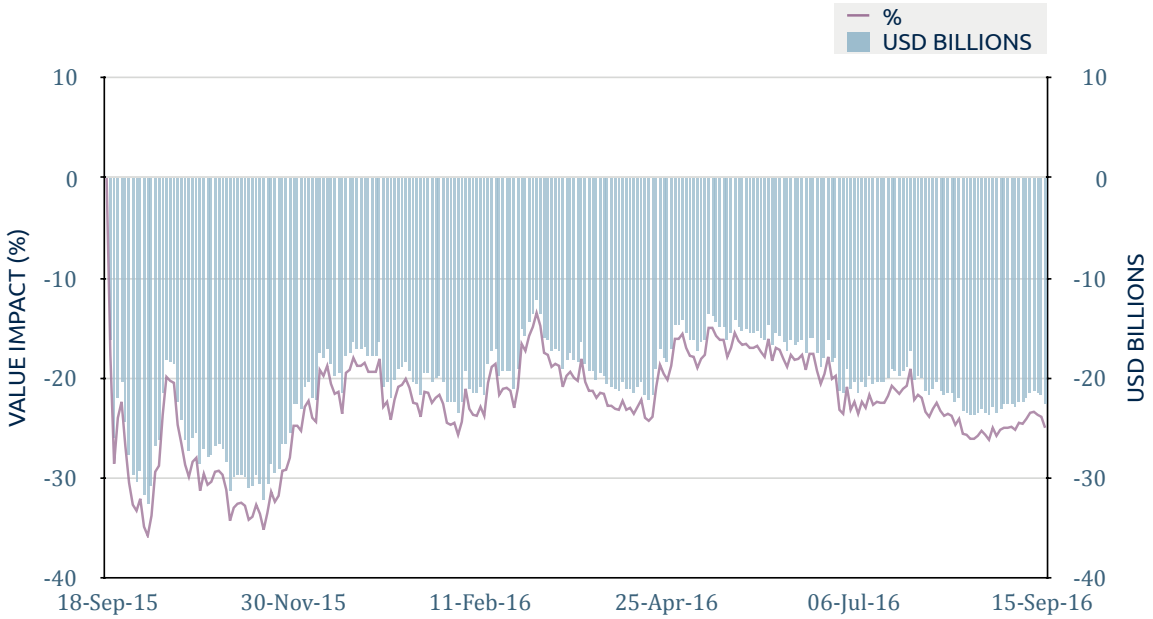
Case

South Korean technology firm, Samsung Electronics, unveiled its Galaxy Note7 smartphone in New York on 2 August 2016 to great fanfare, beating the launch of arch-rival Apple's iPhone 7. Exactly one month later, Samsung announced a global recall of 2.5 million units, following reports of handsets overheating and catching fire. As safety concerns mounted, telecommunications companies halted issuance of the handsets and they were banned from major airlines. It soon became clear that the replacement units were faulty also and a second global recall was announced. The cause ultimately was identified as a design flaw in the original batteries and a manufacturing defect in their replacements. On 11 October, Samsung suspended permanently sales and production of the Galaxy Note7.

Consequences

The recall is estimated to have cost Samsung over USD5 billion. The considerable brand value and reputation premium of Samsung were threatened substantially but withstood the pressure and, a year later, almost USD50 billion (over 20%) in shareholder value had been added to the company. All this, amid a massive corruption scandal and a corporate leadership on trial. In July 2017, Samsung launched the Galaxy Note Fan edition, which comprised components of new, unsold Note7 handsets and attempts thereby to minimise the adverse environmental impact. There is also a plan to extract 157 tons of gold, silver, copper and cobalt from used devices, and reuse camera models and displays. The Galaxy S8 was unveiled on 29 March 2017, and has enjoyed positive reviews and strong orders.

Volkswagen emissions software



Case

Not the only auto manufacturer to do so, Volkswagen installed in its vehicles software devices designed to falsify emission levels during testing. Following Volkswagen's formal admission to the US Environmental Protection Agency (EPA), the agency issued on 18 September 2017 a public notice of violation of the Clean Air Act. From an initial estimate of 500,000 cars in the US being affected, Volkswagen revealed that 11 million diesel cars could be affected worldwide. The company suggested that customers could have their vehicles fixed on a voluntary basis and offered US customers the opportunity to apply for a USD500 pre-paid card to do so. On 15 October, the German auto industry regulator ordered a product recall. Stories of Volkswagen obstructing official investigations filled the headlines as internal files and emails allegedly were destroyed or withheld from regulators.

