KPMG
cutting through complexity

Technology Risk Radar

Second Edition – Corporates

kpmg.co.uk

Introduction

Jon Dowie

Kiran Nagaraj

Andrew Shefford

Paul Holland

Technology failures, data losses and other incidents are increasingly in the news. How does one filter through the noise? In the 2nd edition of the Technology Risk Radar, we seek to apply data analytics to better understand the evolving risk landscape.

In this Corporates version we have surveyed KPMG industry specialists and asked them to provide a forward-looking perspective on the top risks which they believe the Consumer Markets & Retail, Technology, Media & Telecom, Healthcare, Pharmaceuticals, Oil & Gas, and Transport industries will face in the next three years. We then conclude with some practical tips from our risk management specialists on what organisations can do to address some of these risks.

Why does this matter? Technology is no longer a functional area within a business operating in isolation. Those days are long over. Increasingly, businesses are seeing themselves first and foremost as technology companies, with the technology sitting at the centre of the value chain and their core operations. The fact that technology is at the heart of everything we do, makes it all the more crucial for businesses to understand the risks associated with IT – first their cause, but just as importantly, how they can be managed, mitigated or avoided.

Based on feedback from our readers and our clients, we have extended both the scope and the methodology of our analysis from 2013 to present a broader picture that can help business leaders focus on the main threats to which technology can leave them vulnerable. Cyber security-related risks still dominate some industries. But, as the findings clearly suggest, other core technology risks – such as availability and quality – need to be brought to the fore.

Past incidents can provide an indication of the risks that organisations face regarding their technology systems and infrastructure. Together with a forward-looking perspective and risk mitigation options, we hope this report will be a useful tool in informing risk assessment activities and prioritising risk mitigation investment, as well as benchmarking.

The Technology Risk Radar is relevant – indeed essential – reading for a wide audience. The most likely readers are Chief Information Officers, Chief Risk Officers, Heads of Audit and Chief Operations Officers. It's also vital reading for those with an interest in technology risk and control, including Executive and non-Executive Directors.

Our message to these readers, based on our findings and our experience, is that organisations need to do more to avoid the avoidable and exercise better control over their technology environments, processes and people. The only way to achieve this is by elevating the profile of technology risk. We have already seen some organisations use technology risk management not only for value protection, but also to drive competitive advantage. We believe that this will be the way forward.

Investments in technology will continue to rise as businesses embrace digital and other opportunities, but this needs to be matched by investments in assessing, managing, mitigating and monitoring the associated risks. At a time, when even our regulators have shown themselves to be vulnerable to technology risk, no one can afford to be complacent.

> ***"We hope this report will be a useful tool in informing risk assessment activities and prioritising risk mitigation investment, as well as benchmarking."***

Produced by CREATE | August 2015 | CRT039402

Contents

1

Media-reported events: key findings

2

Looking forward: top ten risks

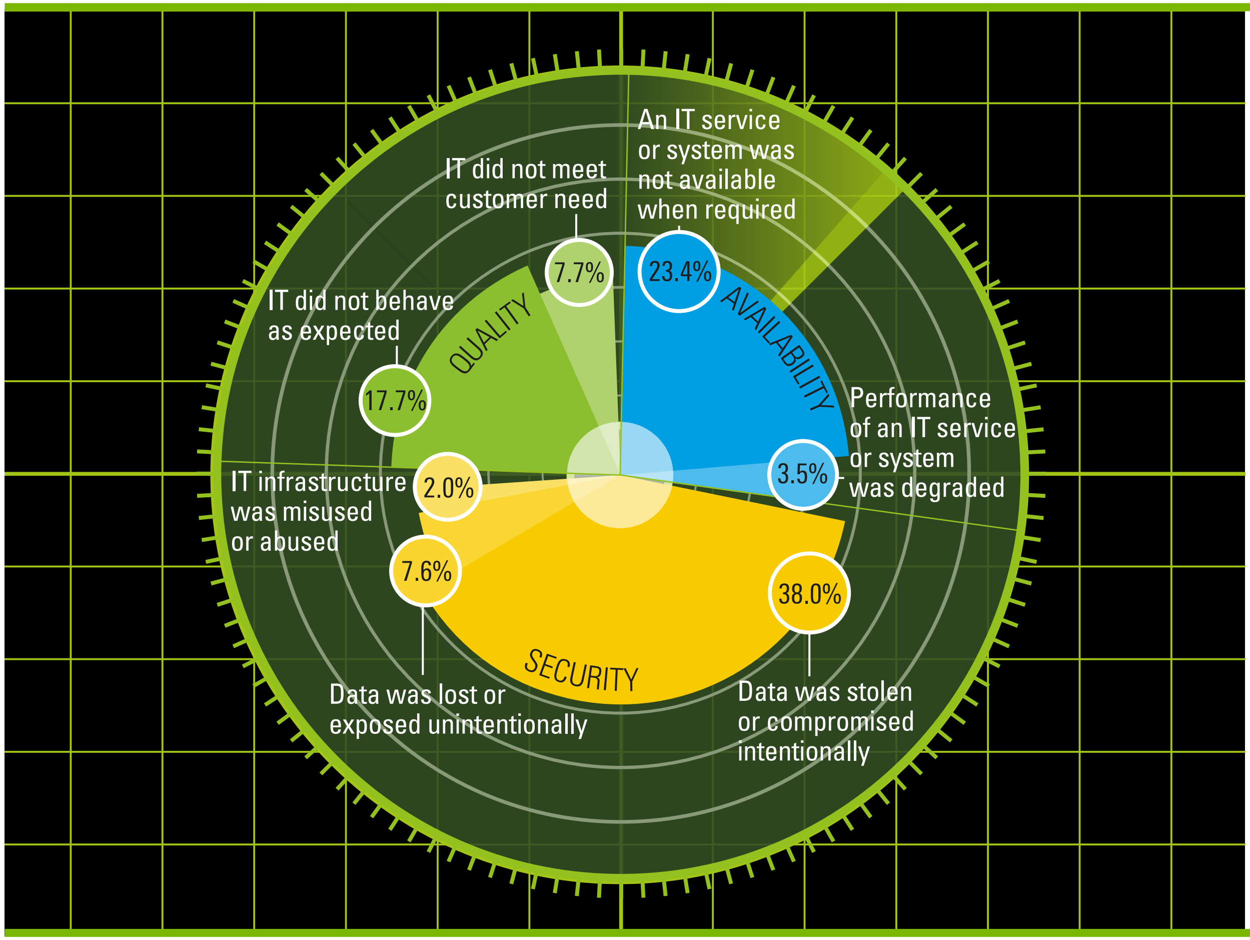
3

Responding to technology risks

1.

Media-reported events: key findings

Media-reported events: key findings – What happened?



One of the most interesting findings is that what while cyber security tends to be the attention-grabbing element of IT risk, security-related incidents accounted for less than half of the total number of incidents.

The very term "security" usually conjures up visions of theft. And yet a considerably large number (nearly 16%) of the security issues involved the unintentional loss or exposure of data. This proportion is even higher in some industries – almost 36% in Healthcare & Pharmaceuticals. These statistics are alarming as these incidents must arise from a failure of internal controls – checks which should be a basic element in any security control system, technological or otherwise. Cyber security continues to be a key area of concern for organisations. Later in this document, our cyber security specialists provide some practical insights on how organisations can protect themselves and better prioritise their investment in this area.

Availability accounted for about 27% of all incidents in our analysis. Financial Services and Technology was the industry with the highest proportions (almost 40%) of incidents related to availability. You may be thinking: what about the incidents that didn't make the news?

- *Some incidents may have resulted in more than one type of impact (e.g., an incident could have caused data loss and service outage)*

See Appendix for more details on how we obtained and analysed the incident related data used in this section

Produced by CREATE | August 2015 | CRT039402

Media-reported events: key findings – What happened? (continued)

Indeed, internal operational failures aren't typically made public. It is clear from our analysis that the incidents that do make into the news may just be the tip of the iceberg. While regulation in some industries requires that a loss of data or data theft be disclosed, there is generally no such requirement for internal operational failures such as server outage. So, given that the lack of availability is a top risk facing organisations, what approach should companies adopt to address this? Later in this document, our specialists discuss some ideas to improve technology resilience.

More than one-quarter of incidents concerned IT quality issues. We believe that this proportion will rise as businesses introduce new technology to digitise more of their processes. Risks change in step with the introduction of new technology platforms and processes – and so should the investment to manage and deal with the resultant risks. The right level of technology governance and programme management capabilities should enable an organisation to deliver its technology projects on time, to budget, and to requirements, creating a win-win situation for all the organisation's stakeholders.

Many already recognise that IT risk is about much more than cyber security. Our findings help reinforce this view. The results from the Radar emphasise the need for organisations to take a more integrated approach to any technology risk management exercise and make sure they it fully consider the risk landscape. Availability and quality considerations should not be over-looked. Indeed, we have seen a focus by some regulators on resilience and system availability.

Technology risk management is very much about protecting organisations from direct and indirect financial impact. From our analysis, we estimate that on average, an IT incident can cost the affected organisations over £410,000 – slightly higher than the average cost of a data breach as estimated recently by the Ponemon Institute. While media-hype continues to focus on the generally more sensational and emotive incidents such as cyber attacks and data breaches, our analysis suggests that system outages and IT quality issues can prove to be just as costly for organisations.

By the numbers

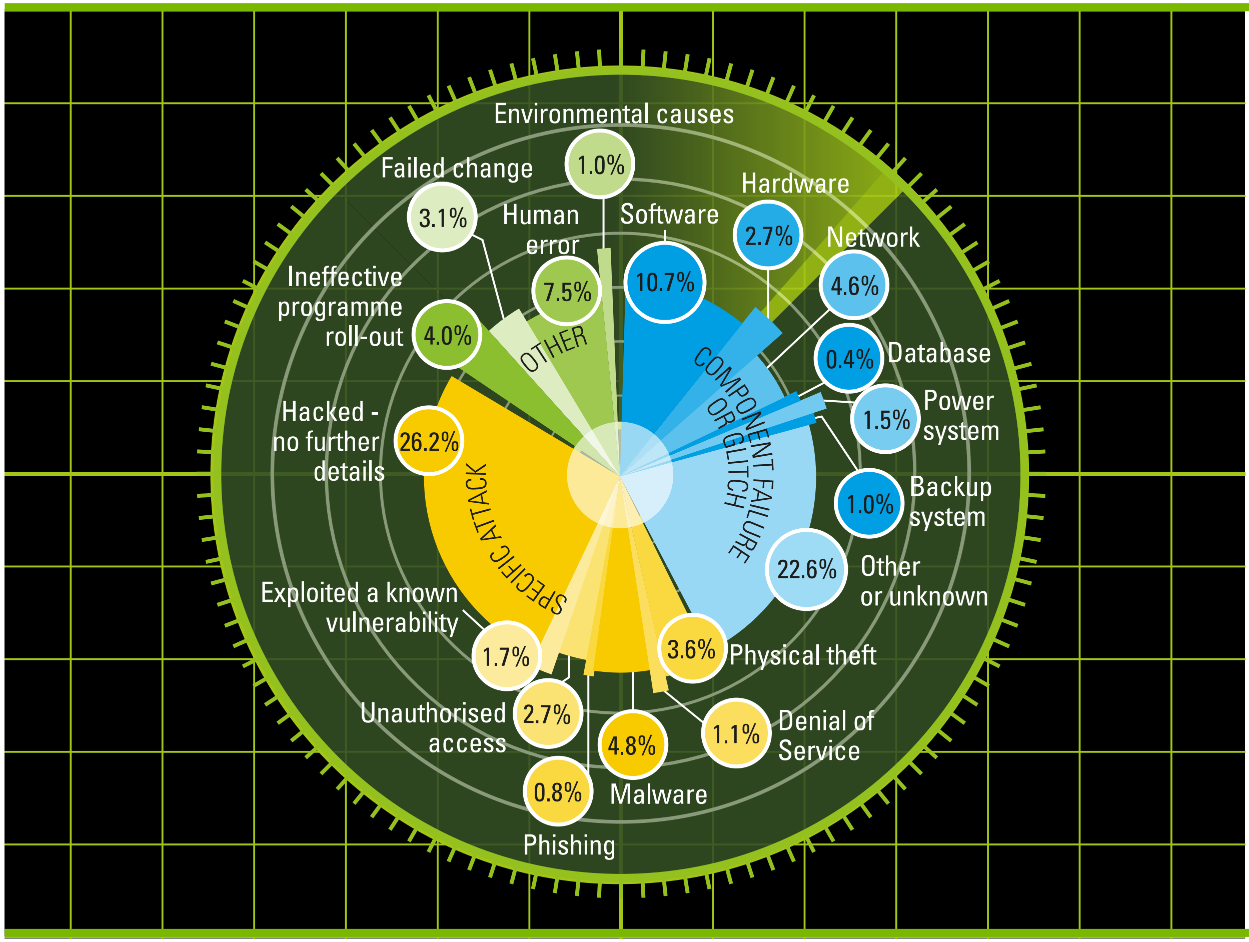
£410,000
Approximate price tag for an IT incident

4 million
Average number of financial accounts (e.g., credit cards) affected by an IT incident

776,000
Average number of people (e.g., individuals, patients, employees) affected by an IT incident

• Based on a subset of incidents which had relevant data publicly available

Media-reported events: key findings – What were the causes?



