The Economist Intelligence Unit

A report from The Economist Intelligence Unit

INFORMATION RISK

Managing digital assets in a new technology landscape

SPONSORED BY:

hp

Contents

About the report

Information risk: Managing digital assets in a new technology landscape is an Economist Intelligence Unit report, sponsored by HP. It is intended to explore how organisations view and approach information risk and its management in the era of "big data" and cloud computing.

This report draws on two main sources for its research and findings:

- In August 2013 The Economist Intelligence Unit surveyed 341 senior business leaders, 41% of whom are C-level executives or board members. Those in general management make up the largest group of respondents but at least one-quarter have responsibility for either finance, IT, risk or strategy and business development. Respondents come from across the world, with 31% based in Europe, 27% in North America and 33% in Asia-Pacific, and the remaining 9% from the Middle East and Africa. A total of 18 industries are represented in the survey. Just over half of respondents come from the following four industries: financial services; manufacturing; professional services; and IT and technology. The sample represents organisations of various sizes: 42% have annual revenue of more than US$1bn.

- Alongside the survey The Economist Intelligence Unit conducted a series of in-depth interviews with the following senior executives and experts (listed alphabetically by organisation):

  - Jim Routh, chief information security officer, Aetna
  - Chris Sutherland, chief information security officer, USA, BMO Financial Group
  - Micky Lo, head of information risk management, APAC, BNY Mellon
  - Massimo Russo, partner, Boston Consulting Group
  - David Sherry, chief information security officer, Brown University
  - Kamlesh Bajaj, chief executive officer, Data Security Council of India
  - Paul van Kessel, global IT risk and assurance leader, EY
  - Denise Wood, chief information security officer, FedEx
  - Amar Singh, chief information security officer, a FTSE 100 company
  - Mark Jones, director, information technology security, compliance and governance, Heathrow Airport Holdings
  - Steve Durbin, global vice-president, Information Security Forum
  - Gram Ludlow, information security professional
  - Malcolm Marshall, head of information protection and business resilience, KPMG
  - Marcus Alldrick, chief information security officer, Lloyd's of London
  - Choy Peng Wu, group chief information officer, SingTel
  - Phil Cracknell, chief information security officer, UK, TNT Express
  - Stefan Fenz, researcher, Vienna University of Technology

The report was written by Clint Witchalls and edited by James Chambers. We would like to thank all interviewees and survey respondents for their time and insight.

Executive summary

Companies are now generating, collecting and analysing unprecedented amounts of information. The strategic importance of this information across the business, from top-level strategy and decision-making to product development right through to sales and marketing, means it needs to be available to the right people at the right time in the right form.

The perceived value of this information has never been higher. In a survey of global executives conducted by The Economist Intelligence Unit, nearly one in three respondents estimates the value of information held by their organisation to be between 10% and 50% of total assets.

But just as technology has transformed information into a valuable business asset, outsourcing, cloud computing, social media, "bring your own device" and other technology-enabled business trends mean that information is increasingly being dispersed across the globe. This has increased its appeal and accessibility to competitors and attackers, as well as making it more vulnerable to careless employees.

The combination of this elevated risk landscape and a growing appreciation of the value of information is causing businesses across the world to recognise information as another corporate risk to be managed. This report looks at the approaches that companies are taking to managing this risk. The key insights in this report are based on a global survey of 341 senior executives and 17 in-depth interviews.

Key findings from the report include:

Information is now big, borderless and beyond the control of individual companies. Technology developments like cloud computing are perceived to have increased the risks to information. Greater collaboration and data sharing with other companies, through the likes of open innovation, supply chain integration and outsourcing, is elevating risk even more. As these trends create "borderless" information beyond the control of the individual company, addressing and governing the future risks will involve closer collaboration, involving businesses as well as governments.

Risks to information are on the management agenda, but cyber-attacks dominate attention. High profile cyber-attacks have placed information risk on the boardroom agenda. Now the biggest barrier to raising the priority of information risk is a lack of understanding of the issues. More than three-quarters of respondents believe that information risk can largely be mitigated by technology fixes to hardware and software. Yet the focus on cyber-attacks and

technology fixes threatens to overshadow the central role that employees play in mitigating—and creating—risk.