Consequences

Five days after the EPA disclosure, Volkswagen's Chief Executive resigned. By the end of the year, concerns had spread to petrol engines, Volkswagen had posted its first quarterly loss in fifteen years and the automaker was suspended from the FTSE4Good ethical index. Estimates of direct costs, compensation and environmental repayments are over USD20 billion, approximately half of which is allocated to buyback offers. A year after the EPA disclosure, and the value loss also is over USD20 billion; approximately 25% of Volkswagen's pre-crisis value. Under agreement with the US Justice Department, Volkswagen must cooperate in the investigation and allow an independent monitor to oversee compliance for three years.

Lessons

Embrace standards – from alleged misconduct, it's a long road back to trust.

Recognise the task – to rebuild trust requires the company to go above and beyond a minimum, national offer that appeared to undermine the credibility of remorse expressed.

Be transparent – when the apparent error has been to deceive, any perceived opacity in response will only make matters worse.

Protect your brand – the software devices pierce the heart of VW's brand values of environmental stewardship and technology for good.

2 Social Media, Cyberattacks and Shareholder Value

Presented in this section is new evidence on the dynamic between reputation risk and shareholder value. The research summarised examines a portfolio of 125 reputation events occurring over the last decade: the 2018 study portfolio.

Reputation risk does not discriminate by industry or country, and the study portfolio encompasses a wide range of each. Equally diverse is the root cause of each crisis analysed. The study includes, for example, mass fatality events, poor governance and business practices, product and service failures, cyberattacks, accounting irregularities, and marketing and communication blunders.

The research addresses three key questions:

1. Has social media affected the value impact of reputation crisis?
2. Have the drivers of value recovery changed since the advent of social media?
3. Do cyberattacks impact shareholder value?

FIGURE 4
The impact of reputation crisis on value

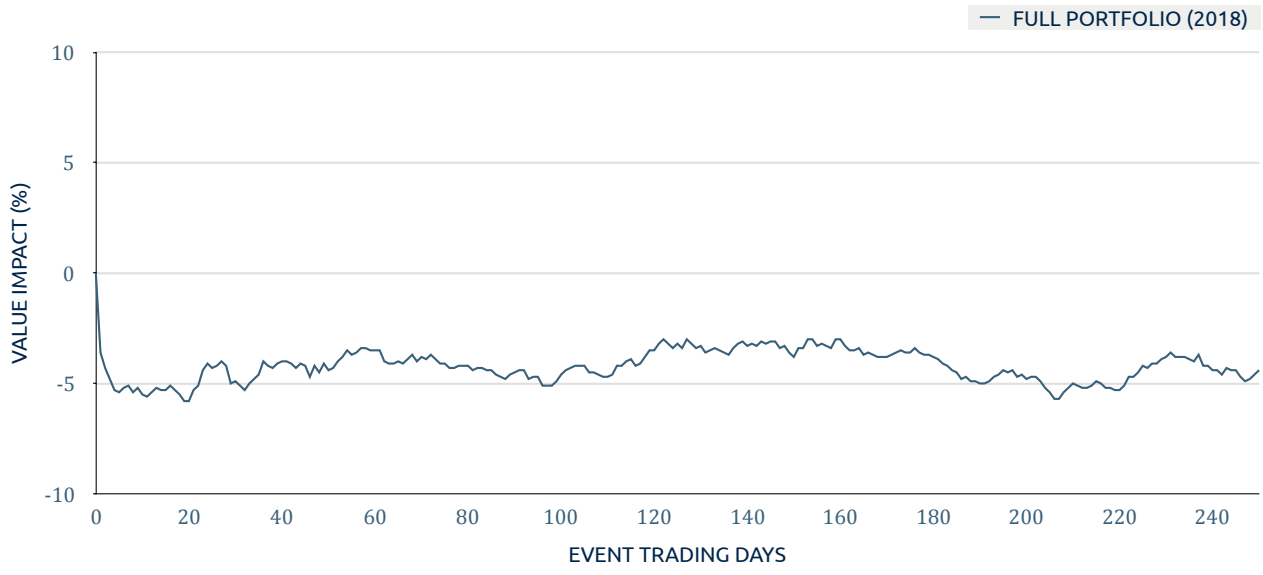


Figure 4 shows the impact on shareholder value of the portfolio of reputation crises for one calendar year (252 trading days) following each event. The calendar dates of all crises are converted into event time and aligned such that Event Day 0 is the day each crisis broke, irrespective of calendar date or stage in the market cycle. Daily share prices are modelled against the relevant market index to measure the excess returns, and all returns are risk-adjusted using pre-crisis data. These procedures ensure a clean measurement of impact, specific to the company and beyond market fluctuations and cycles.

