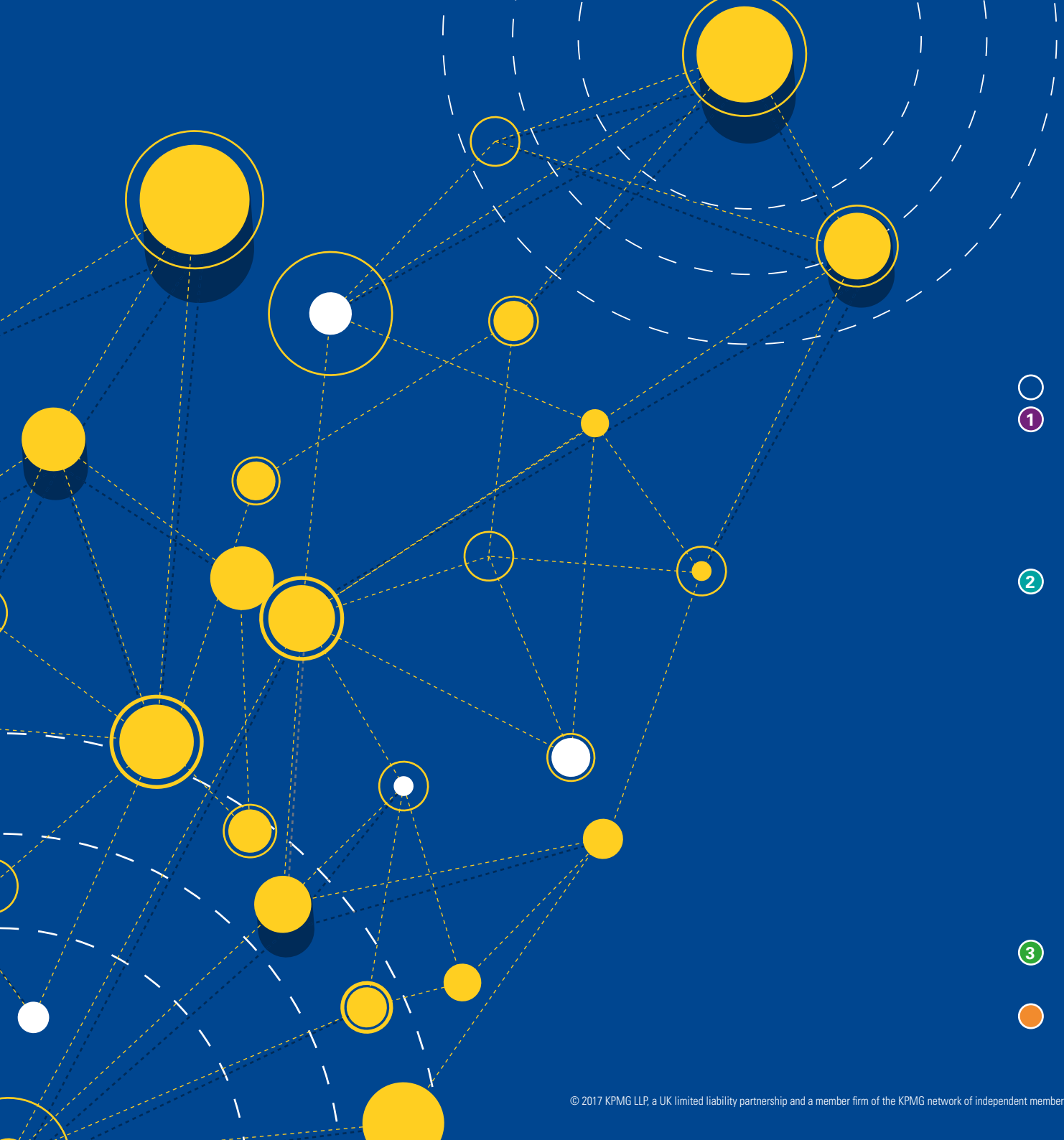
KPMG

Technology risk radar

Third edition



Contents

Introduction

What are the current and emerging technology-related risks that businesses face? What types of incidents have been reported in the press? What are the trends in different industries? And what are the risks on the horizon facing businesses tomorrow?

KPMG's Technology Risk Radar seeks to provide answers to such questions by combining extensive analysis of reported technology incidents with qualitative insight from industry specialists. It provides a broad-ranging view of the global technology risk landscape by offering insight into what's going on, and what's going wrong, across the market.

The Technology Risk Radar enables risk and audit professionals to make better informed decisions about the risks they should address while providing insight into where reputational risks may lie. Clients have told us that they have found this information invaluable in audit and risk planning exercises as it helps point them towards where the risk lies and what's driving it.

This third version is a refresh from 2015 and is based on another year of research covering numerous publications and web sources around the world. We filtered these for duplication, categorising and cross-referencing them to produce an overall analysis and a view sector-by-sector. KPMG member firms' industry experts then complemented this data by providing a narrative.

Across most sectors we saw new topics emerge such as digital labour and social media. But KPMG member firms continue to see well-known risks around cyber security, use of third-party services and legacy systems.

We all know there is a universal shift to a more digitally connected world. This means businesses need more advanced risk governance and management. The increased speed of technology developments and their impact on business models and operations means businesses have to keep a constant eye on evolving risks, taking a rolling view on what is relevant to them.

And, as organisations increasingly partner with other organisations and service providers, they need to consider risks from the 'extended enterprise' perspective. The value chain is only as strong as the weakest link.

On the plus side, IT investment is back in vogue and many organisations are replacing legacy systems to allow them to keep up with competitors and new entrants. The best way to succeed with new IT investment is employing the right level of assurance over the right risks – for which this edition of Tech Risk Radar should help.


Andrew Shefford

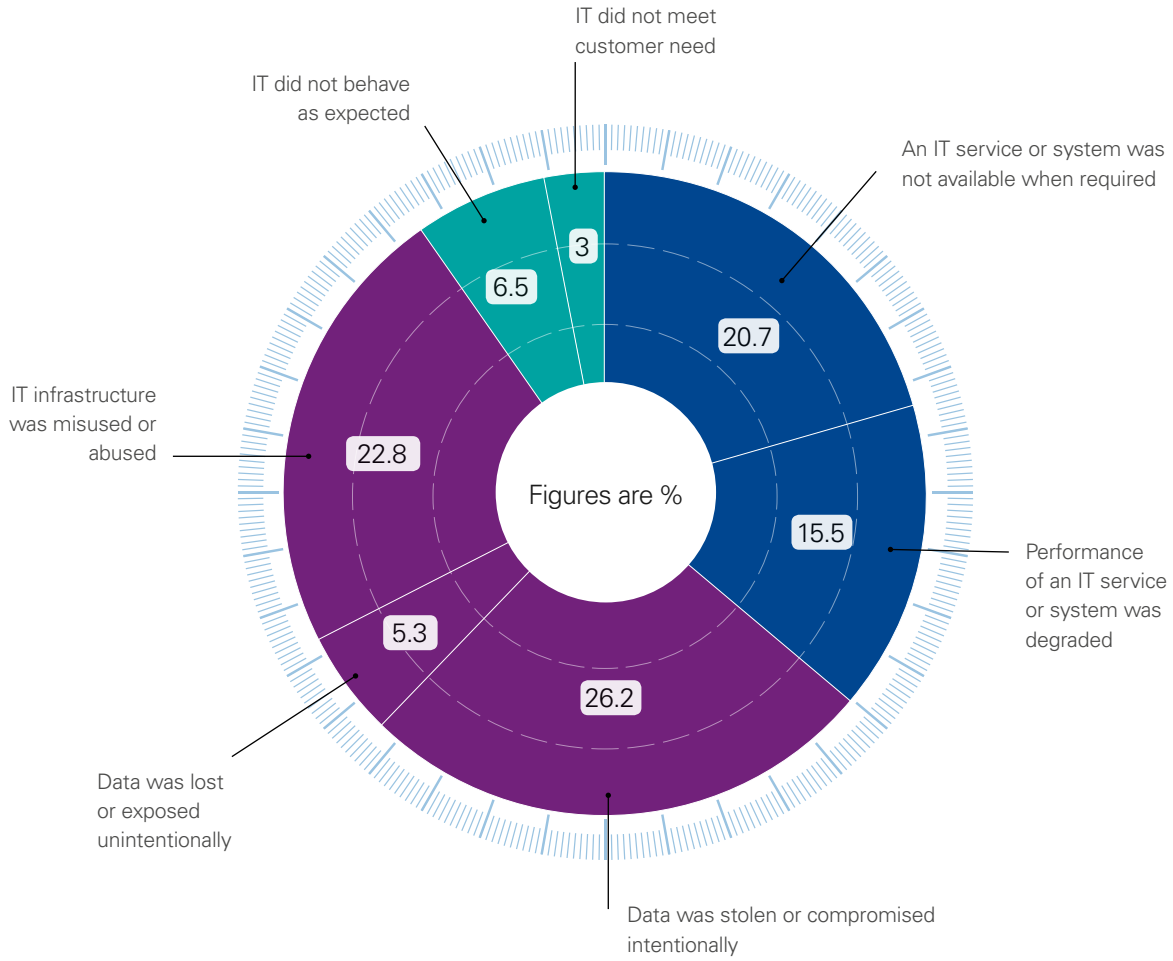

Kiran Nagaraj


Paul Holland


Priya Mouli

Media-reported events: Key findings

What happened?