Placing a monetary value on information is a tricky but growing practice. Only one in ten companies have assigned a monetary amount to all types of information they hold, but the trend is moving in this direction. Half of all companies are either putting a monetary value on some information or actively considering doing so. This can be difficult to implement. Patents, copyright and industrial design are the types of information most likely to be assigned a monetary value, even though executives believe most mission-critical information resides in the finance department.

Awareness of information risk does not extend across the business. Most companies are failing to create a culture of awareness. Only one in four companies (27%) report an extensive awareness of information risk across the organisation. The most knowledgeable departments are IT and finance, where the most critical information is thought to reside. This low level of awareness across the company is equally true vertically: the importance of protecting information has not filtered down to lower levels of the organisation, according to the majority (57%) of respondents.

Education is important in order to feel prepared, but it is not commonplace at senior level. Senior business leaders are generally ill-prepared for a loss of information at their company: fewer than one in four respondents (23%) would know enough to take the lead in the event of a breach, despite nearly half of organisations experiencing a loss of information in the past two years. Training increases the perception of preparedness, but in the past year over half (57%) of CEOs have not been trained on what to do after information has been lost or stolen.

Government efforts to advance collaboration and knowledge sharing are encouraged. The majority (62%) of respondents to our survey are looking to governments and regulators to take a greater lead in information risk management, particularly efforts to encourage knowledge sharing between companies about cyber-attacks. A co-operative approach is supported here, not simply new legislation. An even larger proportion (68%) of respondents would welcome greater regional harmonisation of the rules surrounding data security.

Promoting information risk management

The following have emerged from our research as steps practitioners can take to advance the practice of information risk management in their organisations:

Capitalise on high-profile cyber-attacks: Use board-level attention of prominent cyber-attacks on other companies to win support for a comprehensive, company-wide view of information risk

Break out of the IT silo: Move beyond the view of information risk as an IT problem. Technology is only a part of effective information risk management

Get closer to the business: Understand how information is used by the business and include business units in working out what information is most critical to the organisation

Turn risk management into a reflex: The need for education at all levels of the organisation is pressing. Regular training should be tailored to the audience and avoid tick-box exercises

Develop a robust policy for deleting data: Employee carelessness is a perennial risk for companies so the less information that has a chance of getting lost or stolen the better (and cheaper)

Secure the supply chain: Business trends like outsourcing require more third-party organisations to get access to secure networks; less attentive partners can be a "back door" into your organisation

Share knowledge with competitors: Break the code of silence around cyber-attacks. Take the lead in sharing information with peers rather than waiting for government encouragement—or enactment

Press refresh: Data is expanding, technology is developing and attacks are evolving, so the most valuable information should be periodically updated and the risks to it regularly assessed

Introduction

> “We no longer control a network perimeter over which we can throw a safe blanket and say that everything within the network is now safe and contained.”
>
> *Steve Durbin, global vice president, Information Security Forum*

“Information is the new oil” is a common refrain among businesspeople nowadays. The description goes far beyond world famous proprietary information like the recipe for Coca-Cola or Google’s search algorithm. This new oil is increasingly being extracted from “big data”—the petabytes of data being collected by companies from the connected universe, a lot of it about consumer habits.

Marketers can now identify spending patterns through loyalty cards and use that information to cross-sell other products; developers can mine social media to find out what their customers think of a new service; as more products are being embedded with sensors as part of the so-called Internet of Things, companies will have greater insights into how their products are used. This information can be fed into building better products and services or even into the development of new business models.

A global survey of senior executives, conducted by The Economist Intelligence Unit and sponsored by HP, found that information in all its forms is a significant part of most organisations’ assets. Close to one in three survey respondents estimate the value of the information their organisation holds to be between 10% and 50% of total assets; about one in ten respondents estimate this to be greater than half of total assets.