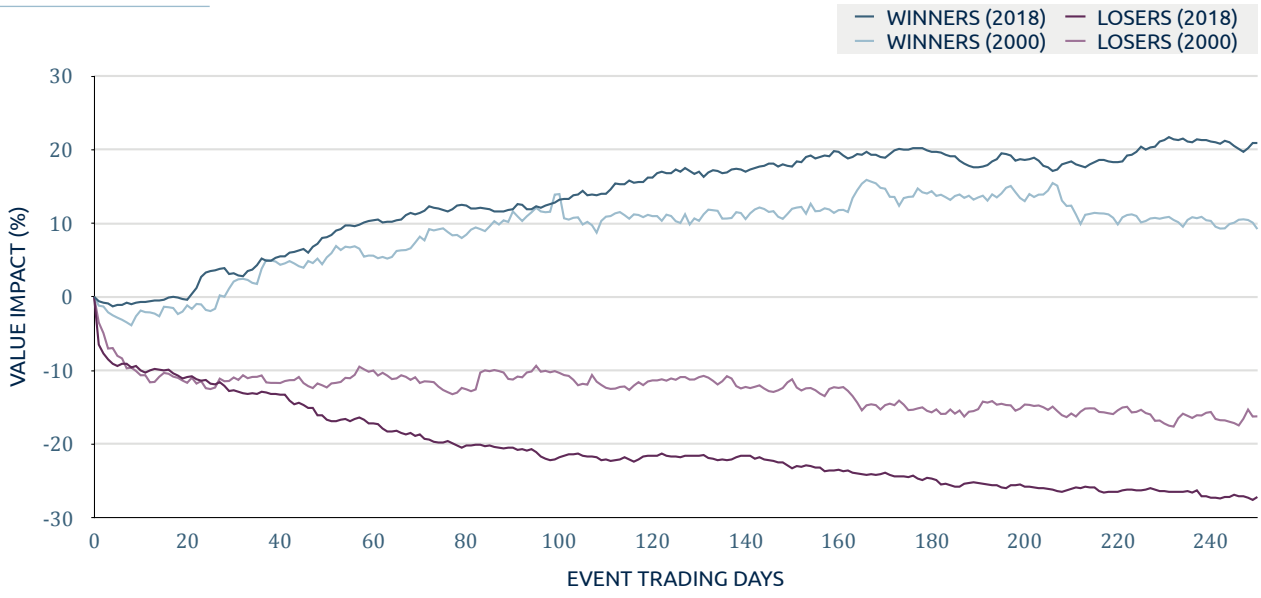
On average, 5% of shareholder value is lost over the post-event year. A company's equity beta is 9% higher than in its previous year, directly impacting the firm's cost of capital. However, this average picture masks significant differences across firms in their ability to recover value following a reputation crisis.

> Winners go on to outperform investors' pre-crisis expectations.

The results shown in Figure 5 support the 2000 study which demonstrates that companies fall into two relatively distinct groups, according to their value trajectory following crisis: Winners and Losers. The Winners from the 2000 study go on to outperform investors' pre-crisis expectations and proceed, on average, to gain 10% in value over the first year. In contrast, the Losers from the 2000 study experience a sustained fall in value of approximately 15% on average. The market is rapid in its judgement as to which group a company will belong and it takes only a few trading days for the divergence in performance to become clear. The value loss by Day 5 is a strong predictor of the value position at the end of the post-event year.

Whereas the 2000 study portfolio is before social media entered our lives, the 2018 portfolio reflects entirely a post-social media world. The shareholder value gained following reputation crises by these more recent Winners is 20%, while the value lost by the Loser portfolio is close to 30%.

FIGURE 5
Winners and Losers



The full portfolio is split fairly evenly across the two groups, with 61 Winners and 64 Losers. Neither the size of firm, nor the size of reputation premium a firm enjoyed prior to the crisis, offers any protection against value loss. Other factors certainly will be at play but it is striking that, for both Winners and Losers, the post-crisis value impact in a social media world is double that of the pre-social media portfolio.