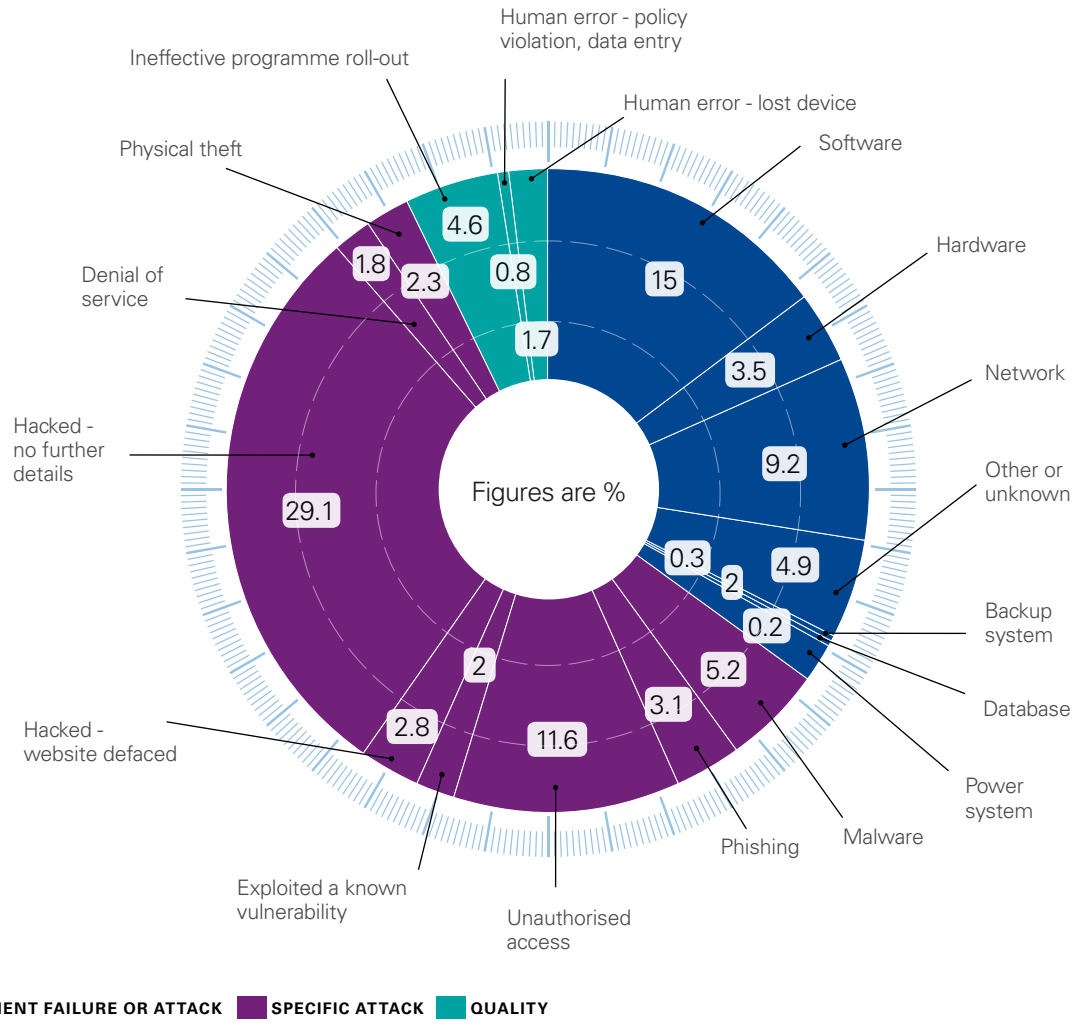


Cyber security incidents continue to be the attention-grabbing element of technology risk within business today. But here is something interesting that our research uncovered - only a little over half of the 700+ surveyed IT incidents were security related, with most being attributed to data being stolen or compromised intentionally. About 36 percent affected the availability or performance of a key IT service. And an additional 9 percent affected the quality of a key IT service with IT either not behaving as expected or not meeting customer need.

The proportion of incidents related to security, availability and quality followed the same order across all ten industries surveyed, i.e., security related incidents were most prevalent, followed by availability and quality related incidents.

These statistics are alarming, as these incidents must arise from a failure of internal controls – checks that should be a basic element in any security control system, technological or otherwise. Cyber security therefore, continues to be a key area of concern for organisations. Later in this document, KPMG member firms technology risk specialists provide some practical insights on how organisations can protect themselves and better prioritise their investment in this area.

What were the causes?



Over half (60 percent) of the total incidents across all industries were caused by specific attacks, including hacking, unauthorised access by an insider/third party provider, malware, phishing, and website defacement.

For example, Technology, Media and Telecommunications (TMT) was primarily impacted by incidents caused by hacking followed by unauthorised access by an insider/third party provider. As organisations in this industry increasingly outsource their IT service development and delivery, a number of third parties have greater access to the IT systems and the data housed, thereby exposing these organisations to substantial risk.

In Energy and Natural Resources (ENR) almost 50 percent of incidents were caused primarily by specific attacks such as hacking and malware. Though there is a high level of cyber security awareness in the ENR sector, organisations are often unable to allocate sufficient budget to effectively manage IT risk due to the complex system footprint, huge IT inventory, speed-to-market considerations, lower crude prices and compliance obligations, resulting in reduced profitability.

Around 54 percent of total incidents in the education sector were due to hacking and unauthorised access. These statistics seem high but make sense as the education sector manages a lot of Personally Identifiable Information (PII) such as the personal information of students, intellectual capital, and Protected Health Information (PHI), as universities are often affiliated to hospitals. Additionally, smartphones used by the student community prove to be easy targets for cyber-crime. Of the total incidents across all industries, about 30 percent were caused by glitches associated with software, network, hardware and backup systems.

What were the causes?

We found that a shockingly high proportion of incidents were caused by factors generally considered "avoidable" in the TMT and Government sectors. Avoidable causes, such as component failures contributed to by software and network glitches, led to around 35 percent of incidents in these sectors. These are avoidable as they can generally be prevented by taking the right precautions, exercising rigour when testing systems and building the right level of resilience to enable failover.

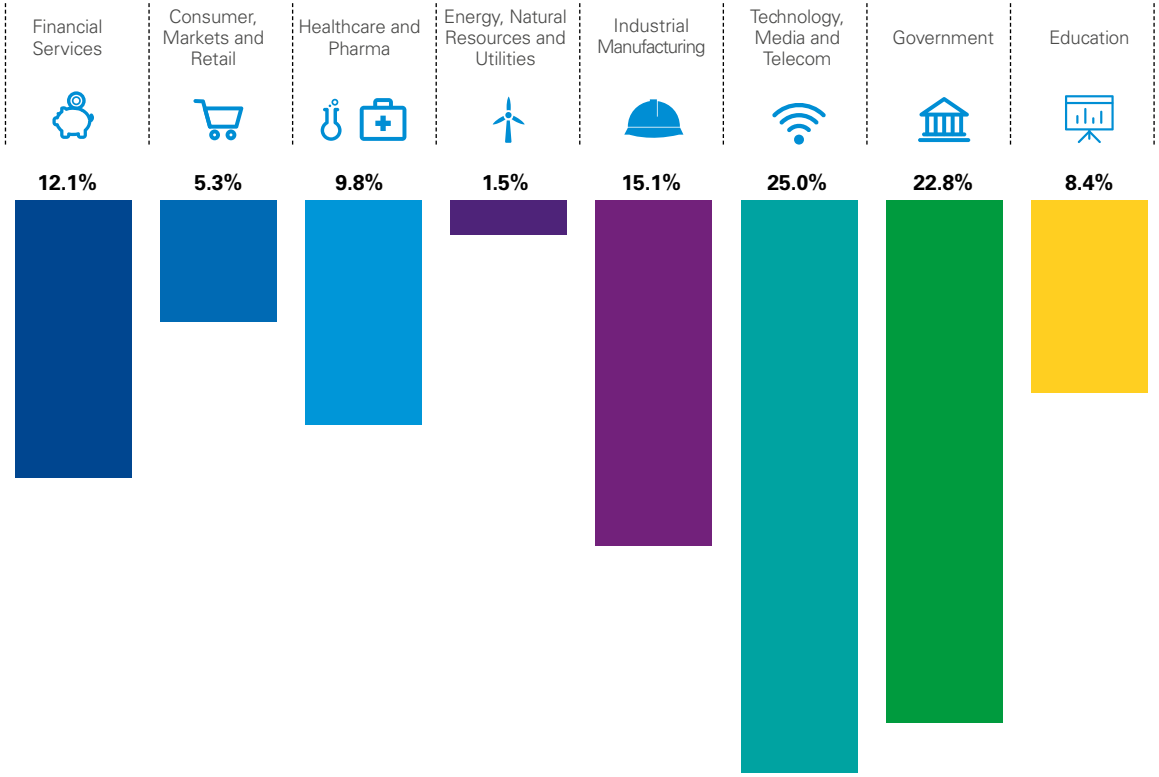
Though specific attacks continue to be a major threat, many organisations are still not getting some security basics right.

ENR had almost 20 percent of incidents attributed to power system failures. This is interesting given that this is the very industry that provides electricity and power for its customers. As mentioned above, some organisations in this sector are unable to invest sufficiently to manage IT risk.

Financial services (composed of banking, insurance and investment management and funds) suffered almost half of incidents caused by component and system failures with the leading culprit being software. Organisations in this industry could consider investment in improving their application and system development processes: implementation of better testing practices and better software quality management approaches (including for outsourced services) can reduce the risk presented by component failures. However, the increased investment focus for such companies is to scale up their operations and innovate, to keep up with the competition and disruption in the industry.