Just as the valuation of these assets is going up, likewise the risks to this information are increasing. All of the information security professionals interviewed for this report agree that information risks have grown significantly in the past few years, driven by the business and technology trends we will explore in the following chapter, which have pushed information beyond the control of individual companies. If ever the guardians of an organisation’s information assets had their work cut out for them, now is surely the time.

“We operate now in a completely cyber-enabled environment: we are always on, we are always connected, and we are highly mobile,” says Steve Durbin, the global vice-president of the Information Security Forum, a not-for-profit organisation. “We no longer control a network perimeter over which we can throw a safe blanket and say that everything within the network is now safe and contained.”

Nearly one-half of the firms represented in the survey have suffered information loss in the past two years. This ranges from a low of 43% in North America to a high of 54% in Asia-Pacific. The majority of these incidents are considered to be minor or of no determinable value, but the organisational damage is not always easy to quantify. Often the damage is primarily reputational.

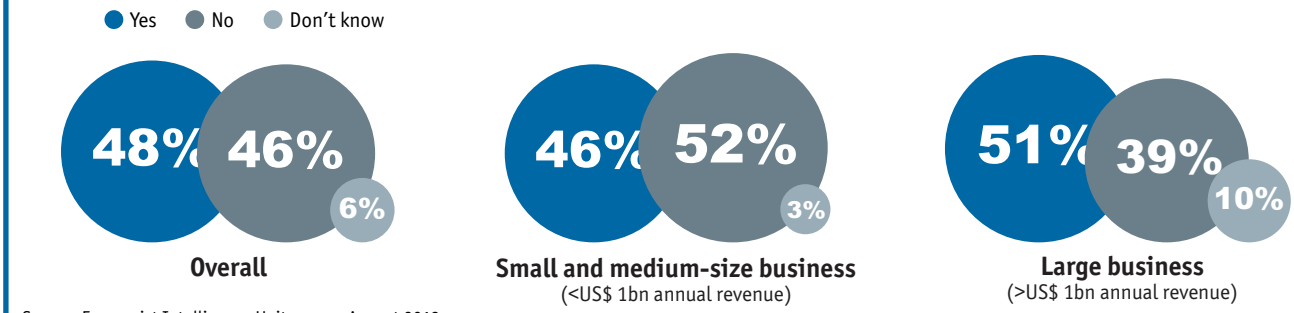
To limit reputational damage, managers are reluctant to discuss data breaches at their firms. Accordingly, most losses or breaches go unreported. Even so, media coverage of some very large cyber-heists has been pushing information risks higher up the corporate agenda, particularly in the banking sector: earlier this year hackers managed to steal US$45m from the Bank of Muscat in Oman and the National Bank of Ras Al Khaimah (RAKBANK) in the UAE.

Still, data theft is only one part of the risk equation. Increased focus on cyber-attacks is drawing attention away from the other, less spoken about, side of information risk: data integrity. The risk of making business decisions based on poor quality, outdated or even incorrect data can be as damaging as a data breach.

The final act for information is deletion: with fewer than half the firms in the survey being strict about deleting data, many are exposed to unnecessary criminal, legal and regulatory risks, not to mention the costs of storing increasingly large amounts of data.

Chart 1: Easy targets

Q **Has your organisation experienced an information loss in the past two years?**
(% of respondents)



Source: Economist Intelligence Unit survey, August 2013.

1 Managing a riskier landscape

The two most common risks to company information are generally considered to be employee carelessness, such as losing a company laptop or using an unapproved device on the corporate network, followed by hacking or some other criminal theft of information for financial gain. Other risks related to people or technology similarly feature high on the list, including disgruntled employees maliciously destroying or leaking sensitive information, employees leaving the company and taking confidential knowledge or information with them, and technology failure.

Many of the risks to information are not new, yet the same technology developments that are viewed as good for business productivity have increased the likelihood of these risks being realised: "big data", cloud computing and "bring your own device" are three of the top five business trends heightening the risks to information, according to our survey respondents. Organisations now have to deal with a wide variety of risk-laden information channels, such as the remote worker connecting to the office through a virtual private network; a disgruntled employee airing grievances on social media; or a sales person using a personal smartphone to take down the details of an order.