> The value impact of reputation crises has doubled since the advent of social media.

Neither group escapes a higher equity beta in the aftermath of reputation crisis; the Winners on average have a beta 6% higher than over the pre-crisis year while the Losers' beta is up 12% on average. A higher equity beta increases a firm's cost of capital, signalling higher risk associated with the firm and suggesting that a higher return would be required by investors to assume additional risk.

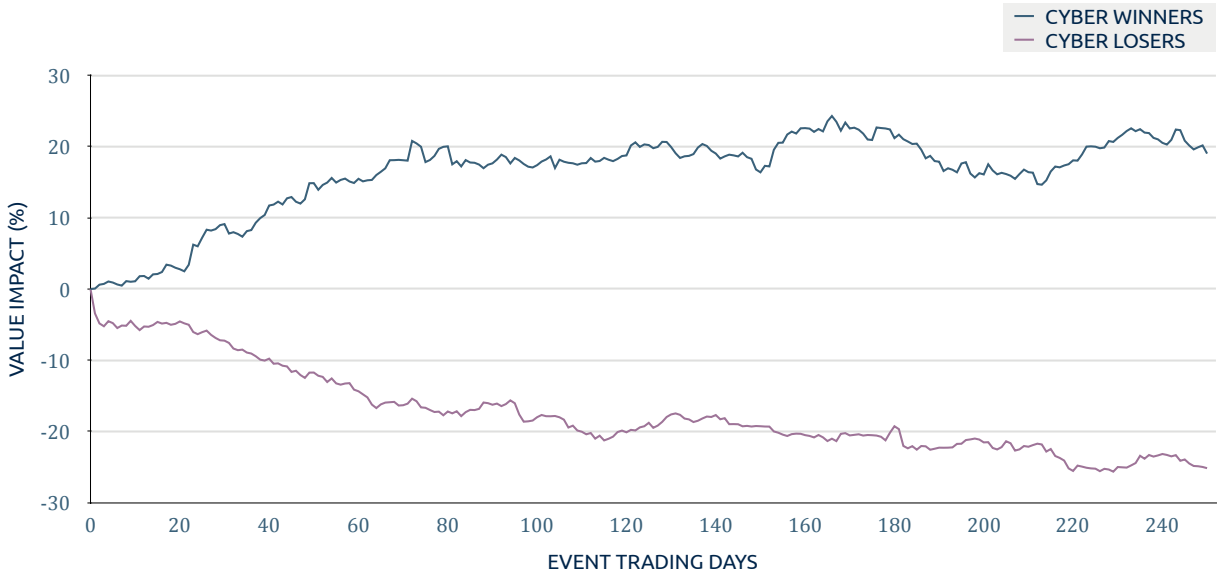
At times of crisis, the market receives substantially more information about a company and, in particular, about its management, than would be received in usual circumstances. Investors use this additional information to re-assess their expectations of future cash flow. The result of this re-estimation process is a dramatic divergence in the consensus view that is reflected in the market price. Some management teams impress, and expectations of future performance are even higher than prior to the crisis. Others disappoint, and investors' confidence in the ability of management to generate value is shattered.

Another key difference in the two studies lies in the composition of portfolio. In the 2000 study portfolio, there was no example of cyberattack whereas the 2018 study portfolio includes 23 cyberattacks (approximately 18% of the portfolio). This is a sign of the times and a warning of what is to come.

Much has been written about the apparent absence of share price impact from prominent data breaches. Commentators have pointed to isolated examples, without modelling, and observed that any impact on share price appears to be short-lived. The evidence suggests otherwise.

> It is increasingly important that reputation risk management strategies embrace in their scope cyber risk and exposures from emerging technologies.