We found that a shockingly high proportion of incidents were caused by factors generally considered as "avoidable". Avoidable causes such as component failures, programme or change failures and human errors led to more than one-half of the incidents. These are considered avoidable as component failures, for example, can be prevented by taking the right precautions, exercising vigour on testing components and building the right level of resilience to enable failover.

The leading culprit for component failures was software. Where information was available about the specific component that failed, nearly one-half (51%) related to software. Organisations could implement better testing practices and improved software quality management approaches (including for outsourced services) that can reduce this risk.

Specific attacks continue to be a major threat. But it's worrying to see that a number of organisations still aren't getting some security basics right. Physical theft was surprisingly high, accounting for about 24% of cases where the cause was a known type of specific attack. Physical security is generally thought to be a mature control area for organisations, but it would appear this is not always the case.

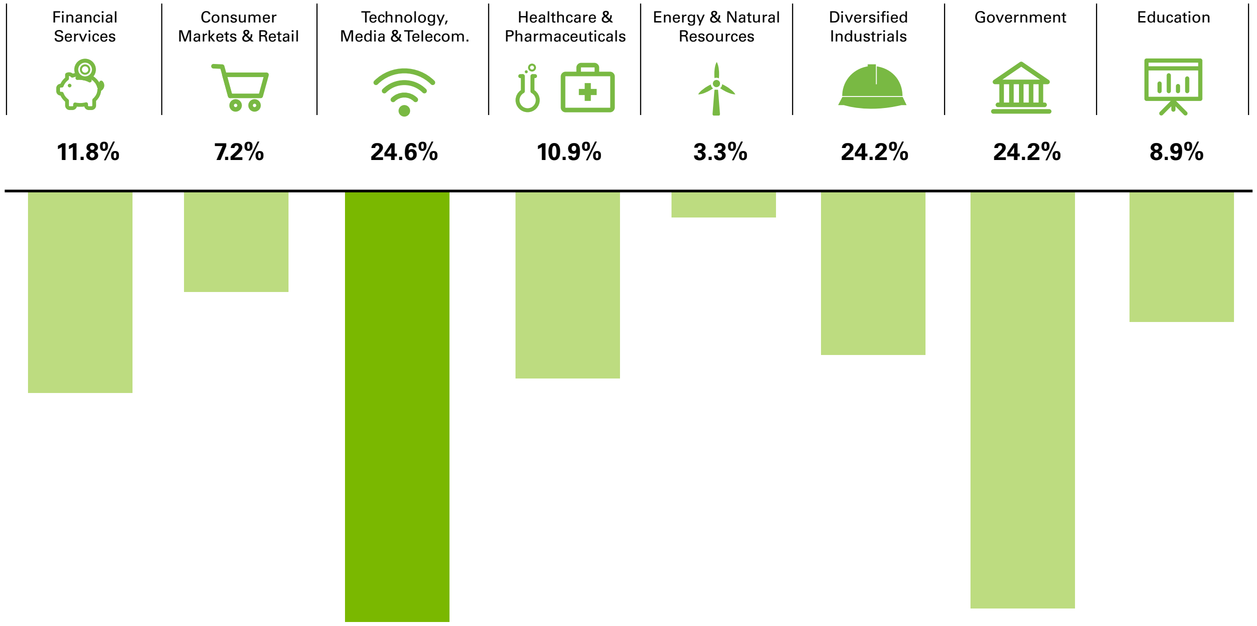
Media-reported events: key findings – What were the causes? (continued)

Human errors (e.g., information sent to wrong recipient, data entry error, etc.) contributed to more than 7% of incidents – a high proportion given that in today's digital age many controls are automated. Any investment in technology should be accompanied by investment in training and awareness – a point which a number of organisations have clearly ignored to their cost.

There's a common theme which runs through the incidents described here – the importance of better risk management and controls. There is little an organisation can do to avoid being attacked by hackers. But all organisations can continually monitor their risk safeguards and prioritise action against IT risks. Later in this document we talk about the need for better governance and oversight, particularly for tomorrow's technology. We also discuss how to build a better risk management capability to ensure the business, its customers, the Board and IT itself are protected.

Avoidable causes such as component failures, programme or change failures and human errors led to more than one-half of the incidents.

Media-reported events: key findings – Which industries were affected?



Click on the industry icon above to find out more about what happened within each industry.

The top three industries affected were the same as in 2013, although their rankings have changed.

Technology has now the dubious privilege of being the industry most affected by IT incidents, according to our research. The growth of the Internet of Things and the ubiquity of devices suggest that this industry will keep this top spot for some time.

In second place is Government, with this high ranking probably because technology failures at government bodies often impinge on the general public, meaning that the media gets to hear about them.

Financial Services has moved down to third place. While we believe that the industry is getting better at managing IT risk, the impact of individual incidents may be on the rise. We observed that, on average, about 4 million FS accounts (e.g., credit cards) are affected by an IT incident.

This point relates also to other sectors. For example, one very high-profile incident in the Retail sector generated hundreds of news articles, and affected around 40 million people. And yet in our study this counts as one incident. So while the total number of incidents in Retail is lower than for Government or Financial Services, the impact might well have been proportionately higher.

What is also interesting is that specific types of incidents are affecting some industries more than others. For example, Financial Services and Technology had a higher proportion of availability-related incidents than any other industry.

2.

Looking forward: top ten risks

We asked a number of industry specialists from KPMG's global network of member firms to tell us which of the top ten, in some shape or form, will be the biggest technology risk facing the Consumer Markets & Retail, Technology, Media & Telecom, Healthcare, Pharmaceuticals, Oil & Gas, and Transport and why. Over the following pages, they provide their answers.

Sectors at a glance

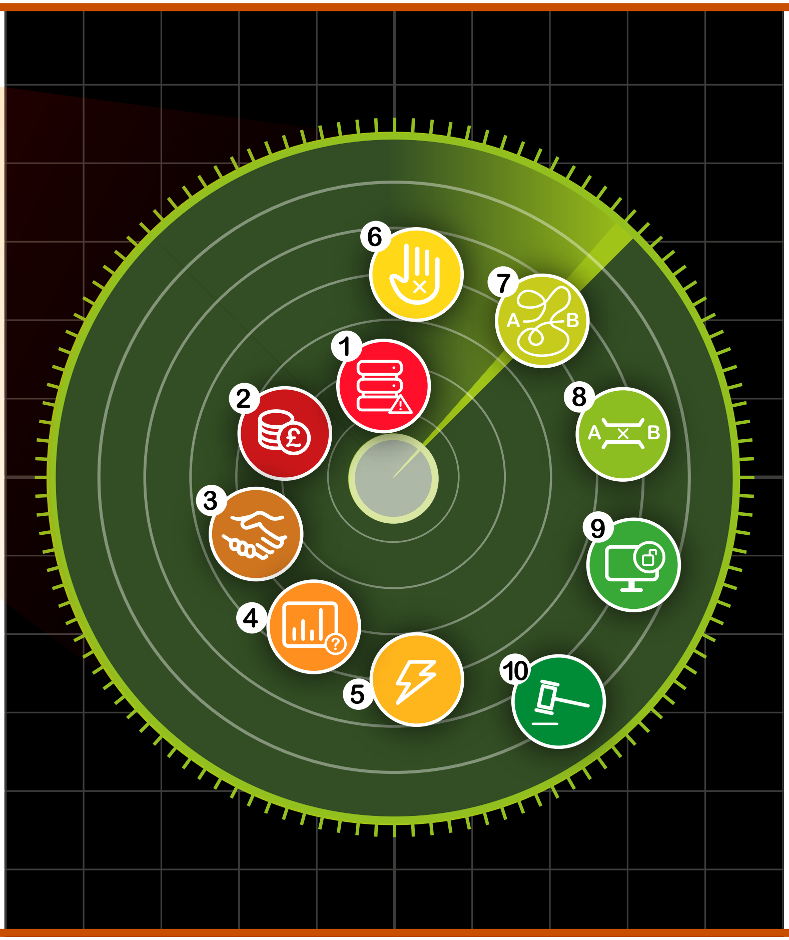
Top 10 risks identified for each sector

HIGH RISK	1	2	3	4	5	6	7	8	9	10	LOWEST RISK

Risk impact and probability in descending order PER SECTOR	Retail and consumer goods	Telecoms and Technology	Education	Central Government	Healthcare	Oil and Gas	Transport	Pharmaceuticals	**Overall avg score** (lower the score the more critical across industries)
Cyber-crime and unauthorised access	9	1	5	2	2	1	1	5	3.3
Inability to use and govern data for business needs/competitive advantage	4	9	3	3	3	2	3	2	3.6
Poor alignment of IT investments and projects with business needs	2	6	4	1	5	9	2	7	4.5
Regulatory pressures and non-compliance	6	2	2	6	1	10	8	1	4.45
Risk from IT complexity	7	5	6	5	6	3	5	4	5.1
Lack of resilience and disaster recovery capabilities	5	4	8	8	4	6	4	6	5.56
Inability to cope with rapidly changing technology	1	8	1	4	7	Not included in top 10 risks	9	10	5.7
Risk from suppliers (and the extended enterprise)	3	3	7	9	9	5	6	8	6.3
Ineffective governance risk and compliance	10	10	10	7	10	4	7	3	7.6
Ineffective deployment and leverage of emerging technologies	Not included in top 10 risks	Not included in top 10 risks	Not included in top 10 risks	Not included in top 10 risks	Not included in top 10 risks	8	Not included in top 10 risks	Not included in top 10 risks	8.0
Ineffective IT service management and delivery	8	7	9	Not included in top 10 risks	8	7	10	9	8.3
Ineffective IT project delivery	Not included in top 10 risks	Not included in top 10 risks	Not included in top 10 risks	10	Not included in top 10 risks	Not included in top 10 risks	Not included in top 10 risks	Not included in top 10 risks	10.0

Looking forward: top ten risks – Retail and consumer goods

HIGH RISK ① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ LOWEST RISK



1. Inability to cope with rapidly changing technology

2. Poor quality of IT investments/ projects

3. Risk from suppliers (and the extended enterprise)

4. Inability to use and govern data for business needs/ competitive advantage

5. Lack of resilience and disaster recovery capabilities

6. Regulatory pressures and non-compliance

7. Risk from IT complexity

8. Ineffective service delivery

9. Cyber crime and unauthorised access

10. Ineffective governance, risk and compliance

Looking forward: top ten risks – Retail and consumer goods (continued)

Andrew Shefford
KPMG in the UK

Today's tech-savvy consumer is no respecter of reputation. Changes in consumer behaviour, often driven by technological change, has meant that some of the biggest household brands have had to learn this the hard way in recent years, from catastrophic sales to outright closure. Our spending habits increasingly include a digital element, whether it be shopping online, using click and collect services, buying books and music as data rather than as media, or simply checking prices.