By "triangulating" data from various sources—especially online sources—cyber-criminals can use this information to gain further information through social engineering (tricking people into divulging confidential information) or they can use it for an attack on an individual, as occurs in spear-phishing (sending a targeted e-mail to an individual from a seemingly legitimate source). However, high-profile cyber-attacks are only one of the risks to company information.

Senior managers and information professionals now have to consider the governance of data that it may use in the business but not own or generate itself; for instance, the privacy issues surrounding the use of social media data by the sales and marketing function to "cross-sell" and "up-sell" to their customers. "Big data may result in increased risks of data mismanagement in the areas of data quality, privacy and storage as an organisation's data governance framework may not cater to this," warns Choy Peng Wu, the group chief information officer at SingTel, a telecommunications service provider.

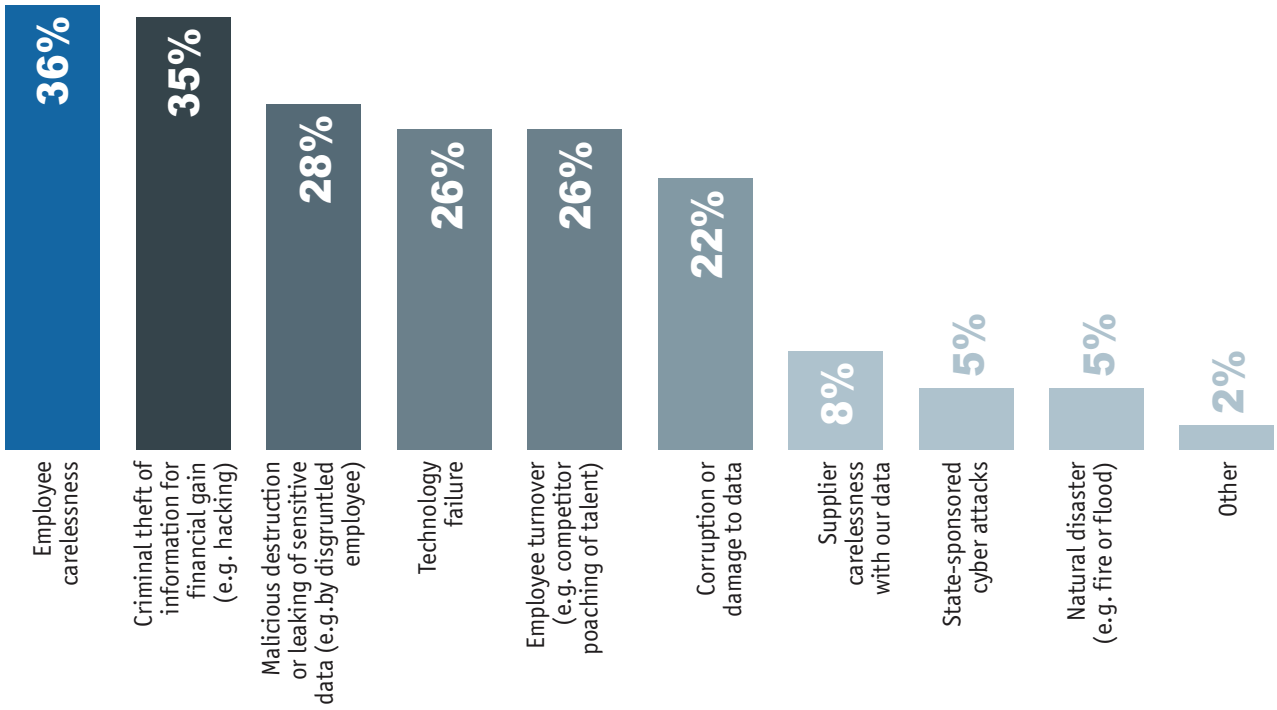
Cloudy computing

With burgeoning volumes of data to manage, businesses are increasingly pushing the storage of some or all of this information from on-site data servers to external providers, operating in "the cloud". Some newer business are going straight to cloud storage, eliminating the need for up-front capital expenditure and making use of the cloud's scalability and flexibility to support growth. The involvement of external providers in the storage and control of information unsurprisingly introduces new risk trade-offs for companies to consider.