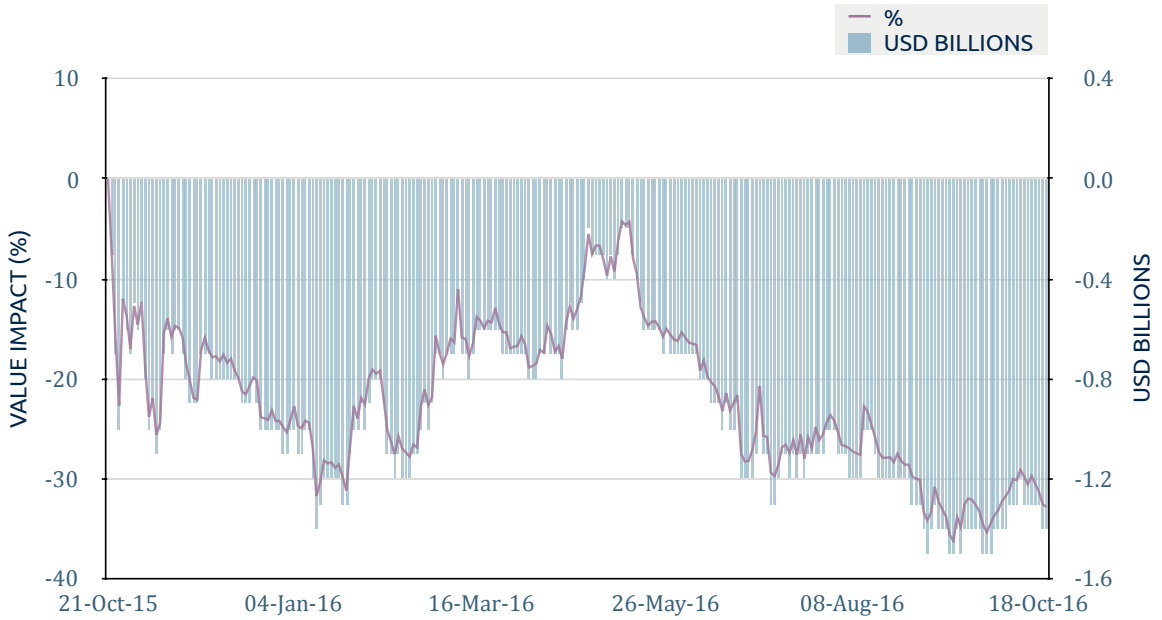
FIGURE 6
The impact of cyberattack on value



Shown in Figure 6 is the sub-portfolio of cyberattacks and their impact on shareholder value. Once again, the now familiar pattern of Winners and Losers is apparent. The winning portfolio adds approximately 20% in value over the post-event year whereas the losing portfolio suffers a sustained fall in value of approximately 25%; not so different from the full portfolio of all types of reputation crisis. The dynamic is no different, as investors make an assessment of managerial capability and the company's prospects for generating future cash flow. It is increasingly important, therefore, that reputation risk management strategies embrace in their scope cyber risk and exposures from emerging technologies. The impact of cyberattack on shareholder value can be substantial and sustained.

The next section addresses questions of value recovery: why do some firms recover better than others, and have the drivers of recovery changed since the advent of social media?

TalkTalk cyberattack



Lessons

Know the facts – match the response to the evidence and communicate what is known to be true.

Respond immediately - the CEO apology video was released two days after the attack became known, by which time social media had appropriated the story.

Be coherent – expect scrutiny from experts and prepare to communicate the core technical details, particularly where the reputation event is technology-related.

Test the plan – a robust and tested incident response plan is essential to avoid it taking, "longer than expected to return the business to normal operational effectiveness".