The remaining 10 percent of the total incidents across all industries were attributed to avoidable errors such as ineffective program rollouts. Though many organisations invest in security related training, measuring its effectiveness is more than merely a measure of the training attendance and assessment success rates. Organisations need to think increasingly about enabling and promoting a 'Risk Culture' to increase risk-conscious behaviour and this needs to be driven from the top.

Industries affected



The top two industries affected were the same as last year, although their positions have changed: Technology, Media and Telecommunication, and Government, in order.

- Technology now has the dubious privilege of being the industry most affected by IT incidents, according to our research. The growing shift to a digitally connected world with the pervasiveness of the Internet of Things (IoT), social media and digital labour, and the ubiquity of devices suggest that this industry will keep this top spot for some time.
- Government comes in at number two. We believe that the government sector has this high ranking due to the public nature of its operations, increasing third party risk and ineffective project management.
- The financial services industry has moved from the fourth most affected industry to the seventh among the ten industries surveyed. This may be attributed to the heavy regulatory environment within which FS organisations have built risk management capabilities that have arguably matured over the years. Interestingly the Fintech sector, which is a hybrid of Technology, media & telecoms – the most affected industry, and FS, is expected to face similar regulatory scrutiny.

What is also interesting is that specific types of incidents are affecting some industries more than others. For example:

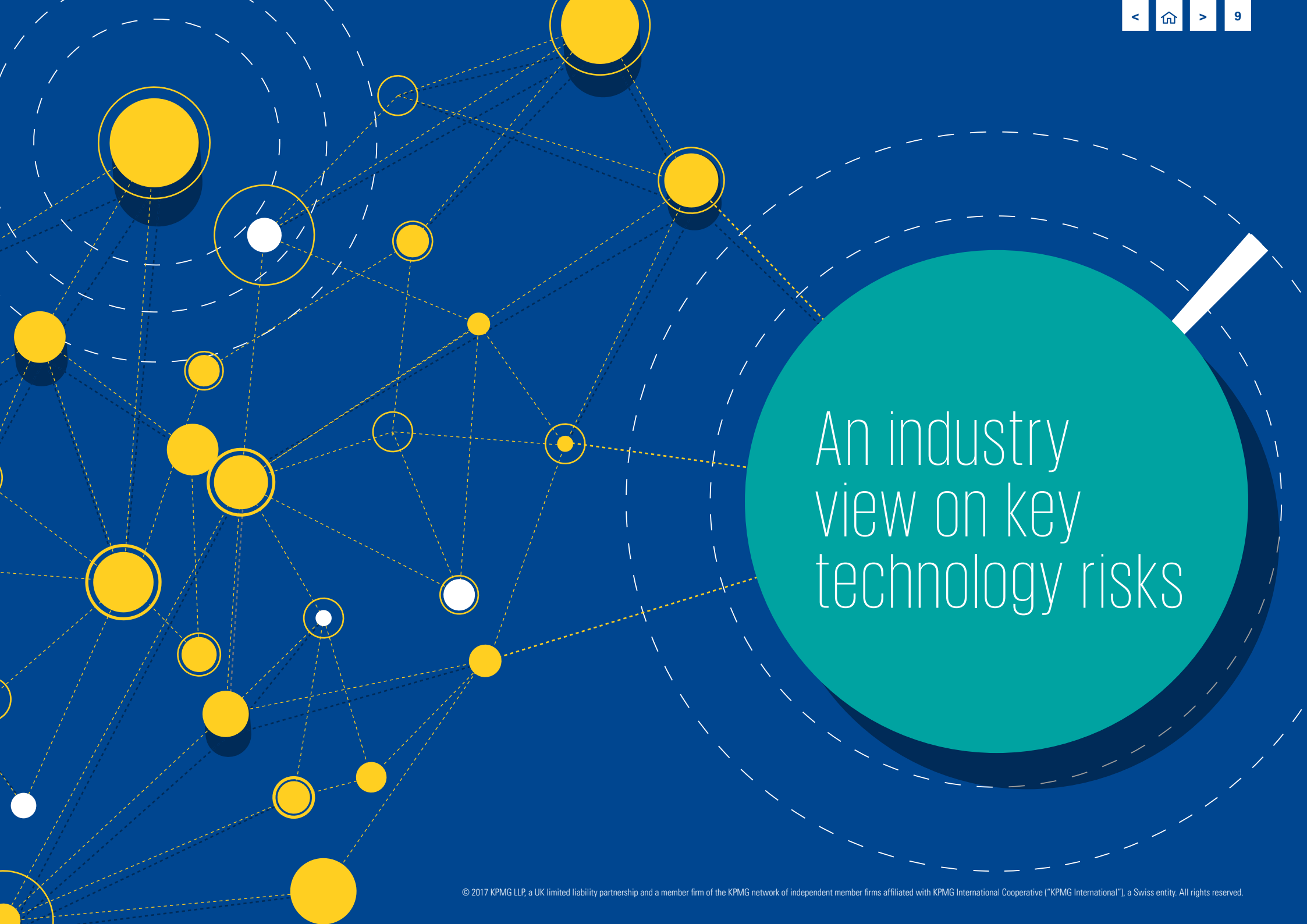
- Industrial manufacturing had a higher proportion of availability related incidents than any other industry. Availability also appeared to be significant problem in the financial services industry with 40 percent of incidents related to availability.
- Quality issues continue to be a problem in the Government sector with almost 17 percent of incidents related to quality.

Sectors at a glance

TOP 10 RISKS IDENTIFIED FOR EACH SECTOR

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

Risk impact and probability in descending order PER SECTOR		Banking	Insurance	Investment Management and Funds	Consumer Markets and Retail	Technology, Media and Telecommunications	Healthcare and Pharmaceutical	Energy and natural resources	Industrial manufacturing	Central Government	Education (Universities)	**Overall avg score** (the lower the score the more critical across industries)
Poor risk management alignment across organisation and process	1	6	4	9	6	4	4	6	9	9	1	**5.8**
Dependence on inflexible and undersupported legacy systems	2	4	6	4	6	6	4	4	6	9	6	**5.5**
Poor cyber security, cyber-crime and unauthorised access	3	3	4	4	4	4	6	6	6	4	9	**5.0**
Non-compliance with regulation and legislation, e.g. privacy	4	4	3	4	6	4	9	4	2	6	6	**4.8**
Lack of IT strategy and lack of board representation	5	6	6	6	4	2	2	6	2	4	9	**4.7**
Inadequate data quality and lack of capability to leverage data to manage risk	6	4	2	9	2	9	6	2	2	4	1	**4.1**
Inability to deploy and exploit emerging technology	7	6	9	1	9	4	1	2	2	2	4	**4.0**
Failure to deliver programmes and to build in control, resilience and security	8	3	4	2	2	2	6	6	4	9	2	**4.0**
Reliance on, and poor security and control in, vendors/third parties	9	9	3	6	6	2	2	3	1	6	1	**3.9**
Ineffective service management and delivery	10	6	2	6	4	2	2	2	2	2	1	**2.9**
Ineffective IT asset management	11	2	2	2	2	3	3	2	3	3	4	**2.6**
Inadequate resilience and disaster recovery capability	12	3	2	2	2	2	2	2	4	2	2	**2.3**



An industry view on key technology risks

Banking

David DiCristofaro

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability

There have been a few red faces in banking over the past couple of years. High-profile technology-related incidents have caused ATM networks to fail, payment systems to seize up – and even central bank systems to go down. Media and public attention has made those affected respond fast.

Root cause analysis has shown that many of these incidents were due to problems with third-party suppliers. It's not the banks' own operations that have been putting them at risk – often it has been the operations of the vendors and partners they rely on.

The good news is that it appears that the number of these incidents is falling. If this is the case, we believe that it could be because of greater management focus, improved remediation, and a healthier understanding and management of the risks associated with third-party providers. Banks realise that their business partners need to have at least the same high bar on risk thresholds as they do. And that is forcing better governance, risk management and compliance in those wanting to partner banks.

While third-party dependence continues to be a major risk issue, our view is that it is being overtaken by other risks, including poor IT strategy, cyber-crime and the risk of business interruption.

One of the main root causes common to all is the management and control of super-user access. Theoretically only a very small number of users should be able to do everything in a system. But as time goes by, banks often lose control of the numbers of super users. When perhaps three developers had super access to a system they were installing or doing an access review over, it's common to find that a year later that number has risen to 10. Potentially most dangerous is when one of these is a vendor.

Banking (cont'd)

This comes back to the point about third parties. The whole vendor risk management programme is huge and critical for every bank. Questions banks should be asking include: how do we pick our vendors, how do we monitor them, and how do we remove them when they cannot meet the standards we need. Banks that aren't focusing on this yet should put vendor risk management at the top of their regulatory agenda right now.

Sadly no system is foolproof. Manual processes fail, sometimes through lack of proper training. Hardware components break down, occasionally within weeks of scheduled maintenance. It is impossible to legislate for all possible system fragilities.

But there are still measures banks can take. First they should try to automate their processes as much as possible. Second, they should make sure they have the right kind of backup and redundancies. And third, recovery must be as swift as possible. No matter how good the backup, responsiveness to the root cause analysis is critical, not least to reduce the risk of the issue happening again.

And for brand management reasons. The power of social media means that outages are trending around the world within minutes, not hours or days. Banks simply have shorter response times to work through problems than in the past – something they are factoring into their remediation processes.