Maintaining business as usual in this 'omni-channel' environment requires continual investment in data systems, which many are currently not willing or able to make at the level required. However, if their systems are not up to the task, they could end up paying the ultimate price.

Established retailers have been grappling with digital for some time. As well as an opportunity, it presents risks that grow more sophisticated as shoppers use ever-smarter smartphones to check competitors' prices, in store, in real time. Despite this fundamental challenge to their business model, too few are responding quickly enough. Whether in store, on a mobile device or on a computer, consumers want a seamless, clear and integrated shopping experience. One of the best ways to deliver this is by investing in smarter data systems.

So why are more retailers and consumer goods producers not heeding the lesson?

Many of these businesses rely on aging operational and financial systems which are too costly to replace but too valuable to fail. Investing in new digital platforms and replacing enterprise software systems in any major business requires very strong planning and project execution and a huge investment.

IT departments may struggle to secure that kind of budget when there are competing priorities for investment; especially when the financial gain from this investment can be hard to quantify. They are also not used to thinking about data and their systems at the core of their structure and are likely to worry about lost productivity while they undergo the switch to a new system.

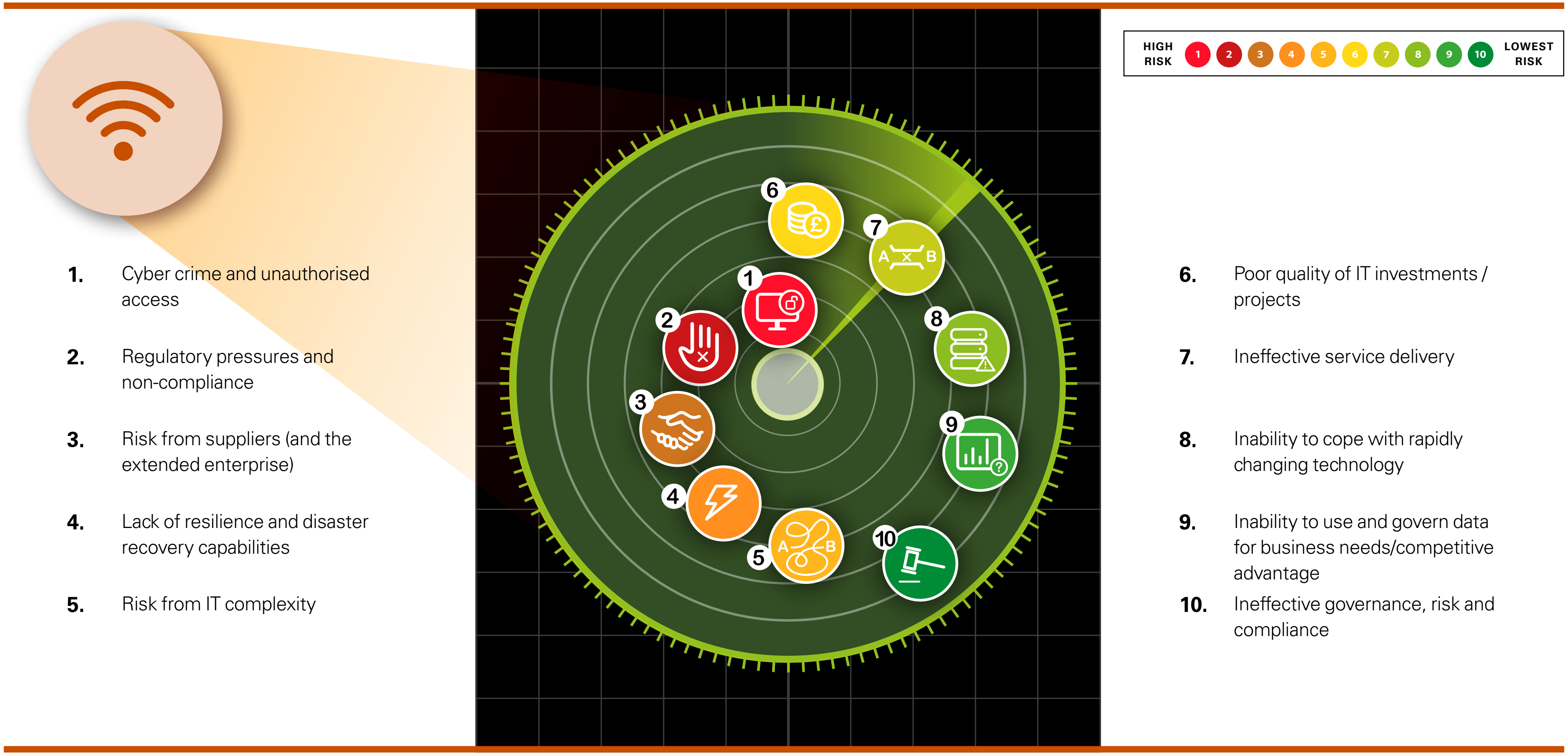
But not investing in data systems is not a viable option. Legacy systems will struggle to deal with the operational and reputational risks companies face today. I believe this is the most overlooked risk in the sector.

To put it into context, manufacturing processes in consumer organisations could be compromised if someone accidentally, or maliciously, changed the data used in the manufacturing process. Such an incident could lead to unquantifiable legal and reputational damage.

Similarly, imagine the cost to a supermarket whose online store crashed because of a technology outage caused by fragile data systems, when online represents a sizeable percentage of revenue. The effects would ripple across the business: from lost customer orders, to staff not being paid, to millions of pounds-worth of produce rotting in distribution centres.

Companies that do not prioritise data management and robust data systems will increasingly become vulnerable to both operational risk and competitors. Although such companies are unlikely to disappear overnight, I do believe they are on borrowed time. Customer service delivery will keep on evolving and I have little doubt that data will be instrumental in supporting what comes next. Without the right tools to keep up with customer demand, their consumers will drift elsewhere.

Looking forward: top ten risks – Telecoms and technology



1. Cyber crime and unauthorised access
2. Regulatory pressures and non-compliance
3. Risk from suppliers (and the extended enterprise)
4. Lack of resilience and disaster recovery capabilities
5. Risk from IT complexity
6. Poor quality of IT investments / projects
7. Ineffective service delivery
8. Inability to cope with rapidly changing technology
9. Inability to use and govern data for business needs/competitive advantage
10. Ineffective governance, risk and compliance

Looking forward: top ten risks – Telecoms and technology (continued)

Fayyaz Cheema
KPMG in the UK

Telecommunications firms have never been more central to our lives. Digital devices rules how we work and socialise; how we shop and relax. Telecommunications companies (telcos) are becoming less of a service provider and more of a utility service on which we all depend.

That is why I believe the telco industry will need to fundamentally shift from a model focused on speed-to-market and innovative technology to one that is focused on managing service delivery risk.

Don't get me wrong, innovation and speed-to-market will still be important, but dependable data, safe and secure transmissions and strong coverage and connectivity – either by 4G/5G or fast broadband – will supersede that as more and more of us get online. Sixty-eight percent of adults in the UK now use internet on the go[1] and more operators are moving into the sector as prices fall. We are already witnessing telcos consolidating in order to share infrastructure, such as O2 and the Three network[2] and this will undoubtedly continue as the customer demand for a one-stop shop or 'quad play' provider (i.e. mobile, broadband, landline and TV) increases[3].

The challenge for companies in meeting consumers' rising expectations of an integrated and seamless service, will be to improve their management of their expanding supply chains. Through the sharing of infrastructure or integrating IT, telcos companies may also become more susceptible to technology risks. They will therefore need to build trust around areas such as data security, privacy, cyber threats, fraud, data transfer performance and resilience with the suppliers that they partner.

They must also draw up strong disaster recovery and contingency plans. Indeed, customers are unlikely to care or know about the complex partner relationships that underpin the telco products and services they use. If something is not working, they are likely to complain or take action against the telco, regardless of who is at fault.

The regulator is likely to take a similar view as they take greater interest in ensuring consumers get good value for their money. Indeed, over the past five years we have seen more regulator activity in this space, such as Ofcom's revisions to the Metering and Billing Direction in 2014[4]. Additionally, in May, Business Secretary Sajid Javid warned O2 to "sort it out" on Twitter when customers were subjected to a network outage[5].

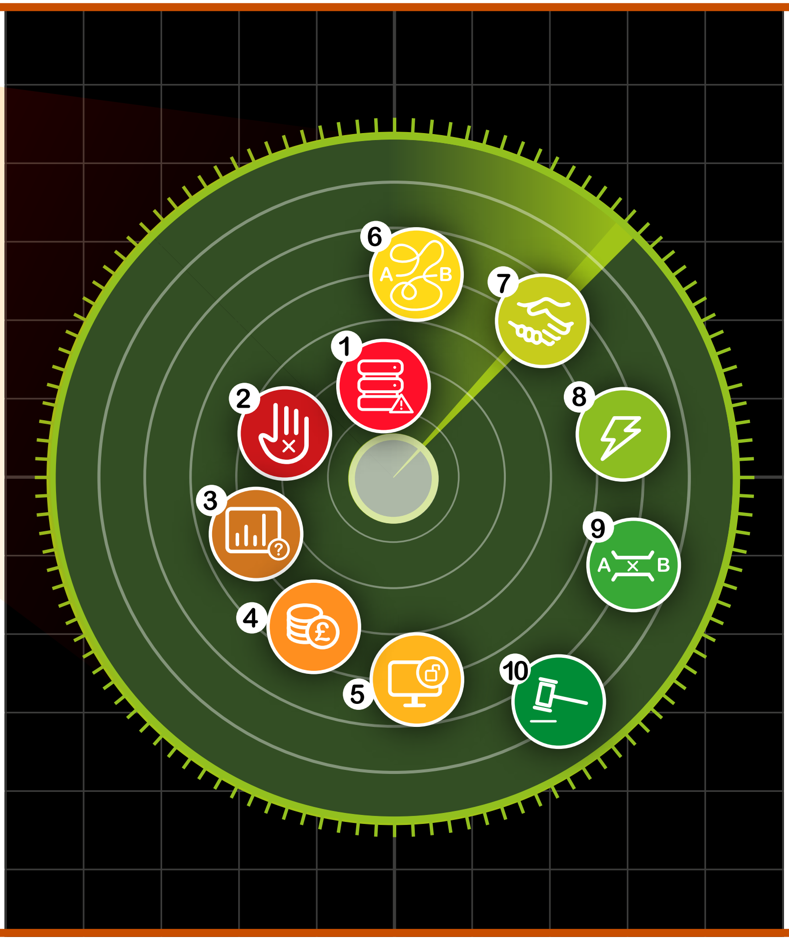
Despite the increased presence of the regulator, taking a prudent approach to governance, risk and compliance is still new to the telco sector, with a potential shift from being driven by their marketing and sales teams, to IT and technology departments. This will need to be re-assessed if companies want to put dependability at the heart of their offering.

The recognition that communication is now a virtual utility must first come from the board. It will be too late if the penny drops only after an operator suffers a major service disruption; the brand damage will already be done.