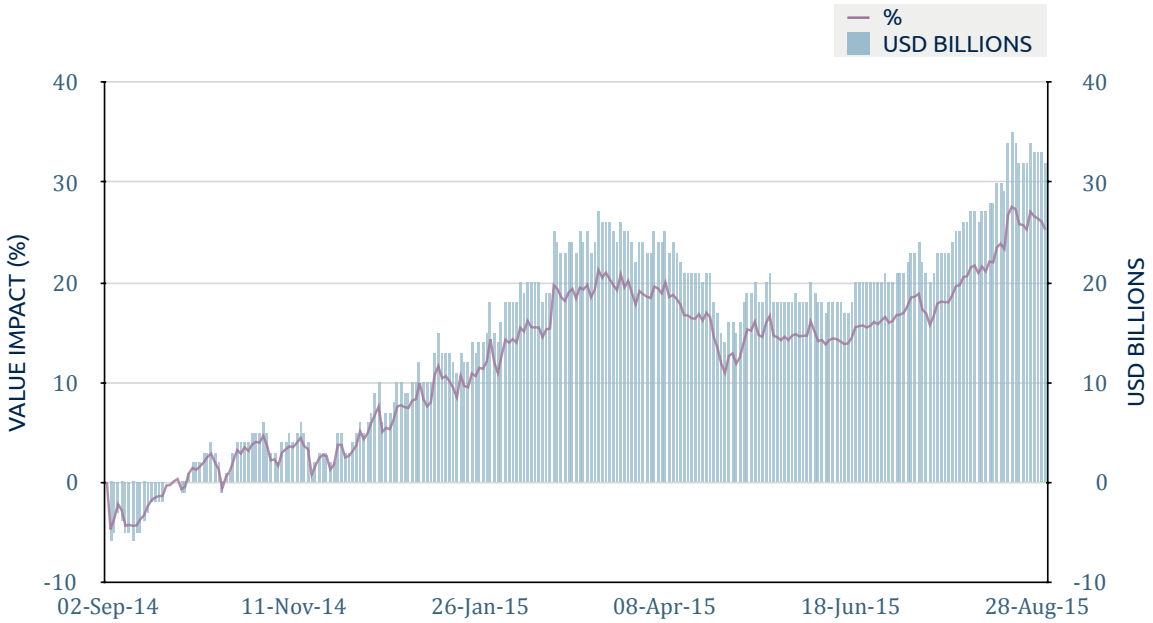
Case

News first broke that something was awry when UK telecommunications firm TalkTalk revealed on 21 October 2015 that its website was unavailable due to "technical issues". Later the same day, the company disclosed that it had taken the site down deliberately. The following day, TalkTalk confessed that it had done so because it knew that it was the target of a cyberattack and, one day later, revealed the attack to be, "significant and sustained", with a chance that customers' personal data had been compromised. At the time, it was believed that up to 4 million customers could be affected. Communications continued in this vein, emerging from the company piecemeal and often less than technically coherent. TalkTalk's CEO made every effort to be visible, take responsibility, and prioritise customers but patchy technical knowledge undermined credibility.

Consequences

By 6 November, TalkTalk revealed that the personal details of 156,959 customers had been hacked. With the benefit of hindsight, the company's well-intentioned and immediate response appeared to have been overdone. The attack cut trading revenue by over USD20 million, forced TalkTalk to book exceptional costs of between USD60 million and USD70 million, and resulted in the loss of 101,000 customers. By the end of the post-crisis year, one-third of the company value had been wiped off shares; approximately USD1.4 billion. As always, context played a role. It was the third data breach to affect TalkTalk in 2015 and, in its July update, the company had warned of weaker demand for broadband services.

Home Depot cyberattack



Case

On 2 September 2014, Home Depot opened an investigation into a potential security breach of its payment card systems. A statement on 18 September revealed the breach not only to be real, but the largest of its kind, exposing the details of 56 million customers' debit and credit cards, and dwarfing the 40 million cardholders affected by the Target breach the previous year. The malware that stole the data had resided on Home Depot's computer systems since April, and was custom-made by the hackers and so able to avoid detection by traditional anti-virus software. In the wake of the theft, Home Depot offered customers free credit monitoring, took the affected terminals out of service, eliminated the malware from its computer systems, rolled out enhanced encryption technology and continued to follow its Incident Response Plan.

Consequences

Estimates place the cost of the attack at USD10 billion. Home Depot performed strongly following the data breach, adding over USD30 billion (25%) in shareholder value by the end of the post-crisis year. Arguably, Home Depot's greatest asset in its hour of need was its chairman, whose response to the potential reputation crisis was immediate and unwavering. Also in Home Depot's favour was its dominant position in the US home improvements market, with an approximate 60% market share, and the fact that it was not the first retailer to suffer from a major security breach. The company thereby escaped some of the more dramatic headlines swirling around Target in the wake of its breach at the height of holiday season in 2013.

Lessons

Prevention is key – the breach may have been prevented if Home Depot had responded more quickly to warnings from security experts following the prior breach to Target.

Take responsibility – despite being just weeks from retirement, rather than passing responsibility to his successor, Home Depot's chairman embraced accountability, empowered his team to fix the problem and gave customers top priority.

Respect your customers – communications went beyond the technical, and showed understanding of the customer experience: fear and frustration.

Respond rapidly – remedial action was swift, efficient and customer-focused.

3 Consequences for Reputation Risk Management

The clear divergence in performance between the Winner and Loser portfolios begs the question as to how to ensure that one's company is firmly in the value-creating group.

The original research in 1993 established that the key determinant of value recovery following crisis was related more to managerial factors than to the direct financial consequences of the loss. Whilst the initial impact on share price was correlated with immediate market estimates of financial loss, the subsequent recovery in value was influenced more by issues of managerial responsibility and behaviour.