The push for this must come from the top. Board members have to understand technology. They have been slow to grasp this challenge but KPMG member firms are seeing signs of change. Some boards are designating one of their members to keep an eye on technology; increasingly non-executive directors are challenging the auditors and management about technology risks. We applaud this trend but believe that more banks need to follow suit.

We also feel the lines of defence need to be better aligned with the business. It's not unusual to find that internal audit is working to a different set of risks than compliance – and that the business has a different view again. The technology risk organisation in the business must have good communication with compliance to bridge any risk gaps. We are seeing some banks set up a one-and-a-half line of defence to align their risk management better. This is a good start. But we believe that more banks should be taking this direction, focusing on getting compliance and the business to work better together while maintaining the independence demanded by the regulators.

Risks vary according to bank. Most are talking to the regulators about four issues: cyber risk, protecting against system outages; third parties and reliance; and IT strategy through matters such as automation and robotics.

There is no silver bullet to deal with each of these. But the one overarching factor that does make a difference is having more technology expertise on boards. Only then can those at the top have the confidence to challenge business strategy, to point out the risks, to make informed decisions on risk appetite and to decide how best the risks should be managed.

"The whole vendor risk management programme is huge and critical for every bank. Questions banks should be asking include: how do we pick our vendors, how do we monitor them, and how do we remove them when they cannot meet the standards we need. Banks that aren't focusing on this yet should put vendor risk management at the top of their regulatory agenda right now."

Insurance

Jill Farrington

Jon Dowie

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability

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

Time plays a key role in the insurance business. Not only when writing business, but crucially when looking at the sector's technology risks. On a day-to-day basis companies are worried about performance, cost, security and data breaches. On a longer term basis they are dealing with legacy systems while moving into newer technologies and digital services to secure their future. The time scale involved might vary, but the technology threats from each are equally serious.

Consider the moves into digital. This is affecting the way that insurers promote, distribute, and underwrite their products. While in the past business was conducted through brokers and agents, now insurers interact directly with consumers through mobile solutions. This has a direct impact on risk. Insurers need to make sure that their products are always secure, are constantly available, and that the integrity of data is maintained.

Then there's the overhaul of systems. Insurance companies are moving from often decades-old systems as they transform their processes and technologies. This brings a whole raft of risks, not least in the migration of data, but also, again, over the integrity and security of that data.

What should companies do when faced with these major transformative projects? We believe that they must make sure right from the start that technology risk is incorporated into the design and deployment of their new systems and processes. Only then can the appropriate security and controls be designed and built in to the overall lifecycle of these new solutions.

This starts with the board setting strategy, thinking through all requirements before starting work building them in. And, vitally, it includes ongoing maintenance. Organisations must make certain that once they have deployed their

Insurance (cont'd)

latest technology, there is a strong infrastructure in place to continue to manage and govern risk in the end state.

Insurance companies are getting better at having the right skill sets at the board level to oversee and manage technology risk appropriately. But we feel there is room for improvement. Boards should be asking more questions about the risk governance process. They need to have a better overview of what is going on and be sure that the organisations they govern have the resources, processes and protocols in place to understand incidents, to know how to respond to them, and to ensure a fast response.

Part of the reason why this is hard for boards is that insurance companies often think about technology risk tactically, such as by thinking about security as managing data and the perimeter walls. We believe that boards need to concentrate on the overall picture, embedding a technology and risk management strategy into everything the business does. Some companies already do this. But we think the practice needs to be more widespread.

And this approach does more than help manage technology risk. Having embedded security, rather than slotting it on as an afterthought, can be a great market differentiator when it comes to deploying new solutions.

Another of the technology-related risks facing the insurance sector comes from outside – from new technologies in other sectors. Self-driving cars, personal health devices and home monitoring devices all carry their own technology risks, the biggest of which relate to security and integrity of data. Liability for breaches is shifting from being consumer-oriented to being product-oriented. That will have a big impact on insurers' underwriting business – raising questions about what information and control, if any, insurers have over the technology being used.

This brings us back to the wider point: the impact of technological change. There is a lot of disruption in the insurance industry and much of it is down to advances in technology. KPMG member firms have seen this trend increase over the past few years and know that it will only grow further and faster.

Much of the current focus within insurers is on business processing, such as claims processing. But some are starting to turn to cognitive technologies and advanced analytics to get rid of manual processes. This is just the start of a greater trend to use robotics higher up the value chain as a more integral part of the business. And this trend will demand an even greater concentration on security and controls.

Boards and executive management are starting to pick up on the risk element of these new and emerging technologies. Managing those risks effectively is only going to get more important as organisations move into uncharted territory. The implications of not doing it right are enormous. This is why our main message is simple: for insurers to embed technology risk management into every product, every service, every new platform and every business decision.

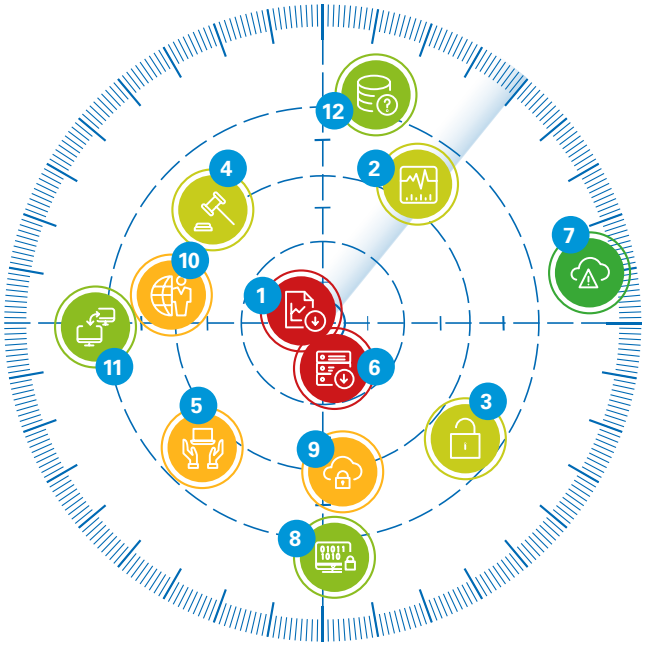
"Insurance companies are getting better at having the right skill sets at the board level to oversee and manage technology risk appropriately. But we feel there is room for improvement. Boards should be asking more questions about the risk governance process. They need to have a better overview of what is going on and be sure that the organisations they govern have the resources, processes and protocols in place to understand incidents, to know how to respond to them, and to ensure a fast response."

Investment management and funds

John Machin

Ameet Sharma

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability



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

In current market conditions where generating alpha is tough, investment management companies are under huge pressure to do more with less. Cost-cutting programmes are rife. Short-term affordable bolt-on tactical solutions are often considered more favourable than longer, larger complex strategic programmes. But implementing off-the-shelf packages often comes at far greater cost than the supposed savings achieved.

We believe that a key technology risk for the sector lies with investment management firms not having the effective oversight or proper controls and processes in place. This is often because organisations feel they do not have the luxury of time or money to fully understand how they might truly transform what they do, by making it more effective and efficient through simplification and standardisation. Instead they tend to buy a solution to plug a gap. Often the solution simply doesn't provide the functionality it needs to. New solutions generally provide a mountain of exception reports – but there is no process or appropriate personnel to sift through and make sense of these, working back to and eliminating the root causes as necessary. Instead KPMG member firms often see a sticking-plaster approach taken to individual incidents.

Without a strategic mindset to ensure a comprehensive and effective approach to technology risk management, too many organisations find themselves in fire-fighting mode. We can see the result through response and remediation times for all kinds of incidents – security, availability and quality – these are generally rising at the same time as the number of people who can deal effectively with these incidents is falling.

Investment management and funds (cont'd)

But how might boards effectively tackle this? They can certainly start by having clarity on overall responsibility for technology risk and gripping this challenge more tightly. They need to realise why this is crucial –as unless the full range of risks and their root causes are properly understood, the organisation itself is at peril through reputational risk arising from catastrophic failure.

There's no doubt this is a tough call given the huge regulatory pressure on the industry. Fund managers feel as though they are constantly chasing their tails to keep up with compliance changes. They desperately need to divert whatever money is available to deal with the regulatory burden. Turning to third-party solutions seems an easy get-out in the circumstances. But KPMG member firms experience is that major technology incidents in financial services – both reported and unreported – come directly from the use of and interface with third parties. Worryingly, many board members are not aware of this.

Fund managers acknowledge that the industry has specifically underinvested in data in the past. Many admit to issues around aspects of data classification, processes, quality and privacy. With MiFID II, Europe's ambitious reforms in response to the financial crisis, companies have a better view of the requirements around data regulation. This is already driving a great deal of interest and sorely needed investment in data management and governance, and about time too.

The good news is that we see boards' involvement in data and broader technology risk issues also increasing. Partly this is due to the number of incidents where data leakage has caused reputational damage over the past few years. Non-executive directors are particularly keen to be seen to challenge and to find out what can and is being done to improve matters in a sustainable manner that they can be assured on.

But we need to see this being more wide spread across the industry. Boards need to accept that quality data is vital to the quality of business decisions and must be managed in a more strategic way. They have to think about opening new platforms and solutions to simultaneously meet client service needs and regulatory requirements. This means they must better understand what is happening at the sharp end of their businesses – in their core processes and back office – than they have in the past. Without a thorough understanding they may assume greater comfort than is warranted based on poor quality and badly presented management information, and not really understand the uncomfortable realities of resilience, back-up and recovery capabilities within their organisations.