1. http://www.ons.gov.uk/ons/dcp171778_373584.pdf
2. http://www.mirror.co.uk/news/technology-science/technology/three-buying-o2-10-billion-5397438
3. http://www.managementtoday.co.uk/news/1346174/quad-play-pays-off-bt/
4. http://stakeholders.ofcom.org.uk/consultations/metering-billing-2014/summary
5. http://www.cityam.com/216424/sajid-javid-o2-sort-it-out

Looking forward: top ten risks – Education

HIGH RISK 1 2 3 4 5 6 7 8 9 10 LOWEST RISK



1. Inability to cope with rapidly changing technology
2. Regulatory pressures and non-compliance
3. Inability to use and govern data for business needs/competitive advantage
4. Poor quality of IT investments / projects
5. Cyber crime and unauthorised access
6. Risk from IT complexity
7. Risk from suppliers (and the extended enterprise)
8. Lack of resilience and disaster recovery capabilities
9. Ineffective service delivery
10. Ineffective governance, risk and compliance

Looking forward: top ten risks – Education (continued)

David Timms
KPMG in the UK

If UK universities and higher education institutions do not invest more in state-of-the-art technology, they are in danger of slipping down global rankings. For many years the UK has prided itself on its world class institutions, but as an increasing number of foreign universities develop new ways of studying through the latest technology, British institutions will find it harder to compete on their brands alone. We are living in an era in which education is almost universally regarded as a human right[1]. Yet UK students are paying up to £9,000 a year for their university education.

Advances in technology and the internet have created cheaper alternatives that offer a richer learning experience, from video and live web-conference courses at Harvard University's Extension School to classroom aids, such as iTunes U. Obviously, digitised learning will not appeal to all aspiring students.

As more technology providers and higher education institutions follow suit, I believe universities will increasingly need to show they are making the best use of technology if they are to attract and retain the best students.

Many were dubious when former California governor Arnold Schwarzenegger said eBooks were the future of classroom learning back in 2009[2], but today tablet computers can be found in 70 percent of primary and secondary school classrooms in the UK[3].

It would be naïve to think that as future generations of young people enter higher education, they will no longer have this expectation of technology learning resources.

The traditional university model of lectures, followed by individual reading and study, may become irrelevant as students demand greater bang for their buck. Many universities require their students to do work or research online before attending lectures, so time can be better spent on professor Q&As. We are also seeing professional training organisations devoting full-time staff into developing the technology tools to help students study.

However, despite numerous innovations in and outside the classroom, many universities are still failing to ensure that IT investment is spent in the right areas, such as e-learning.

Although universities must focus upon delivering a better, technology enabled, student experience, they are held back by a general lack of co-ordination on IT governance and spend. This is particularly common in older universities with separate colleges, departments and faculties, who often work independently.

But standardising IT processes across a whole institution is complex and costly. It requires a change in mind-set for the long-established institutions whose leaders might be less au fait with digitised learning. Enforcing a joined-up approach to IT across institutions could therefore lead to some tensions across departments.

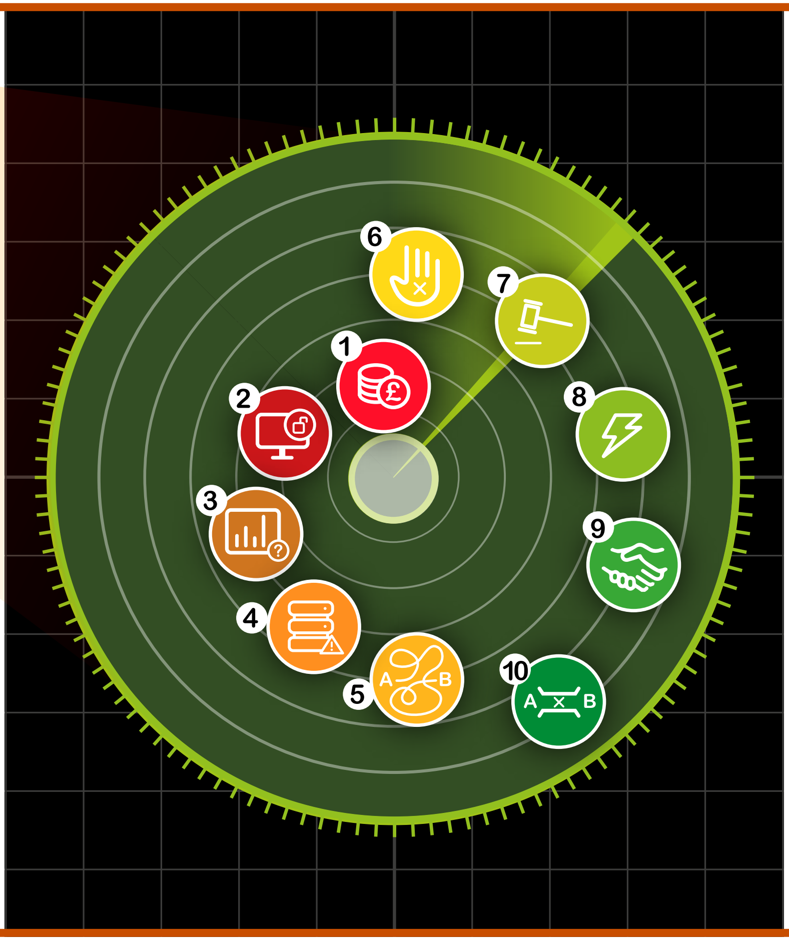
The long-term benefits of centralising IT will almost always outweigh these considerations however. From a risk perspective, it is a far safer and more cost-effective solution than dealing with IT issues as they arise.

And again, from a credibility perspective, it should be in an educational establishment's best interests to promote a safe and well-resourced environment for IT-based learning in order to remain competitive, both in the eyes of prospective students and of commercial partners.

On its own, the presence of strong IT is unlikely – at this point – to sway the brightest students from wanting to study at those institutions traditionally perceived to be the best. But as challengers invest more resources in IT learning who is to say technology will not be a game changer for higher education institutions?

[1] https://www.nesri.org/programs/what-is-the-human-right-to-education
[2] http://www.theguardian.com/education/2009/jun/09/ebooks-arnold-schwarzenegger
[3] http://www.bbc.co.uk/news/education-30216408

Looking forward: top ten risks – Central government



HIGH RISK	1	2	3	4	5	6	7	8	9	10	LOWEST RISK

1. Poor quality of IT investments / projects
2. Cyber crime and unauthorised access
3. Inability to use and govern data for business needs/competitive advantage
4. Inability to cope with rapidly changing technology
5. Risk from IT complexity
6. Regulatory pressures and non-compliance
7. Ineffective governance risk and compliance
8. Lack of resilience and disaster recovery capabilities
9. Risk from suppliers (and the extended enterprise)
10. Ineffective IT project delivery

Looking forward: top ten risks – Central government (continued)

Andy North
KPMG in the UK

The government holds more data on us than anyone else but they are struggling to use it to improve services. If this continues, the public will not only become increasingly frustrated with government, but ultimately society's progress will suffer.

Almost every day we hear of people falling through the cracks, from communication breakdowns between local authorities and care services, to border controls. More effective public sector data sharing can help curb these incidents.

So why isn't it happening? My answer to this is that no one in government seems to have a clear understanding of what data is held and who holds it. This is partly due to the siloed nature of the public sector's various organisations, but more crucially, because there is no overarching, senior government role to understand the information held and how it could be used.

The Information Commissioner's Office is arguably most able to take on this role, as they are directly responsible for shaping and enforcing data protection policies. Given that they hold a record of all the UK organisations' personal data, it seems a missed opportunity not to make full use of it.

In the private sector the rise of data and analytics has inevitably led to the creation of more senior management roles, such as chief information officer or chief digital officer.

By contrast, in the public sector the person chiefly tasked with data and information management tends to have other competing roles; typically the head of IT; whose time is mostly spent making sure technology systems work, rather than making sure teams are using data to its best advantage.

There is also a keen focus across the public sector on protecting the individual, by sharing data only under certain conditions and with robust safeguards. While this of course must be at the heart of policy making, it seems to me that these efforts go too far.

As a law-abiding citizen, I would be quite happy for my personal information to be shared more widely across public sector organisations on the proviso that it was purely being shared for the benefit of improving the services all citizens receive.

Despite the intuitive benefits of a more integrated public sector, I think that government would still need to invest in understanding and articulating clear cases where data sharing would be of benefit to win over the public.

I am sure all of us have experienced at least one inefficiency due to the public sector not harnessing the power of data. If you change your GP practice for example, you will still have to fill in paper forms, or wait days for your medical records to arrive. This is simply bewildering in an era of digital and data.

Better data sharing across the public sector has the potential to solve so much more than the time spent waiting for your medical records.

I imagine that few would contest surrendering their personal data if they knew it was being used to prevent further child abuse cases[1], or convicted murderers from other countries entering the UK[2].

There have been some successes. If we took the Police National Computer away from all UK forces tomorrow for example, it would have a severe impact on police success and speed in solving crime.

[1] http://www.theguardian.com/society/2014/nov/27/nao-children-care-highest-25-years-baby-p
[2] http://www.telegraph.co.uk/news/uknews/crime/11103663/Alice-Gross-Latvian-builder-suspect-is-a-convicted-murderer.html

Looking forward: top ten risks – Central government (continued)

Although these are compelling reasons, the government will require strong leadership to get people to recognise that this is something we can and should do.

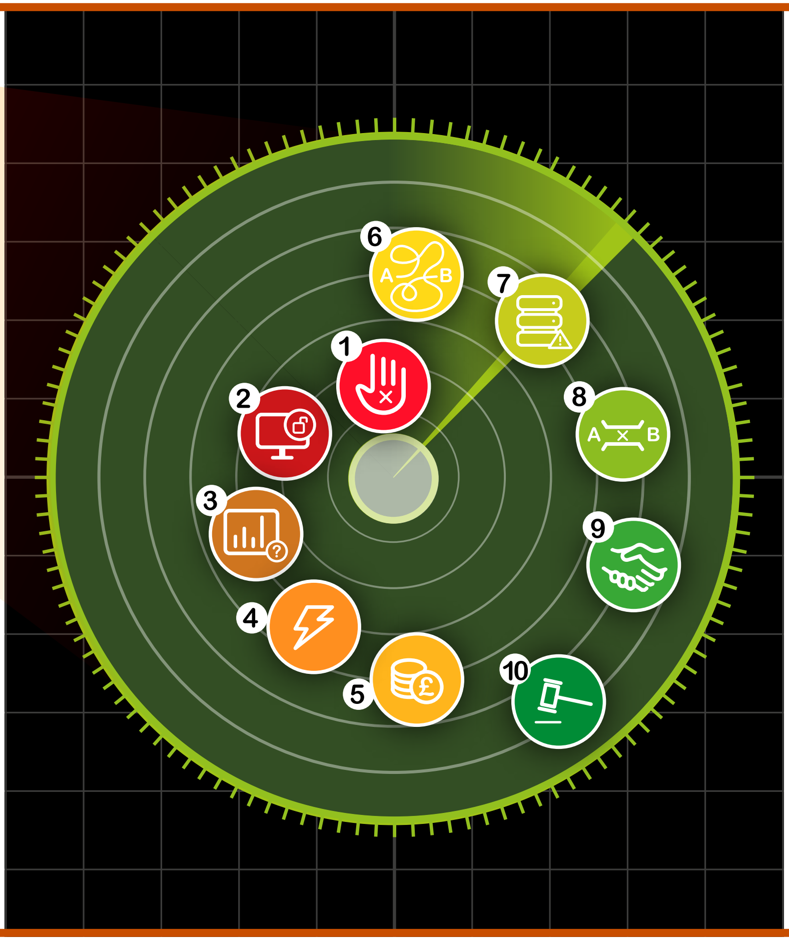
Just as Scotland voted on independence and Britain may soon have a referendum on leaving the European Union, citizens should be consulted on personal data sharing across the public sector. Arguably, reducing crime, improving the quality of services like healthcare and reducing their cost through the use of data has an even greater impact on day-to-day lives than other, political questions.