The subsequent reputation risk study in 2000 examined the issue more deeply, and identified specific attributes associated with the Winners and Losers. Strong, visible leadership from the Chief Executive Officer, swift and credible action to rectify the situation, accurate and well-coordinated communications, and a sensitive understanding of the scale of the task and the need to restore trust, are all critical factors associated with value creation following a reputation crisis.

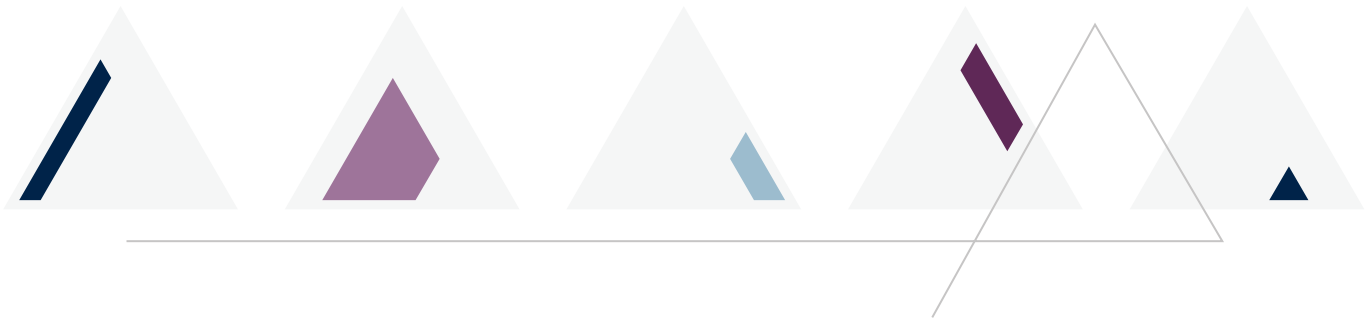
The new, 2018 study endorses the previous results and introduces further evidence that can be attributed to the power of social media, technology and contemporary culture. First, to have any chance of recovering shareholder value and being a member of the winning portfolio, requires that crisis communications be not just swift, but instant and global. This is demanding, especially when complete information at this stage of a crisis is a rarity, but social media is unforgiving.

Greater investment in preparation and rehearsal, and in risk monitoring, such that management is better informed, earlier, is no longer a luxury and will bring rewards when crisis strikes. Technology can help in both respects. Virtual reality simulations, for example, confront us in ways unachievable through more traditional means, and the use of industrial sensors and interconnected 'smart' devices increasingly will allow crucial data to be fed back to senior managers in real time.

The second new attribute to be associated with the winning portfolio is in recognition that cultural expectations are shifting. It is almost assumed now by all stakeholders, but particularly by customers, employees and the general public, that companies should atone for their mistakes and do so conspicuously. In some cases, the reparation demanded can be achieved only through a programme of active, social responsibility that is associated directly with the crisis.

> For executive management, the lessons are clear. There is no hiding place from reputation risk or the advance of technology.

For executive management around the world, the lessons are clear. There is no hiding place from reputation risk or the advance of technology and, on the contrary, the opportunity exists to create significant value, even at times of crisis. Effective preparation lies in remaining vigilant, flexible and open-minded as to emerging technologies, while recognising their potential to disrupt well-laid plans.



About the Author

DR DEBORAH PRETTY

Deborah is the founding director of Pentland Analytics. She is a recognised expert in devising algorithms to solve complex business problems and yield new, actionable insights.

Deborah's research has been published extensively in academic and professional journals, and she has been honoured as guest speaker at numerous conferences around the world. Deborah authored the book, *Risk Financing Strategies – the impact on shareholder value* (1999), and served for many years on the editorial advisory board of *Corporate Finance Review.*

Following her Research Fellowship at the University of Oxford, Deborah co-founded strategic advisory firm, Oxford Metrica, where she remained as Principal for fifteen years. She worked previously as an Assistant Director at Sedgwick Oil & Gas, and as a risk analyst at Tillinghast in London and the United States.

About Aon

Aon plc is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

aon.com

About Pentland Analytics

Pentland Analytics provides advanced analytics and advisory services to the executive management of the world's leading companies. The firm converts complex business issues into analytics solutions that yield clear insights and direction. The results inform strategic decisions and help to build clients' resilience, reputation and shareholder value.

pentlandanalytics.com