Above all, Boards need to make sure there is an effective three-lines-of-defence system in place. But how can they do this in these cost-constrained times? In part the answer lies in having more streamlined intelligent systems (such as leveraging cognitive techniques and robotics) to achieve more straight through processing and involve less human intervention, in order to increase efficiency and effectiveness and reduce errors.

Boards have a vital role to play in ensuring the balance between investment managers making short-term returns and protecting the business and its assets in a sustainable manner. The costs of implementing robust and intelligent systems might be high. But with fundamental changes in regulation, problems of legacy systems, and proliferation of spreadsheets and manual processes, the downside of not making this investment now could greatly outweigh the costs to the business of not seeing this through in the long term.

> "A key technology risk for the sector lies with investment management firms not having the effective oversight or proper controls and processes in place. This is often because organisations feel they do not have the luxury of time or money to fully understand how they might truly transform what they do by making it more effective and efficient through simplification and standardisation. Instead they tend to buy a solution to plug a gap."

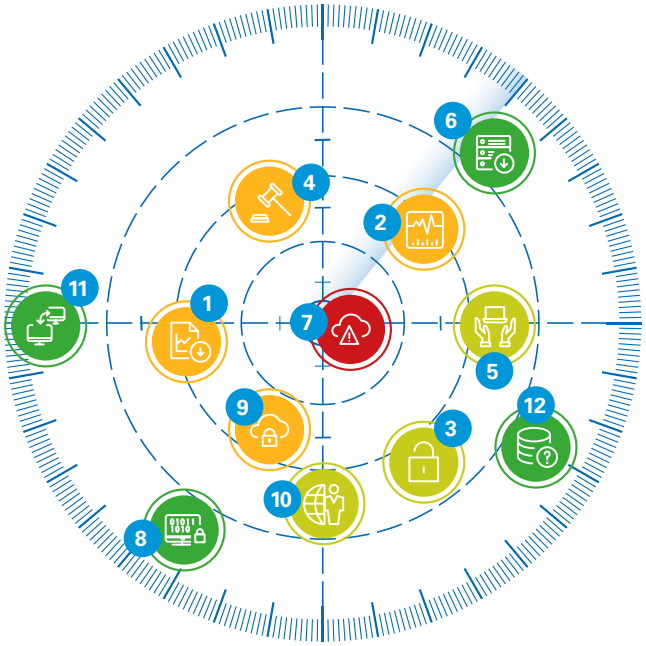
Consumer markets and retail


Andrew Shefford


Paul Holland


Michael Isensee

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability



Technology continues to be a major business disruptor in the consumer markets and retail sector. Digital disruptors are driving every part of the sector's biggest changes, from new delivery models such as drones and 3D printing to greater automation in industrial production and connectivity via the Internet of Things.

Yet we believe that, despite these innovations, the technology risks which consumer markets and retail businesses face are not so new.

Take automation. New technologies that are driving developments in digital at the front end and connecting industrial control systems at the back end need to be safe, secure, repeatable and reliable. These are all issues that already apply to back-office functions, often running on legacy systems, such as administrative processing facilities and increasingly connected manufacturing systems.

Now consider the integration of legacy systems with the newer digital systems required to connect with today's consumers. These older systems are often neglected. There has been little investment in updating them and many are simply not as adaptable as modern systems. And yet businesses have a lot of valuable data in them. Providing safe access to this data for newer systems presents a set of risks such as data integrity and privacy – risks that businesses already face.

Digital also presents organisational challenges, with many businesses facing challenges where a digital team, either in-house or working with a third party, in effect competes with the IT Department. This is an example of what is sometimes known as shadow IT, as discussed above, where digital products are developed and maintained by a business team rather than by the IT function. Again, creating IT products outside of IT is not new, but where the products are the digital

Consumer markets and retail (cont'd)

face of the organisation and generating revenues and profits, or could contain sensitive data, e.g. confidential personal information, it is a more challenging risk than perhaps it once was.

Major changes to privacy legislation in Europe do not create new risks per se, but companies need to stay on top of the revised rules. Too often companies concentrate on the initial risk: not being compliant with the rules, not having good controls and being vulnerable to data loss. There's also the risk associated with new legislation – of not realising that your organisation is no longer compliant; of no longer having sufficient or adequate controls in place.

Consumer markets and retail companies have been working on these risks over recent years. KPMG member firms have seen progress in their risk management approaches. But the pace of change is so fast that they need to run just to keep up. Change in itself creates risk and as the pace of change increases so does the risk profile consumer markets companies have to handle. With the increased volume and velocity of risk comes a demand to step up risk management capability.

We believe that to manage the increasingly complex risk maze companies need to ensure they are setting clear strategies in key areas.

First is leadership. We see room for more IT leadership sitting on boards and taking a leading role in the c-suite. The person who is driving technological change needs to take a leadership role to ensure a fully-integrated view of how the technology will deliver, what the associated technology and business risks are, and how to address them.

Second, many 'modern' technology risks can still be reduced by quite basic measures. For instance, making sure your organisation has a decent password policy and that you enforce it. Putting processes in place to see that in-house servers are patched correctly. Using a reputable outsourcer and writing a decent contract. And reviewing the state of security at any third parties.

You might think those are indeed basic measures and you will have a complete handle on such issues, but it wasn't long ago when a KPMG member firm was asked by a leading listed company to review its IT security. We broke in to the ERP system using the basic passwords that the system had been shipped with and got full admin control. This was a real shock to those in charge.

We know that margins are tight in consumer and retail businesses and that resources are hard to come by. But we believe that modest thoughtful investment in basic risk management processes integrated into Enterprise Risk Management (ERM) can solve a lot of problems without breaking the bank.

Above all, do not fall into the trap of thinking that concentrating only on cyber security is everything. Fixing cyber threats will not fix the company's change management process.

If your organisation does not do this then it faces today's overarching risk: of not being able to grasp opportunities. Existing consumer businesses are under threat from new, agile companies unburdened with old IT infrastructure and flabby systems. Your organisation needs to be ready to compete with them. Building in good compliance processes is a key starting point. Lean and pragmatic processes are critical.

Managing risk well presents a great opportunity to challenge processes and make them fit for purpose. Remember that new companies are creating their risk management processes from scratch. Only by adapting to this new reality and having smart and lean systems fit for the evolving risk environment can existing businesses compete in tomorrow's consumer world.

"We know that margins are tight in consumer and retail businesses and that resources are hard to come by. But we believe that modest thoughtful investment in basic risk management processes integrated into Enterprise Risk Management (ERM) can solve a lot of problems without breaking the bank."

Technology, media & telecoms

Annie Armstrong

David Eastwood

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability

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

Consumers are the life blood of the TMT sector. New media companies, telecoms providers, technology businesses – all have direct connections with consumers. And through those connections they collect a vast amount of personal data.

We believe that the top technology risk facing the TMT sector revolves around data: personal data, business data and employee data. Over half the incidents in our survey results had a security impact, and half of those were around data loss. The sector is responding by putting a vast amount of resource into tightening access and trying to prevent data leakages.

But we think data risk is about more than security. Big data is the order of the day. Companies are keen to know how they can mine their data to drive better business. They see this as the future – and the constant improvement in data analytics increases their interest in the huge potential that big data has for them.

The problem is that this push from the business side is running ahead of societal expectations. As data volumes increase, companies will find they have acquired data in ways they hadn't expected and that they can use it in ways they hadn't expected too. But are they considering the implications – the impacts on privacy or on civil liberties?

We don't think they are thinking about this enough. We believe the real challenge is for TMT companies to judge how society views what they can do, with data, against what they want to achieve. That mismatch between what is possible and what is acceptable will only grow. And that is where the risks arise. Regulators are already on to this and stiffer (and more complex) regulation is on its way.

What should companies be doing? We think that boards need to have a better sense of the data within their organisations.

Technology, media & telecoms (cont'd)

They must have a collective strategy for how big data is created and used – and how it should be used.

This involves having a very clear idea of what is suitable and palatable to the public. Each TMT organisation should appoint someone senior to take an overview on this – to set strategy and keep operations appropriate, defensible and within societal expectations. Too often the data privacy role is seen as a regulatory compliance role. We think it is much more than this: data should be at the heart of business strategy.

The TMT sector faces other challenges with risk implications. One of these is migration to the cloud. Like all sectors TMT is an enthusiastic user of cloud business models. At the same time a number of TMT companies also provide enabling platforms.

As users, TMT companies need to keep control over the cloud services that their people buy. Growing informality around internal purchasing decisions could cause cost, security and data problems unless there are coherent controls around purchasing decisions.

As providers, they need to think about the impact of the movement of applications from one cloud provider to another. Users who want to change providers may have problems migrating data; they might even have to change their business models if they swap platforms. This brings the relatively new risk of migration disputes with service providers. This might not have been on TMT companies' risk radar before – but it certainly needs to be now.

Somewhat ironically, KPMG member firms experience is that some TMT companies are poor managers of their own internal IT systems. Often this is due to acquisition-driven growth meaning different systems have been grafted together.

Having a raft of different systems can produce enormous overloads. Information can be lost and revenue opportunities missed because companies are unable to consolidate their data. Adopting a sticking-plaster approach to repairs creates vulnerabilities. This makes it difficult to work out where problems are, to see who is responsible and to resolve issues. Strategic thinking over spending not only helps minimise problems and resolve them faster – it also reduces the risks associated with having different bolted-on systems.

Ultimately, though, KPMG member firms see data as a common theme running through all these major issues. Whether it's use of big data, data security, migration of data to cloud services or managing data in diverse systems, we believe data is the source of the main technology related risks for TMT companies. More data – and it increases exponentially – means more risk. And that's why we think that data must be at the heart of TMT boards' risk management strategy and their companies' risk management practices.