Successful implementation will require significant investment, but I am confident most UK tax payers would be pleased to support something they knew they were directly going to reap the benefits of, from faster GP clinic registration to less crime committed in their local area.

As the world makes further strides in data and analytics, both citizens and public sector employees are going to wonder why public sector services, of all things, are exempt from these innovations.

Looking forward: top ten risks – Healthcare

1. Regulatory pressures and non-compliance
2. Cyber crime and unauthorised access
3. Inability to use and govern data for business needs/competitive advantage
4. Lack of resilience and disaster recovery capabilities
5. Poor alignment of IT investments and projects with business needs



HIGH RISK 1 2 3 4 5 6 7 8 9 10 LOWEST RISK

6. Risk from IT complexity
7. Inability to cope with rapidly changing technology
8. Ineffective service delivery
9. Risk from suppliers (and the extended enterprise)
10. Ineffective governance, risk and compliance

Looking forward: top ten risks – Healthcare (continued)

Nicolina Demain
KPMG in the UK

Your medical data is worth 10 times more on the black market than your credit card information, Reuters reported last year[1]. With the proliferation of technology geared to health and wellbeing available to consumers, I can only see the commoditisation of health data increasing. Worryingly, I do not think the healthcare industry has fully recognised this fact.

The digital health market is booming[2]. But with this comes an exponential increase in the volume of health-related data and unfortunately, the potential for data loss and theft.

We often hear about health data being used for commercial gain in targeted advertising[3], sold on Ebay[4] and inappropriately shared with third parties[5]. I fear it will only be a matter of time before we hear about more data hacking incidents due to the increased use of these technologies, and more data breaches because healthcare staff don't realise the danger of what they might be doing.

The government-sponsored Trustworthy Software Initiative has warned that the rapidly expanding market demand for healthcare apps and wearable technology is tempting companies to prioritise new devices and features, rather than security and reliability. It added that this could have fatal repercussions for the end-user[6].

Despite such concerns, data security and prevention is still not high enough on the industry's agenda in my view. This is partly due to naivety as to why anyone would want to hack someone else's personal health data. I believe this view is especially prevalent in the NHS, which has been slow to embrace digital working cultures and technologies, compared to other sectors.

As the NHS inevitably undergoes structural change, including more mergers and integrations of trusts and moves towards a goal of being a paperless organisation by 2018, its staff will have access to far more data. That means they will need to learn how to protect that data.

NHS organisations already have to offer their staff training in information governance and security. However, the effectiveness of these programmes is hard to determine. Sometimes organisations and individuals are oblivious to the fact they have come under a cyber attack at all, since the effects can be missed or masked.

Teaching healthcare staff about data security will inevitably seem less urgent than life-saving clinical training. But organisations still have a responsibility to teach their staff about cyber security and how to minimise the risks of data breaches.

Changes in public health legislation could actually be compounding the risk of data breaches. Some organisations have complained that regulations introduced under the 2012 Health and Social Care Act are overly complex. This has created uncertainty around how and when staff can legally share data.

1. http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
2. http://www.forbes.com/sites/zinamoukheiber/2015/05/07/how-health-care-technology-is-minting-a-new-class-of-billionaires/
3. http://www.ft.com/cms/s/0/d510afec-2ecd-11e4-a054-00144feabdc0.html#axzz3WAVaEigU
4. http://www.dailymail.co.uk/news/article-2559876/2-000-NHS-patients-records-lost-day-two-million-data-breaches-logged-start-2011.html
5. http://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/11/EMBARGO-0001-FRIDAY-14-NOVEMBER-BBW-NHS-Data-Breaches-Report.pdf
6. http://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/11/EMBARGO-0001-FRIDAY-14-NOVEMBER-BBW-NHS-Data-Breaches-Report.pdf

Looking forward: top ten risks – Healthcare (continued)

Meanwhile, a successful hack in the private sector could give access to even greater stores of personal information, such as insurance and payment details. This has made the US healthcare industry a prime target for cyber attacks[7].

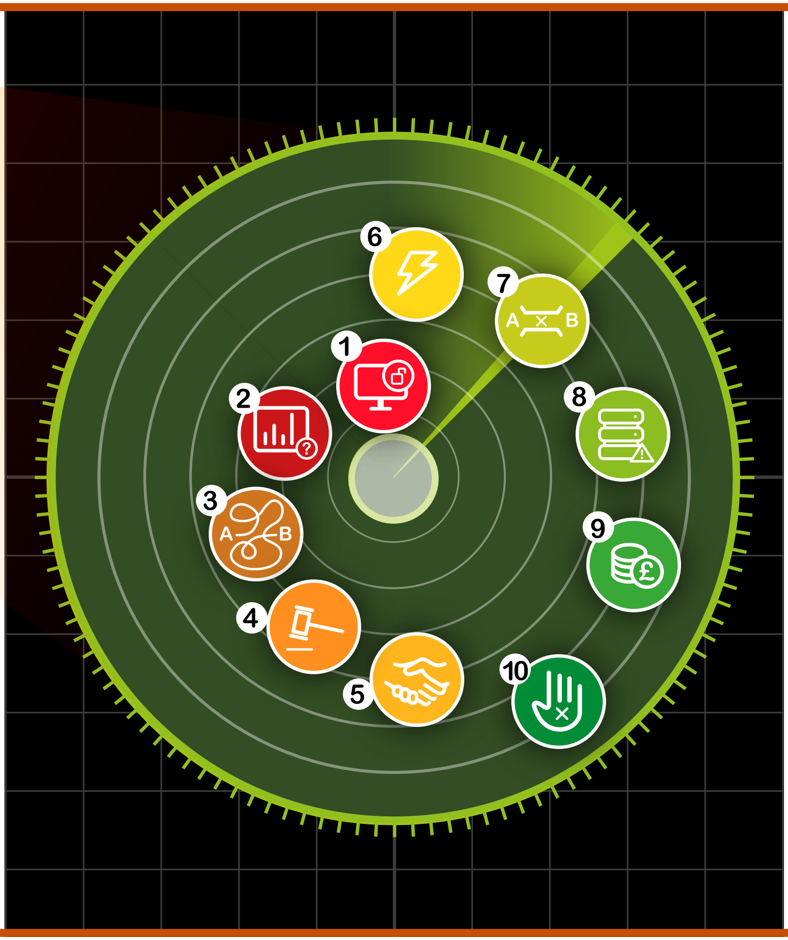
It is clear that health technology, for work and personal use, is here to stay. But with its adoption should come proper management of people's data and clear data standards outlined by the Information Commissioner's Office. While we are seeing more investment in cyber security from the industry and especially the NHS[8], organisations must take responsibility for ensuring their technology is safe to use. If not, they risk jeopardising the integrity of the technology and their organisation, not to mention putting individuals in danger.

> ***As we see this issue moving up organisations' risk radar, Boards should be asking themselves what assurances they have in place to proactively manage and respond to cyber security risks.***

[7] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[8] http://www.information-age.com/technology/security/123458987/beacons-good-cyber-security-celebrating-nhs-digitisation

Looking forward: top ten risks – Oil & Gas



HIGH RISK	1	2	3	4	5	6	7	8	9	10	LOWEST RISK

1. Cyber-crime and unauthorised access
2. Inability to use and govern data for business needs/competitive advantage
3. Risk from IT complexity
4. Ineffective governance, risk and compliance
5. Risk from suppliers (and the extended enterprise)
6. Lack of resilience and disaster recovery capabilities
7. Ineffective IT service management and delivery
8. Ineffective deployment and leverage of emerging technologies
9. Poor alignment of IT investments and projects with business needs
10. Regulatory pressures and non-compliance

Looking forward: top ten risks – Oil & Gas (continued)

Joshua Galvan
KPMG in the US

In an industry where spending billions drilling a hole in the ground is common, oil companies have become increasingly skilled at leveraging the best in science, engineering and computing technology to calculate and manage risk in hydrocarbon exploration projects.

Such is the power of related tools that oil companies could monitor what is happening five miles below the seafloor right from one's (mobile) office in Houston. But now the proliferation of many new technologies and ever-expanding data volumes has unwittingly created a complex patchwork that increases the odds of a major IT incident, from 'mere' data loss or software issues, right through to corruption, theft or the sabotage of billion dollar assignments.

Nobody could contest the value these 'apps' (of both the modern, 'mobile' variety and more traditional computer system sense) bring to oil companies. However, in simultaneously deploying and operating so many highly-intelligent solutions – fully spanning the distance between the drill-bit and the desktop – enterprise-wide IT risk management (ITRM) is becoming all the more challenging and costly.

A key contributor to this problem is that individual technologies are often developed in isolation, internally or perhaps by an external provider or through a multi-partner venture, and are therefore unlikely built to a standard or consistent architecture within the broader company IT context. These apps, which can be leveraged from a whole host of diverse computing environments (such as the Cloud, tablet, mobile or a collaboration network) can together create an enormous mix of complex and not well-understood IT componentry akin to a large patchwork quilt.

The fact that oil company operations tend to evolve in the image of their global distributed operating models exacerbates this. Operating segments, business units or individual assets often have authority over their own budgets and spend for buying or building apps. This can lead to deviation from company standards, inadvertently creating blind spots in the IT fabric and causing security, continuity, integrity and regulatory risk profiles to go unnoticed.

While these agile and high-value analytical technologies have become an essential part of day-to-day business, they must be developed in a way that enables consistency of risk-control, while still scaling to shifts in company performance.

Oil prices have hovered around multi-year lows. While this continues, we will increasingly see the industry challenged to spend less and still achieve appropriate levels of ITRM, governance and assurance.

Given the focus on commodity price and geopolitical news headlines, I fear technology risk slips down the list of priorities for immediate action.

Ironically, investment in technology will make companies' priorities lists, as the pressure to find new, competitive advantages in a down market never ceases. Yet a basic risk oversight, such as a miscalculation in drill positioning by a few feet or a failure to renew a software licence could have major repercussions on an oil company's human safety and environmental impact, regulatory situation, and balance sheet.

Looking forward: top ten risks – Oil & Gas (continued)

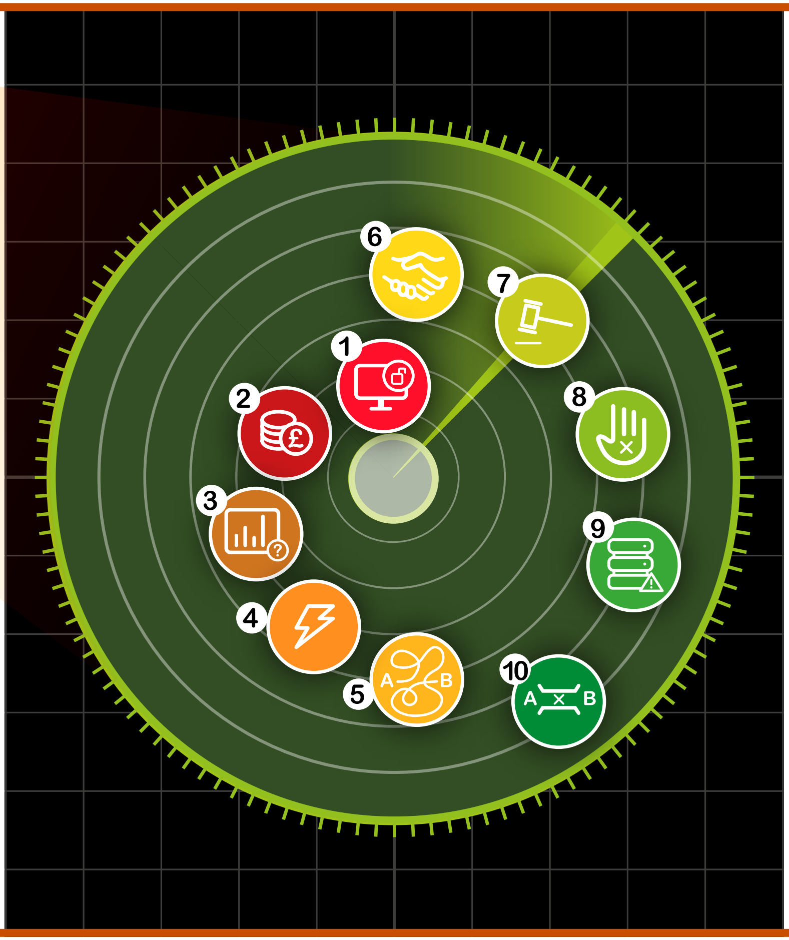
Equally, as oil prices recover, companies that are still not investing in ITRM capabilities will struggle to stay apace of business demands for app development and innovation to drive future growth spurts.