According to Gram Ludlow, an information risk expert, cloud storage can be a boon for organisations with immature or underfunded data security. "With a strong legal agreement in place, the level of security at most large cloud

Chart 2: Risky business

What are the sources of risk to your organisation's information?
(% of all respondents)



Top three risks by region

North America
1. Criminal theft of information for financial gain
2. Employee carelessness
3. Corruption or damage to data

Asia-Pacific
1. Employee carelessness
2. Criminal theft of information for financial gain
3. Malicious destruction or leaking of sensitive data

EMEA
1. Employee carelessness
2. Criminal theft of information for financial gain
3. Employee turnover

Top three risks by job title or function (selected)

CEOs
1. Technology failure
2. Employee carelessness
3. Employee turnover

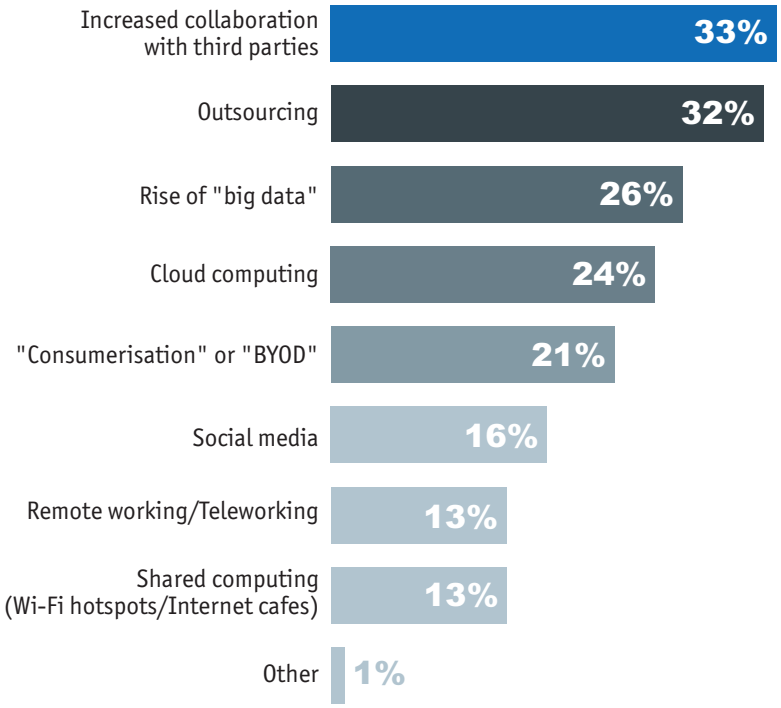
Risk function
1. Criminal theft of information for financial gain
2. Malicious destruction or leaking of sensitive data
3. Technology failure

IT function
1. Criminal theft of information for financial gain
2. Malicious destruction or leaking of sensitive data
3. Employee carelessness

Source: Economist Intelligence Unit survey, August 2013.

Chart 3: Shared drive

What business or technology trends are increasing the risk to your organisation's information?
(% of all respondents)



Source: Economist Intelligence Unit survey, August 2013.

providers can be much higher than the average company," says Mr Ludlow. "The weakness that has to be balanced against that is you may be moving your information to a higher profile target and increasing your threat profile."

Mr Ludlow gives a hypothetical example of a manufacturing company that has weak controls to protect its information, but equally is not on any cyber-criminal's radar because it does not process a lot of credit-card transactions. "But then the firm moves their data to a major cloud provider and becomes a target because that provider is being attacked fairly regularly," says Mr Ludlow.

Even if firms are selective about providers or eschew the cloud altogether, employees or other stakeholders may be less security-conscious. This is a particular concern for David Sherry, the chief information security officer at Brown University in the US. In terms of information risk, Mr Sherry says that the cloud has made Brown University a bigger target. His concern is the free-to-use services aimed at the consumer market. If a researcher uses a note-taking app to store information about intellectual property that Brown is developing, just how secure is that data, he asks.