"Having a raft of different systems can product enormous overloads. Information can be lost and revenue opportunities missed because companies are unable to consolidate their data."

Healthcare and pharmaceuticals


Jamie Thompson


Caroline Rivett


Nicolina Demain

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability

Many organisations in the health and pharmaceuticals sectors focus on cyber security. This is because they see that the number of attacks has increased over the past few years.

But the type of attack is changing too. Ransomware attacks have had a huge impact on the health sector in the past 12 months. Out of 28 NHS trusts that responded to freedom of information requests, all but one admitted to having been the victim of a ransomware attack. In one case a hospital's entire pathology systems was inaccessible for two days as a result.

These threats are recognised by most health leaders. The problem is often making sure that this awareness filters down through the organisation to those who are responsible for entering and managing data. Continued training is vital. KPMG member firms recommend specific awareness training for cyber-related incidents using real-life scenarios to demonstrate the ease with which the attacks can be made and the devastating impact they can have on a health organisation's operations.

The cyber focus is different for pharmaceuticals businesses. They are more concerned about keeping valuable intellectual property safe: not just their own IP and trial data but also that of other research institutes with which they are collaborating.

The pharmaceutical sector is changing. There is a lot of excitement in the sector over the growing adoption of monitors and feedback mechanisms. However there are serious security and privacy implications too.

A number of provider companies are starting to consider how personal data flows from devices onto storage, how this data is protected and the impact of it being lost or stolen. Once these companies start looking at this in detail, they are often surprised at how complex this issue is: at the sheer number of different activities that they need to think about around personal and confidential data.

Healthcare and pharmaceuticals (cont'd)

What should pharmaceutical companies be doing to keep this data private and secure? The starting point is to understand what personal data is being collected. Then they have to understand data flows in transmission, such as from devices to databases. Next is how the data is being protected. This includes looking at regulations, such as the new EU rules on the protection and use of data from medical and monitoring devices.

Meanwhile the health sector faces a legacy system problem. Most trusts have aging infrastructure, are using systems which are no longer supported, or have had consultants develop their own systems to work around the lack of appropriate systems in place. The health service is trying to replace its clunky old systems and remove stand-alone systems which have been added on by frustrated clinicians, moving towards more agile comprehensive digital systems which can better fit the needs of patients and staff.

Such a major transformation must be business-led to succeed. It has to be more than replacing a part-manual, part-computerised series of processes with a digital one – it needs to focus on how to make all processes better. New systems must keep the cultural impact and cultural change at the forefront. Only this way, once the system is fully implemented and people are comfortable and happy using it, can the health organisation reap the full benefits of the transformation.

Another big issue within health is information sharing. The sector is looking at ways of joining organisations to come up with new care pathways, offering a holistic view of healthcare rather than a solid approach. This means sharing more information. Organisations need to understand how to do this while meeting legislation and regulations. Questions to ask include: "are we clear to patients about what information they are sharing, giving fair notice, disclosing what the information will be used for and getting the appropriate consents?"

Robust risk management practices are vital. Boards need to make sure that there are processes in place to identify risks, to prioritise them, and to set their organisation's risk appetite. Some mature organisations recognise the lasting damage done by IT failures and have strong governance in place over new programmes and projects. But we believe this approach needs to be more wide-spread than it currently is.

The health sector only has so much money to invest. It rightly prioritises patient care. But organisations must consider the dangers of not investing in new technology or in appropriate risk management. Technology teams working in the sector might be unused to making a business case for changes. But only by having a robust case to justify new investment can they show boards why investment is needed – and what the real cost of not investing could be.

"Questions to ask include: 'are we clear to patients about what information they are sharing, giving fair notice, disclosing what the information will be used for and getting the appropriate consents?"

Energy and natural resources

Nathan Cain

Joshua Galvan

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability

However distinct the components of the energy and natural resources sector, with their very different processes and customers, we see them sharing various prevailing technology risks today.

Consider first the risk of data loss and theft, particularly with respect to a company's most valuable assets. For oil and gas companies, this translates to engineering specifications, reserves and reservoir data, and technical solutions and processes for extraction, manufacturing and distribution. For utilities this includes customer data, with all the privacy and reputational implications this brings.

ENR businesses can be incredibly complex and so another risk is that of shadow IT – solutions implemented, configured and managed by a non-IT competency in a business unit. Shadow IT introduces various risks such as security, integrity, software licensing obligations and unnecessary IT systems landscape and operations complexity.

The aging computer platforms so common in the industry introduce risk in the platforms themselves and more often in their replacement. Too often the associated large projects aren't well managed and the full remit of business and technology requirements are not properly understood. We have seen many problems with related system implementations causing significant operational and customer-facing issues.

The root causes are several and interlinked. To start, many companies in the sector have an increasingly complex footprint. International oil and gas companies, for example, can have more than 10,000 applications in production. Companies find it increasingly difficult to manage this footprint with sufficiently high standards that provide the needed continuity of performance, security and availability.

Energy and natural resources (cont'd)

Then there's speed to market. Energy and natural resources companies rush to put processes in place whether driven by market opportunity, investor expectations or a desire to outrun competitors. Power and natural gas utility companies think hard about regulations when changing their services. And yet few invest in consolidated packages that offer both business operations and regulatory compliance. Instead they are layering or bolting on to legacy systems to support compliance obligations and business needs.

But the biggest future problem lies elsewhere. Many energy and natural resources companies are seen to struggle in viewing IT as a centre for innovation and growth. Instead IT continues to be seen much as a tool for running the business. This may have been acceptable in the past but it will not work in the future.

Consequently, the biggest risk that energy and natural resources companies will face comes from unexpected competition. In power, smart meters are penetrating, and other new engineering and information technology solutions are lining up. These innovations have the potential to quickly make current business models uncompetitive. This could be as simple as a technology transfer from another sector – something which connects with customers in a new way, or which integrates and automates supply and industrial processing capabilities like never before. These can and will completely change the digital landscape. For this reason we think existing energy and natural resources companies will need to design IT processes, solutions and partnerships that are agile and fit for the future to help them compete.

Energy and natural resources companies must also take a broader and deeper view of IT. KPMG member firms' experience shows that when energy and natural resource leadership and boards consider technology risk, they tend to focus on security. Even then we believe that they are not diving as deeply into security as they should. Organisations are often surprised by the findings when they perform a thorough review of their IT risks, including not only security architecture but also IT service performance and quality, change execution effectiveness, IT third party management, and return on investment in IT programs, to name a few.

For these reasons KPMG member firms encourage energy and natural resources companies to consider "value bundles" as an approach to better understanding and setting risk appetite for IT. These value bundles include continuity of IT service management, IT solution development and innovation, secure access and reliable user experience, sound IT investment portfolio management, and knowledge and collaboration management among others. By considering IT in the context of these bundles, rather than focusing only on individual or aggregated risks, energy and natural resources companies not only mitigate the priority risks but also better optimise IT value and delivery.

There is technology risk in everything this sector does, being so heavily dependent on engineering and information technology for handling the business of some of the world's most prized commodities. A company strategy for managing this risk should be integrated in all it does, making technology risk management part of the fabric of IT, business stakeholder and board-level guidance. In achieving this mode of operation, energy and natural resources companies can better anticipate and manage the diverse technology risks the industry faces, now and just around the corner.

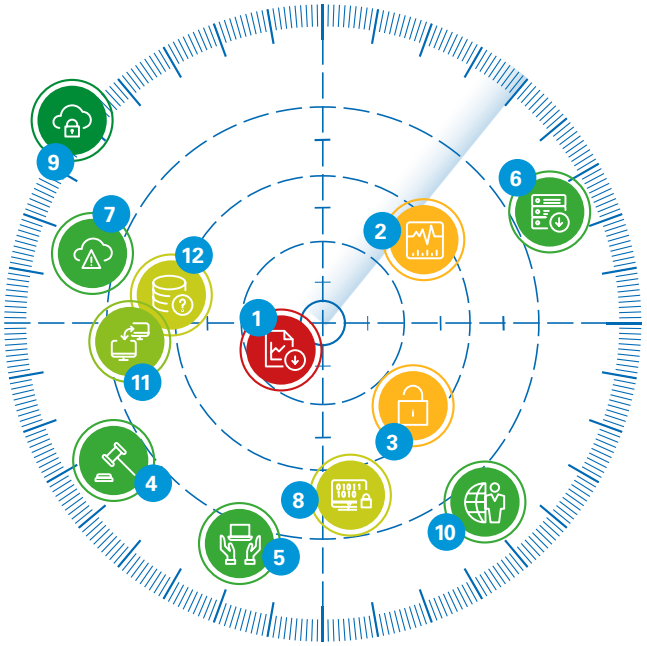
> "Many companies in this sector have an increasingly complex footprint. International oil and gas companies, for example, can have more than 10,000 applications in production. Companies find it increasingly difficult to manage this footprint with sufficiently high standards that provide the needed continuity of performance, security and availability."

Industrial manufacturing

Marcelina Valdez

Beth McKenny

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability



Industrial manufacturers are adept at managing many risks. But we think some of their nets might not be fully aligned with where the technology-related risks lie. This is because they see certain risks as not having a technology cause when in fact they do. Not correctly identifying the root cause is a huge problem – and something that we think could be disastrous for many in this sector.