There is no equation or foolproof figure for investment in ITRM capabilities, but in a business model fuelled by apps and an environment where state and corporate espionage and attacks on the industry are on the up[1], oil companies cannot afford to be indifferent.

> ***I think that organisations are aware of the underlying need – but there is a reluctance to act. I imagine it will take one or two trailblazers to demonstrate how this can be addressed in a transformative way before the rest will follow. Once the prevailing mindset is shifted away from viewing ITRM simply as a costly and time-consuming series of compliance checks, then the opportunity to improve business prospects and results through a risk-balanced approach will present itself across the sector.***

[1] http://money.cnn.com/2015/02/17/technology/security/malware-nsa/

Looking forward: top ten risks – Transport



1. Cyber crime and unauthorised access

2. Poor alignment of IT investments and projects with business needs

3. Inability to use and govern data for business needs/competitive advantage

4. Lack of resilience and disaster recovery capabilities

5. Risk from IT complexity

6. Risk from suppliers (and the extended enterprise)

7. Ineffective governance, risk and compliance

8. Regulatory pressures and non-compliance

9. Inability to cope with rapidly changing technology

10. Ineffective service delivery

HIGH RISK 1 2 3 4 5 6 7 8 9 10 LOWEST RISK

Looking forward: top ten risks – Transport (continued)

Ben Foulser
KPMG in the UK

Transport of people and goods is a critical enabler of the economy; however concerns and inconsistencies in data sharing practices and protocols will prevent a truly integrated transport environment from being realised. This has also stopped a much-needed degree of personalisation to customer travel to ensure a more productive and sustainable transport environment. With personalisation and a better understanding of the customer comes a real opportunity for commercial gain; but careful consideration should be given to how best to exploit these commercial opportunities.

Lack of coordination of data standards in the transport sector up to now has resulted in different organisations doing similar things with their data but in quite different ways. In doing so, they are missing an opportunity to develop solutions that aggregate information across the transport and wider sectors to deliver an enhanced customer experience, generate ancillary revenue opportunities and deliver cost, capacity and carbon optimisation in operational activities.

For instance, developing innovative products that incentivise customers to use different routes and/or services can help to optimise capacity in our heavily constrained systems. Other examples include engaging with customers throughout their journey (from the decision to travel through to arriving at the destination), or to enter into partnerships with organisations outside of the sector to deliver integrated and value-adding services to customers. Ultimately we should be seeking to provide seamless journeys to emotionally-engaged customers whilst leveraging revenue opportunities and minimising costs.

Consumers increasingly expect access to real-time information, decision support tools and personalised, value-adding products, such as personalised fares that span multiple modes of transport.

As time goes on, I believe that the risk of failing to deliver an end-to-end, integrated customer experience will be an inability to leverage revenue growth opportunities but, equally if not more importantly, a failure to recognise or deliver optimisation opportunities that can deliver real cost and environmental benefits.

Of course, it is easier for some passengers than others to switch their mode of transport. But with cars still dominating the commute to work[1], public transportation providers could do more to encourage these groups onto buses, trains and trams.

Passengers should be able to have access to real-time information in respect of their end-to-end journeys, not simply provider by provider, mode by mode. They should also be given the tools and data that will enable them to make educated and appropriate decisions regarding their travel options.

Simultaneously, transport providers should use the understanding of end-to-end passenger journeys and real-time asset condition data to dynamically manage their networks, making maximum use of capacity whilst minimising the inconvenience or impact on the paying customer.

However, for transport providers to be successful in realising such opportunities, they will have to overcome several data related challenges, such as:

- customers trusting that their data will be used in the most appropriate fashion and not misused;
- ensuring data integrity (especially where that data is safety critical, for example, in asset registers); and
- development of a capability to collect, collate and analyse date in real-time to enable decision support.

[1] http://www.bbc.co.uk/news/election-2015-32245068

Looking forward: top ten risks – Transport (continued)

We are already seeing individual providers making innovative use of analytics. Transport for London were recently able to identify a group of passengers stuck in a lift using data from their Oyster pre-payment cards in order to pay them compensation before the passengers even needed to make a claim[2]. Similarly, from next year, registered users of the c2c rail franchise will be eligible for automatic refunds from delayed journeys[3].

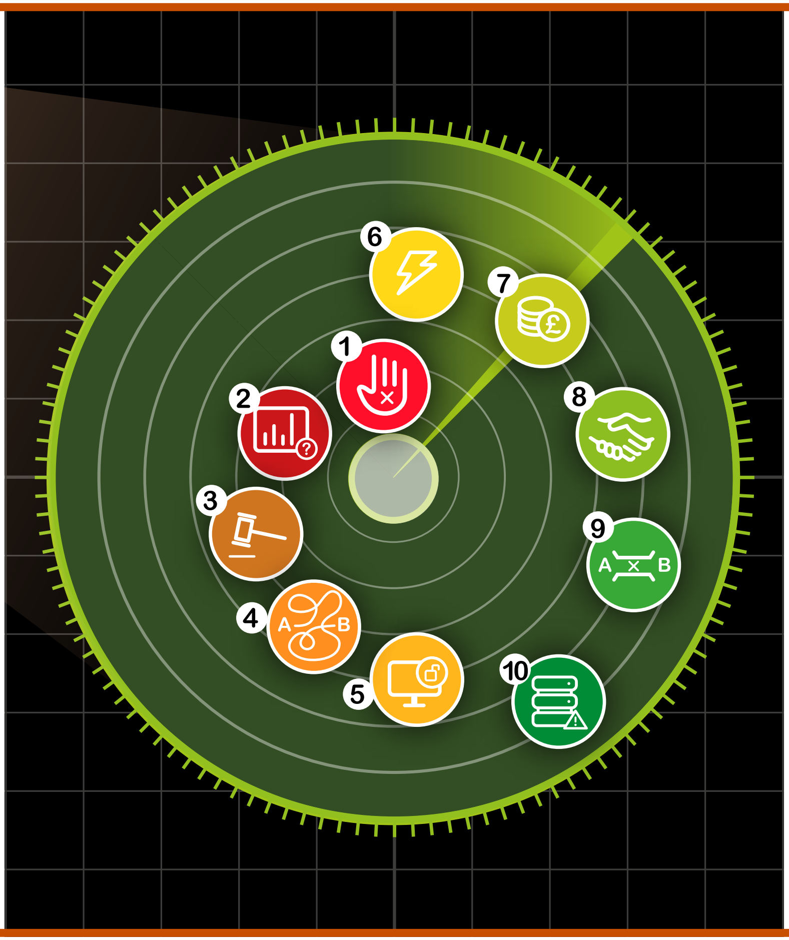
We are also seeing the use of analytics and profiling to leverage and maximise partnership opportunities. For instance, the Piccadilly Circus branch of Crosstown Doughnuts advertises deals on their coffee and doughnuts on underground advertising media when they have low demand, but the transport network is in high-demand. This results in higher sales for Crosstown Doughnuts and revenue opportunities for Transport for London, in terms of advertising revenue and higher rateable value for the commercial floor space in the station.

Companies will have to strike a balance between using their data to enhance customer experience and not veering into commercial exploitation. In 2010, Hong Kong's underground train operator MTR, came under scrutiny for selling customer data for millions of dollars through its electronic payment ticketing system[4].

Ultimately we could – and should – end up with a fully integrated and largely-automated or autonomous transport network, which can leverage unique customer knowledge and the power of predictive, prescriptive and adaptive analytics. The importance of an integrated network is that it does not simply include one mode but is truly multi-modal, covering rail, bus, tram, cycle hire, highways, waterways and even pedestrian to deliver economically and environmentally sustainable solutions.

[2] http://www.standard.co.uk/news/transport/tube-passengers-trapped-in-stifling-lift-with-alarm-sounding-for-over-an-hour-9232100.html
[3] http://www.telegraph.co.uk/news/uknews/road-and-rail-transport/10930813/Automatic-refunds-for-delayed-commuters.html
[4] http://www.bloomberg.com/news/articles/2010-07-26/octopus-sold-personal-client-data-in-hong-kong-for-5-6-million-rthk-says

Looking forward: top ten risks – Pharmaceuticals



HIGH RISK ● 1 ● 2 ● 3 ● 4 ● 5 ● 6 ● 7 ● 8 ● 9 ● 10 LOWEST RISK

1. Regulatory pressures and non-compliance
2. Inability to use and govern data for business needs/competitive advantage
3. Ineffective governance, risk and compliance
4. Risk from IT complexity
5. Cyber crime and unauthorised access
6. Lack of resilience and disaster recovery capabilities
7. Poor alignment of IT investments and projects with business needs
8. Risk from suppliers (and the extended enterprise)
9. Ineffective IT service management and delivery
10. Inability to cope with rapidly changing technology

Looking forward: top ten risks – Pharmaceuticals (continued)

Jamie Thompson
KPMG in the UK

Pharma's can no longer solely rely on blockbuster drugs as demand for niche and tailored compounds increases. This will only be possible if companies become more savvy about using patient data. While this innovation has huge potential, the industry needs to be careful about how it uses, protects and makes decisions on this information to avoid putting patients at risk. Projects such as the 100,000 Genomes Project will enable greater breakthroughs in the use of patient genetics to provide treatment.

When this is combined with the ability to monitor patient health and activity through devices such as Fitbits, the industry will be able to dynamically monitor a patient's lifestyle as well as their health.

There are clear benefits to offer the use of customised drugs such as the provision of treatment specific to the individual and it is clear that patient demand for these complex drugs will only grow. It is important, however, that patients also recognise the drawbacks, such as the need for increased tests before such drugs can be taken. The greater knowledge about diseases affecting patients will help to create improved drugs that will reduce the side effects and improve response.

To do this, a new breed of pharmaceutical companies are working with healthcare practitioners, research bodies and other pharma companies to collect data from a much larger network and in real time. The large, global pharmaceuticals companies will have no choice but to follow these innovators as data-customised drugs become a competitive differentiator in the market.

With the benefits of this new data-driven approach comes an increased need for vigilance. While leveraging this data undoubtedly has huge positive potential, ensuring its integrity is critical. There are also some key data integrity and accuracy challenges that need to be considered as they threaten to tarnish the success of customised drugs. All of this will impact a company's R&D process and how they market a product.

As you would expect, customised drugs require data sets that are far more accurate and specific. That means that the data sets must be tested far more rigorously. Pharma companies would be naïve to assume all third parties with whom and from whom they share and take data have a sophisticated level of technology and security standards.

I have seen huge variation across the industry in this regard and this inconsistency makes producers vulnerable to incorrect decision making on R&D as well as data privacy regulations being breached, IP being stolen and lack of underlying technology to accurately churn vast amounts of data across complex scenarios.

The threats are very real. We are seeing a rising number of cases where companies, including some in life sciences, are becoming victims of data theft and leaks by disgruntled employees.