Old and degraded software is one issue. Having multiple interfaces between multiple systems is another. There are many data sources within the product environment and much data interfaces with other data in many different ways. But not enough effort is put into maintaining this data, these aging systems and these interfaces.

Quite simply, too many industrial manufacturing systems are outdated. Continuing to use these aging complex systems carries major security and operational risks – from the potential for cyber-crime to loss of service.

Moving to new systems does too. Newer industrial manufacturing processes are increasingly digitised and make greater use of robotics and sensors, and growing connectivity. The technology- risks related to these innovations have not really made the headlines – to date. But they will do. And industrials need to make sure they are on their risk radar.

Security has not been seen as as big a risk in industrial manufacturing as it has in other sectors such as health or finance. It can no longer afford to be under estimated, as industrial espionage is on the rise. We see technology as both the cause and the fuel to its growth. As new types of technology are embedded into both operations and the finished product, industrials have more to lose if their secrets are stolen. Failing to protect their products and processes risks operations coming to a standstill or having valuable IP used by a competitor.

Industrial manufacturing (cont'd)

At the same time companies need to manage their partnerships carefully. When systems are connected there needs to be a clear understanding of what can pass across any interface, and a strict segregation of anything not to be shared. Data ownership can be a tricky issue here if the data passes through different systems.

Then there's the Internet of things. The future lies in products with ever increasing technology embedded in them and greater connectivity. Traditional manufacturers now have to consider issues such as data security and integrity – things that have not been an issue to date.

The good news is that some companies are starting to respond to this changing environment. In the past they limited their IT risk concerns to office and corporate systems. Now they are starting to perform risk assessments over all their systems, applying similar risk mitigation to their industrial manufacturing and their product systems as they do to their back-office and customer-facing functions.

How can other companies go about this process? They need to start by embedding governance and risk management within the product development cycle and integrating these factors within the start-to-end product processes. They need to make sure they build the risk management in right from the development stage rather than trying to bolt it on later.

This is starting to happen in consumer product industries. But we believe that it needs to be more widespread. Industrials need to focus on all their IT-related risks by having a fully comprehensive IT risk programme. Once this is in place, companies need to appoint someone senior to think about the technology risks that are specific to that organisation. This person needs to ask: How does IT risk drive each and every decision we make? This involves understanding the company's key assets and main business drivers, seeing how technology affects these, determining the appetite around the different risks, and then investing strategically to mitigate them.

Industrial manufacturing is becoming more technology-oriented, and the technology used by manufacturers and their products is evolving. Technology risk has gone beyond finance and organisational matters and now sits at the heart of products and production. Some companies have been slow to acknowledge this. But they need to catch up with the sector's leaders in embedding technology risk considerations into all of their operations – extending their technology risk radar to everything that they touch and do.

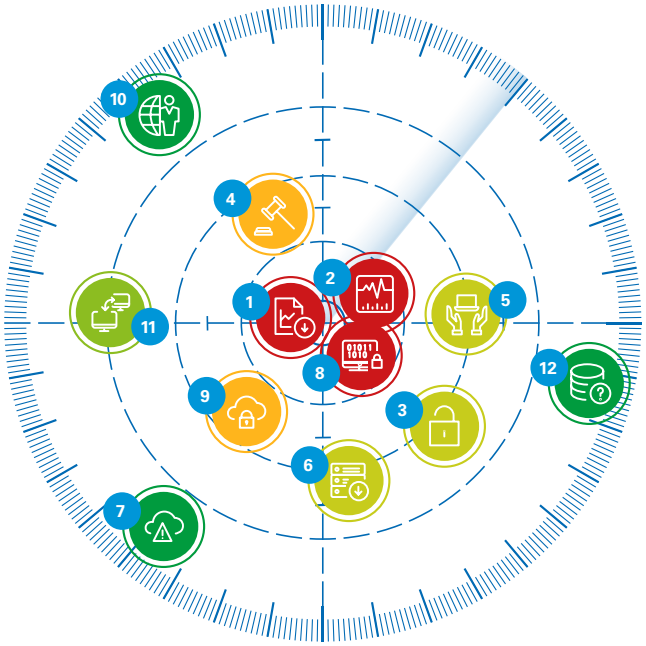
> "Newer industrial manufacturing processes are increasingly digitised and make greater use of robotics and sensors, and growing connectivity. The technology- risks related to these innovations have not really made the headlines – to date. But they will do. And industrials need to make sure they are on their risk radar."

Central government

Andy North

Geoffrey Weber

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability



The relationship between government and citizens is changing. Governments all over the world are transforming the way they provide services, using the opportunities offered by new technology to improve stakeholder engagement, reduce cost and improve efficiencies. Governments are viewed as slower than the commercial world to adapt to digital and apps. But they are now starting to embrace this new world.

We believe that their greatest challenge is their own privacy rules combined with a lack of public confidence in their ability to keep data safe. These prevent them from sharing data effectively and restrict what they can achieve with the vast pools of data they collect. We believe that governments must break down certain barriers to enable them to use some information for the benefit of the public while balancing this with managing privacy issues and the rights of the individual.

Legacy systems are a global problem. The associated risk with managing and delivering services with legacy systems is enormous. Only if these old systems continue to operate can governments provide fundamental public services. The growing number of availability incidents in the survey is worrying and we believe that this reflects a lack of investment and strategy to ensure unbroken service delivery.

Another major risk comes from working with third-party suppliers. As the public sector begins to increase outsourcing of its IT service development and delivery, a number of large private sector organisations are building up a lot of power over public sector systems. These private firms often know more than the departments for which they are working about how those department's systems function. Already there is a huge risk that individual government departments are unable to manage their own systems internally and are bound to the support from external private sector organisations.

Central government (cont'd)

And we think that this risk will only increase as new services develop and even more of the associated development is outsourced.

This links to a fourth major risk: project delivery. The public sector typically has a poor reputation for delivering projects well, on time, within budget and to meet its objectives. Projects are usually large and complex change programmes, coming from a legacy position and often with many tens of systems being replaced by just a few. This complexity and the fear of getting it wrong results in a vicious spiral, with poor history creating a lack of confidence for new investment.

And yet governments could get around this. What's needed is a proactive method for managing the risks upfront: asking the difficult questions and planning properly around the answers. Success hinges on carrying out an independent risk assessment of major programmes, with assurance from the start and revisiting this continuously throughout major change programmes.

Too often the focus is only on cyber risk and security, with no broader view. The risks mentioned above are often simply not on the risk radar at all. Individuals in large government departments are usually responsible for managing their own risk portfolios: integration is overlooked. We believe that this is the biggest risk of the lot, given the complexity of the systems landscape.

What can be done about this? We think boards need to step up to the challenge. They have to take a step back and consider technology risk as part of the big picture of their operations. They need to ask what the critical services they are providing are, and what big risks might affect those services. These might be processing, or availability, or security – they will vary.

But only by understanding the risks involved and drawing up a broad-ranging risk register of all risks, both tech and non-tech, based on services (rather than department) can government see the extent of these risks and assess whether they are being properly mitigated.

Bringing attention back to services rather than departments makes the risk assessment and mitigation process more relevant, effective and efficient. It allows a greater chance for all risks – not just cyber – to be part of the equation. And it enables governments to better protect what they need to do: delivering critical public services competently and in a cost-effective manner.

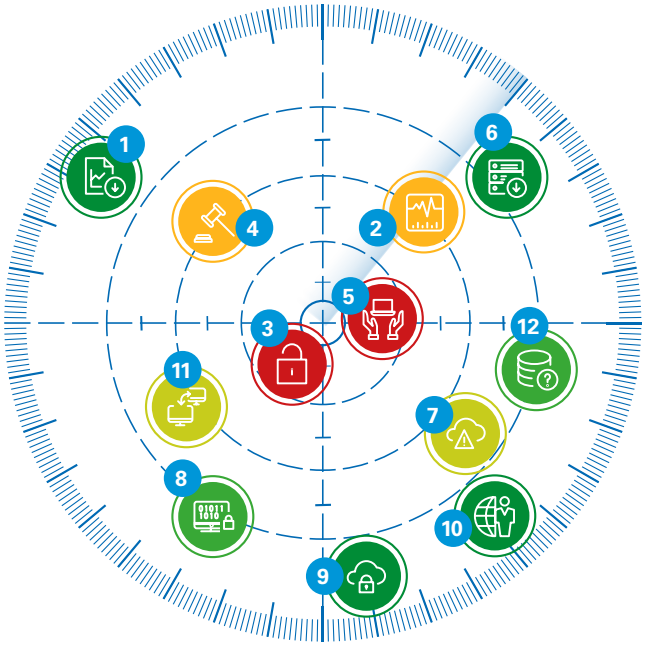
"Boards need to take a step back and consider technology risk as part of the big picture of their operations. They need to ask what the critical services they are providing are, and what big risks might affect those services. These might be processing, or availability, or security – they will vary."

Education

Richard Archer

Hannah Cool

1. Poor risk management alignment across organisation and process
2. Dependence on inflexible and under supported legacy systems
3. Poor cyber security, cyber-crime and unauthorised access
4. Non-compliance with regulation and legislation, e.g. privacy
5. Lack of IT strategy and lack of board representation
6. Inadequate data quality and lack of capability to leverage data to manage risk
7. Inability to deploy and exploit emerging technology
8. Failure to deliver programmes and to build in control, resilience and security
9. Reliance on, and poor security and control in, vendors/third parties
10. Ineffective service management and delivery
11. Ineffective IT asset management
12. Inadequate resilience and disaster recovery capability



Universities start the technology risk challenge in a poor position. Historically they have had relatively open systems with a distinct lack of internal controls.

And yet they have a great deal to protect. The vast research revenue they receive reflects the high value of the intellectual property on their systems. All universities have sensitive staff and student data on their systems. And universities, particularly in the US, which are affiliated to hospital chains carry valuable healthcare information, making their records a tempting target.

Then there's the risk around facilities. Students are becoming increasingly demanding, expecting access to cutting-edge technologies and the most flexible education delivery options. To be competitive, universities have to meet these services and install expensive IT infrastructure. Huge risks come with implementing and managing these new facilities, equipment and processes.

Legacy systems are a recognised problem across the sector, as is the poor integration between different back office functions. Less acknowledged, though, is the lack of skills in universities' internal IT capabilities. They often cannot match the salaries offered to IT professionals in non-tertiary environments. While businesses appreciate how they can use big data for market analysis, universities have been slower in appreciating the value to be unlocked from the data they hold, meaning they have not prioritised data analytics capabilities.

The decentralised nature of most tertiary bodies does not help. Compare them with financial services firms, which operate from a central core from which decisions flow. The historically open networks with lack of central controls are an open invitation to organised crime. They are also the reason for the increase in security breaches – breaches which are becoming ever more targeted. Examples range from trying to

Education (cont'd)

infiltrate nuclear research databases to students hacking the administration office to change their results.

Universities work through management by consensus. The challenge for them is to bring all the departments, schools and institutes that comprise the university together to agree a centralised technology approach: a common hardening of servers, a common offering of encrypted laptops. This includes ensuring access control and policy is properly enforced: too often universities are not using controls such as multi-factor authorisation.

Without this joint approach it can be next to impossible to have systematic asset management. IT is often bought and managed by individual departments. There is no formal process for assessing what data is held on university devices – never mind the individual mobile devices that students bring onto campus, or what happens to university devices when they are no longer needed.

The root cause for all these problems is lack of investment. There are so many other areas which need cash – from faculty buildings and student facilities to professors and teaching staff – that technology is often low down the spending priority list.

We believe that not enough university leaders have taken the issues of cyber security, centralised management and processes seriously enough – despite the high value of the data and intellectual property they hold.

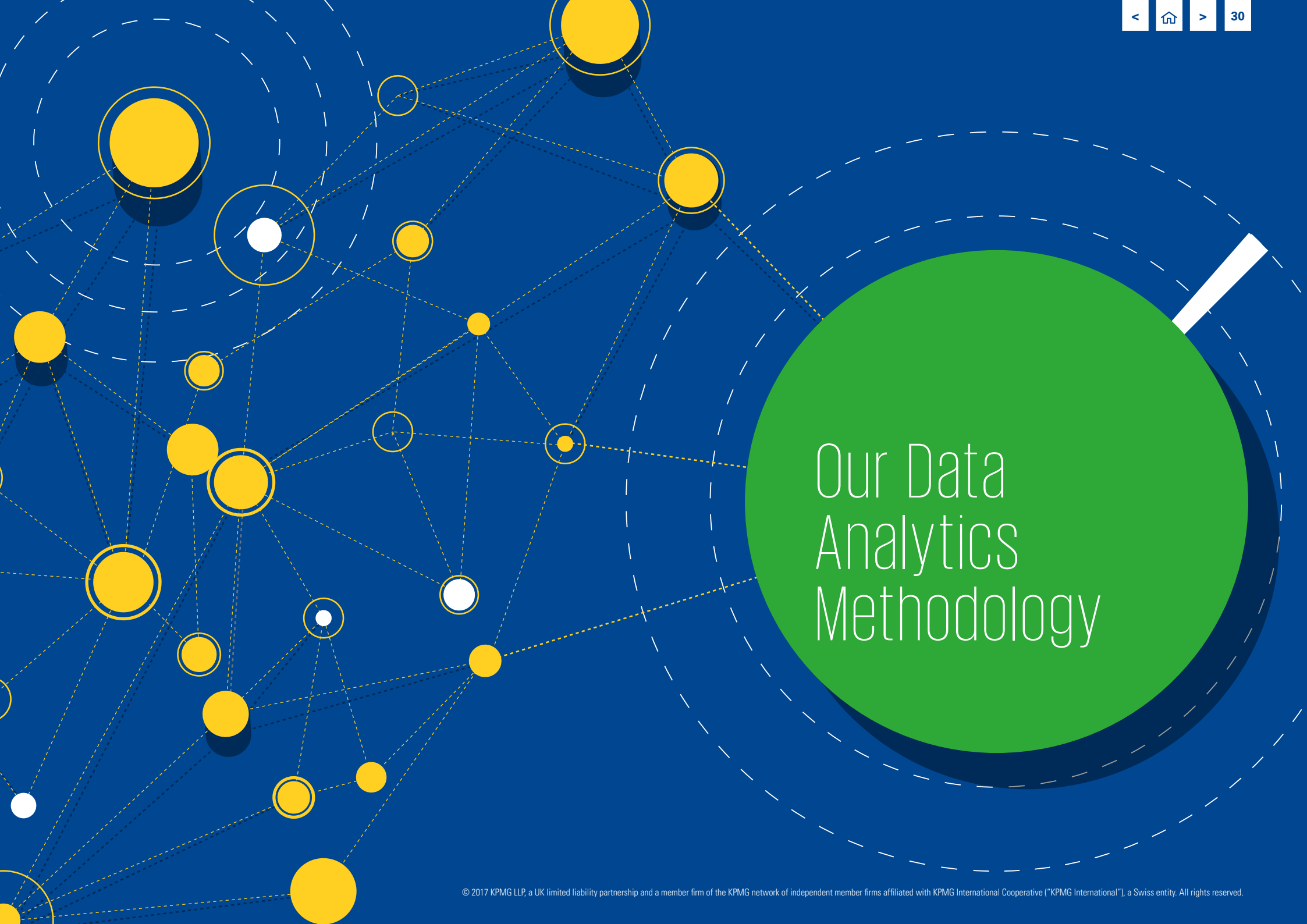
KPMG professionals are encouraged by the shift in awareness and focus we have seen this year. Sadly this increased attention is due to the sheer number of security-related incidents. More university boards than ever have asked us to review their cyber security. And they are shocked by the number of red flags KPMG member firms are raising.

The next step is for them to implement effective practices and policies for their critical data, assets and infrastructure. Many do not yet seem ready for this. But the findings of KPMG member firms risk assessments are pushing them into action. They know that they need to agree on what has to be done, and to sell the idea to their staff responsible for implementation. Ownership at middle-management level is crucial. But it has to be driven by ownership at the top. Boards need to have a member who is assigned to be responsible for information security. This is the first and most crucial step, and one that many universities still have to take.

Our hope is that the scale and magnitude of security incidents will become a springboard for higher education to acknowledge the risks, to form a plan of action, to commit to the investment needed, and to put the processes and people in place to make this happen.

We believe most universities are at a crossroads. Either they will take the challenge or they will flounder. The key for many will be finding a balance between the openness that students value and the protection that the institutions need – establishing critical assets, processes and data, and concentrating on protecting these.

> "Universities, which are affiliated to hospital chains carry valuable healthcare information, making their records a tempting target. Students are becoming increasingly demanding, expecting access to cutting-edge technologies and the most flexible education delivery options. Universities have to meet these services and install expensive IT infrastructure. Huge risks come with implementing and managing these new facilities, equipment and processes."



Our Data Analytics Methodology

Media-reported events: data analytics

How KPMG professionals obtained and analysed the incident related data used in Section 1.

Search methodology

We used KPMG's Astrus infrastructure to scan the internet for publicly available English news articles related to IT incidents the globe across ten different industries.

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. Around 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 actual IT risk incidents that occurred rather than potential threats.
- The result set included incidents that happened during the time period specified above 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, only one of the articles was included in the analysis.

Over 700 relevant IT incidents were included as part of the final result set. Based on a taxonomy defined by member firms IT risk professionals, the incidents were examined and the following attributes were determined:

- What happened?
- What were the causes?
- Affected companies and industries
- What was the impact? (e.g. number of user accounts affected, etc.)

The resulting analysis was presented to KPMG member firms technology risk specialists to draw conclusions, which have been presented in this report.

Contact us

Contact us

Richard Archer
Principal
KPMG in the US

Annie Armstrong
Principal
KPMG in the US

Nathan Cain
Partner
KPMG in the UK

Hannah Cool
Manager
KPMG in the UK

Nicolina Demain
Senior Manager
KPMG in the UK

David DiCristofaro
Partner
KPMG in the US

Jon Dowie
Partner
KPMG in the UK

David Eastwood
Partner
KPMG in the UK

Jill Farrington
Partner
KPMG in the US

Joshua Galvan
Principal
KPMG in the US

Paul Holland
Director
KPMG in the UK

Michael Isensee
Partner
KPMG in the US

John Machin
Partner
KPMG in the UK

Beth McKenney
Managing Director
KPMG in the US

Priya Mouli
Manager
KPMG in the US

Kiran Nagarai
Managing Director KPMG in the US

Andy North
Director
KPMG in the UK

Paul O'Sullivan
Senior Manager
KPMG in the UK

Caroline Rivett
Director
KPMG in the UK

Ameet Sharma
Director
KPMG in the UK

Andrew Shefford
Managing Director
KPMG in the UK

Jamie Thompson
Director
KPMG in the UK

Marcelina Valdez
Senior Manager
KPMG in the US

Geoffrey Weber
Principal
KPMG in the US

kpmg.com/uk

CREATE | CRT075248 | January 2017