A successful hack or loss of data could not only do huge reputational damage, but also shut down drug production and even cause fatalities. Attacks could also be carried out directly on patients through hacking Bluetooth enabled devices such as infusion pumps or pacemakers.

Companies and their partners therefore need a strong, unified approach on data clearance and technology security to navigate this risk-filled landscape.

Increased legislation can be overwhelming, such as data privacy and FDA policies on personalised medicine, and is another reason for companies to invest in robust data processes.

Looking forward: top ten risks – Pharmaceuticals (continued)

They face potential fines if they fail to comply but this legislation also presents a meaningful opportunity for them to improve patient care.

The likely change in regulatory standards, combined with the continued growth of data means that companies should consider making an effort now to allow them to adapt with greater ease to future regulatory standards and avoid being overwhelmed by the future growth of data.

Every day pharma companies are using data to open new possibilities in patient care. The industry must protect the integrity of that data by agreeing secure ways to use and share it or risk squandering its potential.

1. http://www.theguardian.com/society/2014/nov/27/nao-children-care-highest-25-years-baby-p
2. http://www.telegraph.co.uk/news/uknews/crime/11103663/Alice-Gross-Latvian-builder-suspect-is-a-convicted-murderer.html

3.

Responding to technology risks

We asked technology risk specialists from KPMG's global network of member firms to tell us what organisations should be doing to address some of these risks. Over the following pages, they provide their answers.

Responding to technology risks – Building a risk management capability

Jon Dowie
KPMG in the UK

Kiran Nagaraj
KPMG in the US

Phil Lageschulte
KPMG in the US

Vivek Mehta
KPMG in the US

With growing pressure from business partners, customers and regulators, IT risk management has emerged as a strategic business imperative for IT and risk leaders. Despite this, many IT risk functions continue to be under-staffed and rely too often on backward-looking processes and tick-box exercises.

How can organisations move from this less-than-optimal situation to build a technology risk capability that is fit for purpose in the evolving risk landscape?

The first step is to strategise – to understand the starting point and the desired level of maturity. Many organisations who do IT risk well have been on this journey for many years. They follow a risk maturity curve, so over time their risk management flows from fire-fighting and reactive capabilities to being proactive, identifying risks before they hit, and using risk management to add value.

Business context is vital – without it, there will be little business value. After listing the technology risks that affect an IT entity (e.g., service, application, process, supplier), focus on the impact of each risk on the business. Then apply risk management practices.

Ensure the buy-in of all parts of the organisation. Build a common risk language for use across all areas. Clearly define the set of services that the IT risk function provides and establish unambiguous lines of interaction with that function. Each department should view IT risk as a partner function and so the relationship should be treated the same way as that with any other partner.

All technology issues are underpinned by people, and risk management is no different. Staff the organisation with the right people with the right skills, according to both your business and your technology needs. Keep investing in them to maintain staff as a key strength.

Execute your risk processes across the whole risk lifecycle – identify, manage, monitor, and mitigate. Some areas, such as cyber security and resilience, require more discipline so develop capabilities to perform deep-dives in these areas.

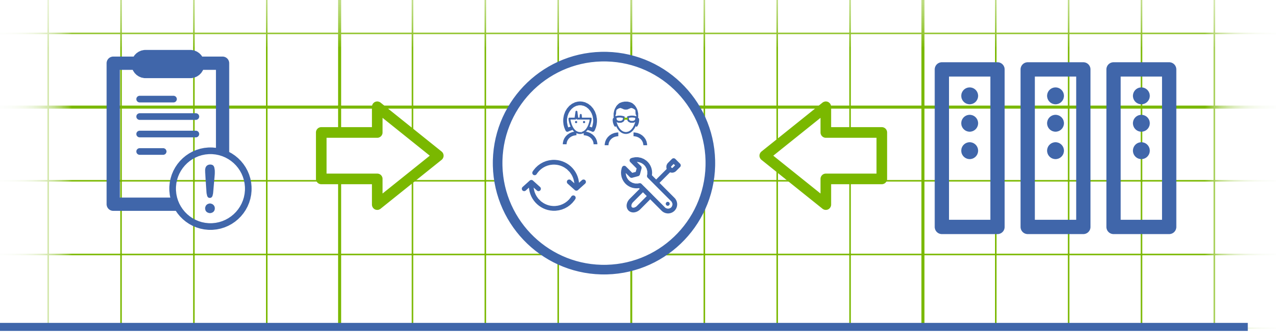
Over the years we have seen certain leading practices emerge in organisations that have created an effective function to respond to technology risks. One of the most fundamental of these is risk identification and measurement. Many organisations which do this well have built the infrastructure to aggregate risk information from different internal and external sources. They apply a combination of proactive and reactive techniques using top-down and bottom-up approaches to identify and measure risks. At the same time, they do not get lost in risk quantification, understanding that this cannot be done precisely – instead they focus on aggregating risk information and bringing the information to the right people.

Responding to technology risks – Building a risk management capability (cont'd)

They also integrate risk management fully into their existing IT governance bodies. Most organisations have IT governance bodies which serve as the decision making bodies for IT. IT risk should have a seat at this table. IT risk lives in the middle of IT and risk and so should have reporting lines to both. They utilise capabilities on either side whether it is extending current risk processes to IT, for example, or employing existing IT metrics to understand risk.

The core components of IT risk management are not new, but their effectiveness requires "risk" to be fully integrated with every IT attribute – strategy, architecture, development, operations, suppliers and data among others – seen in today's organisations. Holistic thinking about risk management needs to start from the top and be fully in tune with the organisation's technology requirements. The role and the scope of the IT risk function should ultimately be driven by business objectives so it can function as the Chief Information Officer's (CIO) "critical friend".

At the same time, they do not get lost in risk quantification, understanding that this cannot be done precisely – instead they focus on aggregating risk information and bringing the information to the right people.



Responding to technology risks – Building a risk management capability (cont'd)

Leveraging these technologies enables companies to become more flexible and better equipped to respond faster in the face of an incident affecting critical technological infrastructure which vital business functions depend upon.

Cloud-based recovery services are on many organisations' radar as they offer a way to achieve advanced data recovery services at a more affordable, subscription-based price. There are concerns over security of the cloud but over time it will be a key component of every disaster recovery programme.

These and other developments in technology have brought about a significant change in how organisations think about protecting themselves in the face of business interruption with a move from recovery to resilience ensuring a robust organisation that can withstand and continue business with confidence.

The biggest challenge to achieving technology resilience is still cash. Technology costs serious money. Those in charge of the technology resilience need to be able to articulate clearly why their project is important and why spending resources will be effective, putting the idea of technology resilience into a business rather than a technology context. A BIA offers the means to build such a business case, as it represents a cost / benefit analysis to make data driven decisions around acceptable risk and technology recovery investment. Building a good business case for technology resilience can save money – and perhaps even save the business.

> ***Those in charge of technology resilience need to be able to articulate clearly why their project is important and why spending resources will be effective, putting the idea of technology resilience into a business rather than a technology context.***

Responding to technology risks – Cyber security

George Quigley
KPMG in the UK

Ronald Plesco
KPMG in the US

Cyber security – it's the headline-grabbing and nightmare-inducing fear of every organisation. But we believe organisations need to avoid the hype that surrounds breathless media reports of high-profile hacking or data theft events, and focus on the real threats and effective methods of militating against them.

There is no denying that cyber crime is on the rise as our economies and lives become more digital. The threat landscape varies depending on the business or activity involved but can be a mix of fraud, espionage, political activism, or even individuals with a grudge.

So how can companies protect themselves? The bad news is that there is no foolproof protection against cyber attack. But organisations can make it a lot harder for attackers and block many of the less determined and sophisticated criminals.

Often this comes down to getting the cyber essentials right – a commitment from the top, action to raise awareness of the issue and basic protection measures around your core networks.

Then organisations need to go one stage further – be clear about what the heart of your business is and what needs additional protection. This might be intellectual property, financial or personal information, or continuity of operations. An analogy for what happens next is physical security in a hotel. Intruders may get into the lobby but you don't want them to get into the safe. So organisations need to put their most important valuables in the virtual backroom and ratchet up security accordingly.

An important dimension to cyber attacks that often gets ignored is people. Too often cyber crime is seen as a purely technical issue with a language all of its own. The reality is that many attacks come down to individuals – sometimes well meaning – who become the weakest link in the organisation's defences. Every business, every public sector body, every third sector association, should educate employees about security risks, how to spot possible viruses or hacking attacks, or unusual behaviour among colleagues that point to a cyber attack from within.

While protection is a vital first step, it isn't enough. But if safeguards fail, all is not lost. The smart response is to limit the damage an attack can cause as it happens. Having a fast incident response process and competent incident response team helps, but so does deft handling of media interest, addressing regulatory concerns and working to restore customer confidence, all as quickly as possible. Time after time, it isn't the incident itself which damages brand and reputation long term – it's the way firms handle themselves when it happens. So organisations need to think through what could happen before it does happen, be ready to exercise and test how to really respond in the heat of the moment, and make sure that decision makers understand their role in a crisis.

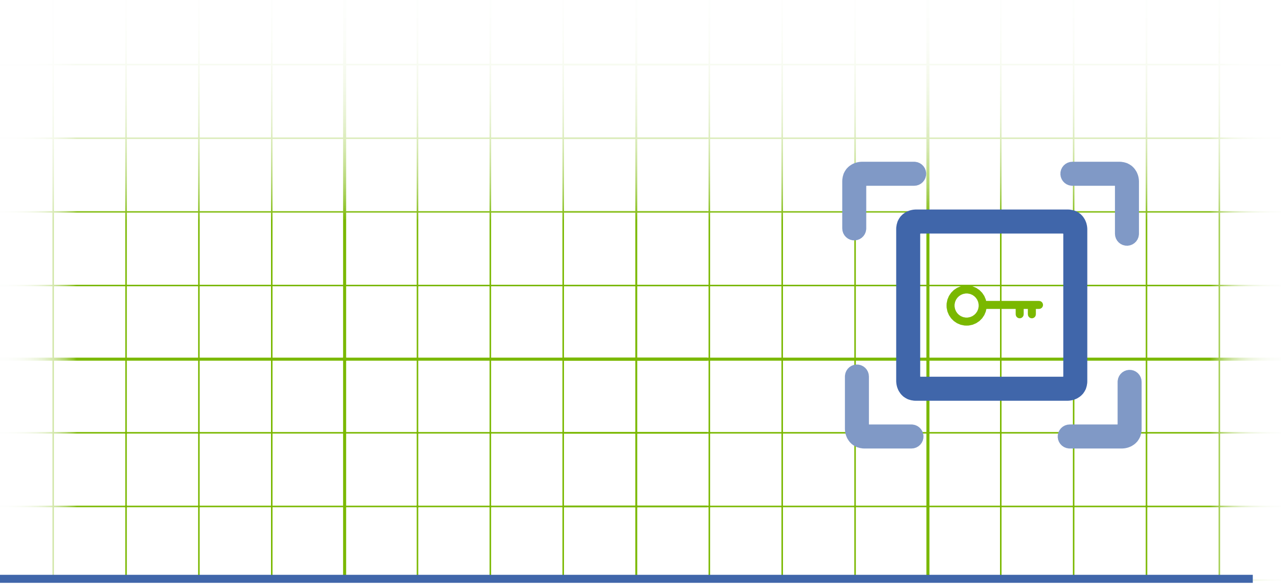
Responding to technology risks – Cyber security (continued)

Importantly, this will help avoid knee-jerk reactions such as unplugging computer systems too quickly before it is clear what data has been stolen or damaged. That evidence may be needed in any subsequent investigation or even as a defence against future lawsuits from disgruntled customers whose personal information was stolen.

Most large companies have a budget for IT security, which is about between six and fourteen per cent of the total IT budget. That budget has grown over recent years but perhaps simple percentages mask the need to think about your exposure to cyber attack and strike the right balance between digital opportunity and cyber risk.

Cyber security needs to be core to every organisation's discussions on new digital opportunities. Done right, cyber security can be an enabler, not a blocker, giving every business confidence to exploit opportunities by understanding risks and how to respond if the worst happens

Often this comes down to getting the cyber essentials right – a commitment from the top, action to raise awareness of the issue, and basic protection measures around your core networks.



Responding to technology risks – Building resilience

Greg Bell
KPMG in the US

Martin Lunt
KPMG in the UK

Curtis Baron
KPMG in the UK

Technology resilience is not just about technology. Its purpose is to enable a business to keep running, delivering its core products, services and activities, in the event of a technology-related disruption.

As technology drives and supports so much of our client's businesses today it is more important than ever that organisations ensure their most critical systems and data remain resilient to disruptive events.

A good place to start is to define which services are most critical to customers and to identify all the upstream and downstream IT systems upon which these services depend. Maintaining robust IT systems also requires strong governance, effective prevention and monitoring controls and clear accountability for the associated business risk of failure. By identifying business risks, both current and emerging, and evaluating the impact of business process disruption, an organisation can prioritise its resilience risk appetite.

The demand for 24/7 service availability has dramatically increased over recent years as consumer habits and business models change. More companies are implementing systems which are resilient by design, moving away from the conventional method of IT system failover. Thanks to advances in system design, monitoring and management, automated switchover between live-live data centres now helps high availability organisations reduce or eliminate downtime following a node failure. Much attention is now turning towards the data itself and how best to appropriately protect it.

Whether organisations rely on manual system recovery or advanced automated failover mechanisms, it remains important to analyse and test this capability. A Business Impact Analysis (BIA) can help organisations identify critical business processes and their dependencies across the business. The BIA should also define the availability requirements based on both the financial and non-financial impacts of possible business disruptions.

The IT function in turn should map the business processes to key systems and validate current recovery capabilities, identifying gaps against the business requirements determined through the BIA. Whilst this is typically completed at an operational level, it should start with a top down approach, ensuring priorities are strategically aligned to protect the organisation's reputation, market share and market value. This requires a co-ordinated response across business lines and support functions.

An effective business resilience strategy must also account for third-party risk exposure, including those providing critical business and IT services. The adequacy and effectiveness of third party resilience strategies must be properly evaluated and assured to pro-actively align expectations and requirements.

Technology development has enabled us to shift away from simply backing up data to physical tape towards real-time data replication and the virtualisation of storage, servers and applications. Whilst our ability to respond to failure and re-deploy critical services has evolved considerably we must always bear in mind that so too has the threat landscape and the expectations of the increasingly demanding customers.

Responding to technology risks – Technology enabled risk management

Andrew Shefford
KPMG in the UK

Paul Holland
KPMG in the UK

Hesham Karim
KPMG in the UK

There is no doubt that today's market place is consumer driven and high velocity, multiplying choice and reducing tolerance for errors or delays. The consumer perspective is clear - 'I want the best quality for the lowest possible price'. Technology is an obvious enabler for many organisations to drive innovation and improve business decision making - ultimately to realise growth or savings. Technology has also changed the risk landscape. The need to manage technology risk is confirmed from the number of adverse events we see in the market today, but we also see a growing role for technology to manage business risk efficiently.

Managing the risk of technology – IT Risk Management (ITRM)
While technology can benefit the organisation in unprecedented ways, it also creates a risk landscape which must be understood in the context of business objectives and well managed in order for the organisation to succeed. We are seeing a growing trend amongst organisations to align their ITRM activities with the wider enterprise risk management model so that the business impact of technology issues and failures can be better understood and investment in risk and controls is proportionate with the value it achieves.

Management of IT risks is not just about protection of IT resources from unauthorised or inappropriate use, it starts from the very alignment of the IT organisation with the overall enterprise, how efficiently it can support and enable the business, how it impacts actual operational activities, and how it can help reduce costs while providing adequate level of protection over IT assets. Because IT risk covers many aspects of the organisation, it is assumed that the 1st and 3rd lines of defence (i.e. operations and audit) will be able to identify, monitor and address these risks. However, that is not always the case, and often, if these functions are performing an element of ITRM, the efforts are not coordinated, consistent or consolidated for an enterprise view.

The ITRM function within an organisation operates as a distinct, but integrated, function within IT. It supports the enterprise as a whole addressing the strategic objectives, mission and business mode of the organisation. An ITRM function manages the organisation's risk posture and appetite for IT risk and security by determining the key IT treats that an organisation faces and leading a proactive response to combat these threats.

ITRM should define a comprehensive view of IT risks; continuously refresh the inventory of IT risk; help create strategies to prevent, mitigate or accept these risks; and monitor risks against defined tolerances. Through fit-for-purpose design, skills and competencies, and GRC tools, the ITRM function provides management an opportunity to proactively operationalise and manage risk, establishes a platform that audit can leverage, and transform its technology risk needs into a capability that plays to the broader enterprise strategy and the critical issues that organisations face.

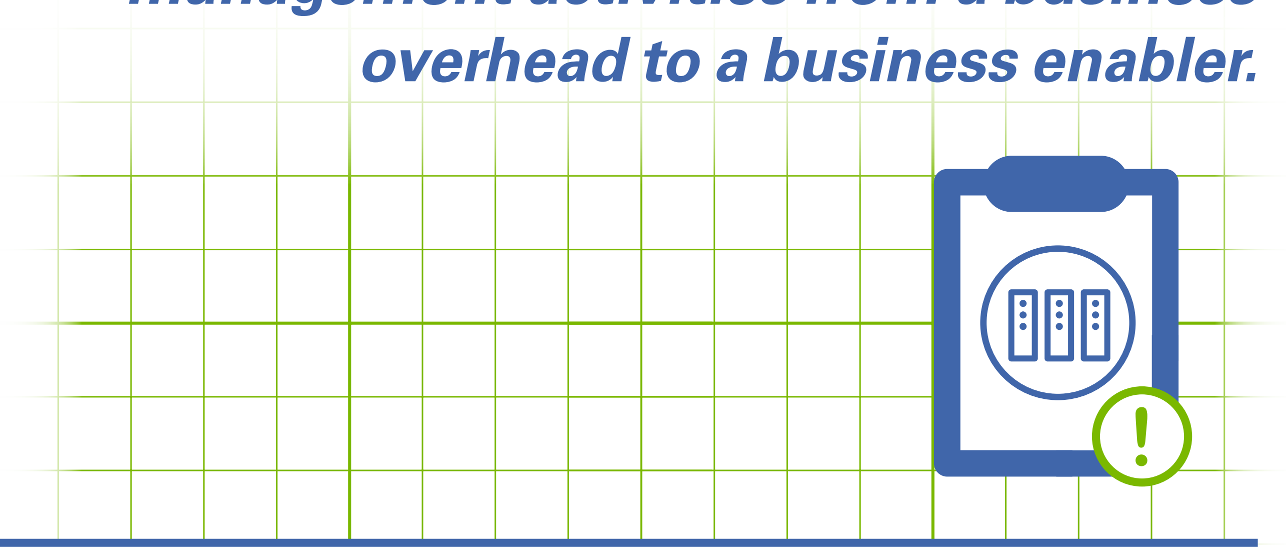
Using technology to manage enterprise wide risks
Technology can be the perfect medium through which risk management can stay close to the business and bring together the three lines of defence, while supporting risk as well as performance objectives. Today, we are starting to see risk tooling achieve some of these objectives. Risk management is evolving into a more integrated and repeatable process, rather than a series of staccato procedures. We are seeing an increase in the functionality of Governance, Risk and Compliance (GRC) systems and the integration of data analytics, making them more useful across all three lines of defence, providing greater reporting and insight but also enabling continuous monitoring/ auditing.

We're seeing organisations increasingly invest in data analytics and continuous monitoring technologies to help identify and understand where operations deviates from the designed processes and controls. This understanding is then used to weed out exceptions, either by changing the

Responding to technology risks – Technology enabled risk management (cont'd)

design or driving higher levels compliance, with in turn reduces risk and increased efficiency. Having a mechanism that integrates risks, controls and compliance across the three lines of defence establishes a single version of the truth – which is vital when dealing with new regulations across jurisdictions and when getting to grips with the constantly morphing global risk environment. Embedding data enabled risk management in the business is the only way to build risk considerations into front-line systems.

> ***Using technology to enable risk management can bring benefits in every area from compliance and regulation to standardisation and predictive analytics, turning an organisation's risk management activities from a business overhead to a business enabler.***



Appendix – Media-reported events: Data analytics

How we obtained and analysed the incident related data used in Section 1

Search methodology

We used KPMG in the UK's *Astrus* infrastructure to scan the Internet for publicly available English news articles related to IT incidents. *Astrus* utilised LexisNexis as the primary data source and included some subscription-only news sources.

The internet search methodology was built on the principle – "an IT (adjective) incident (noun) happened (verb)". By applying this principle, we developed hundreds of combinations which were translated into queries and supplied to *Astrus* to retrieve relevant news articles and events.

We defined an IT incident as an event that affected the Availability, Quality or Security of Information or Technology.

The script was executed for the 12-month period from 1 September 2013 to 31 August 2014. More than 10,000 news articles were retrieved.

Result set and analysis

The result set was analysed using a combination of automated and manual techniques to improve accuracy and relevance so that:

- The result set included incidents rather than potential threats.
- The result set included incidents that happened during the time period rather than after effects (of a prior incident) that were reported during the time period.
- Each article in the result set represented one incident. If a news article included multiple incidents, then each was considered separately. If multiple news articles referred to the same incident, one of the articles was included in the analysis.

A total of 522 relevant IT incidents were included as part of the final result set. Based on a pre-defined taxonomy, our IT risk professionals then reviewed these incidents and identified the following attributes for each incident.

- What happened?
- What were the causes?
- Affected companies and industries
- What was the estimated financial impact?
- How many entities or people were known to be affected?

The resulting analysis was presented to our technology risk specialists to draw judgements and conclusions which have been presented earlier in this report.

The internet search methodology was built on the principle – "an IT (adjective) incident (noun) happened (verb)".

Astrus, KPMG's secure on-line due diligence tool, provides a robust and cost-efficient way to obtain information and assess risks associated with customers, agents and counterparties. Astrus uses advanced search technologies to scour an extensive range of on-line public data sources, global sanctions and regulatory enforcement lists, corporate records, court filings, and press and media archives.

For further information on Astrus, please visit the KPMG website at http://www.kpmg.com/uk/en/services/advisory/risk-consulting/services/forensic/pages/astrus-enhanced-due-diligence-and-astrus-monitoring.aspx.

Contact us: A - Z

Curtis Baron
Director
KPMG in the UK

Greg Bell
Partner
KPMG in the US

Fayaz Cheema
Director
KPMG in the UK

Nicolina Demain
Senior Manager
KPMG in the UK

Jon Dowie
Partner
KPMG in the UK

Ben Foulser
Senior Manager
KPMG in the UK

Joshua Galvan
Managing Director
KPMG in the US

Paul Holland
Director
KPMG in the UK

Hesham Karim
Manager
KPMG in the UK

Phil Lageschulte
Partner
KPMG in the US

Martin Lunt
Director
KPMG in the UK

Vivek Mehta
Managing Director
KPMG in the US

Kiran Nagaraj
Director
KPMG in the US

Andy North
Director RC
KPMG in the UK

Ronald Plesco
Principal
KPMG in the US

George Quigley
Partner
KPMG in the UK

Andrew Shefford
Managing Director
KPMG in the UK

Jamie Thompson
Director
KPMG in the UK

David Timms
Senior Manager
KPMG in the UK

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

www.kpmg.co.uk

Produced by Create Graphics | CRT039402 | August 2015