Out of control

But it is not just technology that has created a perimeter-less organisation. The two trends most likely to increase risks to an organisation are increased collaboration with third parties and outsourcing. Each time a company outsources a business function, develops a more integrated supply chain or pursues open innovation (where new ideas are researched in partnership), it is allowing a third party to connect to its internal systems and expanding access to its data. "If you look at something like a research process in a pharmaceuticals company, the number of different organisations involved in handling that data is now immense, so the governance goes beyond the organisation itself and goes into the supply chain as well," says Malcolm Marshall, the head of information protection and business resilience at KPMG, a professional services firm.

As collaboration between businesses grows, the vast majority of companies are taking a pragmatic and realistic approach to information loss. To a certain extent, it has become an accepted risk of doing business. Only one in five respondents (20%) say that their firm would not do business with an organisation that had suffered a serious data breach in the past year, whereas for two-thirds (66%) of respondents it would depend on the steps taken to prevent a future breach. Even so, the information risks that companies are exposed to here can stretch beyond losing information.

Massimo Russo, a partner at Boston Consulting Group, says that some of his clients are worried about open innovation tools and their impact

on product liability risk. "If an engineer posts a problem on an open innovation website that says he's having a problem with an anti-lock brake system and is looking for a solution—that could be discovered in the future," says Mr Russo. "Once it goes outside of the enterprise and it's in these open collaboration networks, it could potentially be used in a product liability law suit against the company at a future date. Quite frankly, some of the legal boundaries that are driven by geography no longer apply when it comes to digital information."

Terror-bite: Small companies come under attack

Smaller businesses are traditionally considered to be less of a target for cyber-attacks and consequently less prepared for these threats. During a study of Austrian organisations, Stefan Fenz, a researcher at the Vienna University of Technology, found that size of a business is much more of a useful indicator of preparedness levels than industry or sector.

Certain characteristics may, however, mean that smaller companies become more of a risk, including operating in a highly specialised area or being a key supplier to a larger organisation—acting as a kind of "back door". What is more, any complacency here about the levels of the risk could be misguided (see Chart 1). "What you're seeing now is the attackers going down the supply chain because SMEs are an easier target," says Marcus Alldrick, the chief information security officer (CISO) at Lloyd's of London, a marketplace for insurance.

Smaller businesses currently report much lower levels of awareness about information risk across the organisation than larger businesses. Yet there are solid business reasons to support the adoption of a more mature approach to information risk. For one thing, it can facilitate, or at least act as a prerequisite for, entry into supply chains with bigger customers—a commercial justification for allocating limited resources to this area. In extreme cases, it can also be a matter of business survival.

Early in 2013 Efficient Services Escrow Group, a California-based provider of escrow services, was put out of business following a US$1.5m cyber-heist.[1] The attack began in December 2012, when a fraudulent wire transfer diverted US$400,000 to a bank in Moscow. The remaining US$1.1m was diverted to banks in Heilongjiang Province in China. Although the money wired to Moscow was recovered, Efficient Services was unable to recover the money remitted to China and, as a result, was forced out of business.

There are signs, nonetheless, that small and medium-sized enterprises (SMEs) are taking information risk management more seriously—beginning with the allocation of more resources. Currently the CEO is much more likely to have responsibility for information risk management at smaller companies than at larger ones - this is the case at just over one in four (27%) SMEs and less than one in 20 (3%) at larger firms. But Gram Ludlow, an information security professional, says that there is a trend towards SMEs recruiting CISOs. "I'm seeing companies as small as a couple of thousand employees and under a billion annual revenue, hiring CISOs," says Mr Ludlow.

The impact of this, he says, is that over the next three to five years, the market for CISOs and other information risk management professionals is going to get very tight. However, he believes that the net outcome will be positive. "It's going to increase the pipeline for CISOs because now you will have people who have security leadership experience from smaller companies, and there are far more of them," says Mr Ludlow.

[1] http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/ [Accessed September 3rd 2013]

2 Setting the information risk parameters

For more than a decade banks and other firms in the financial services industry have been leading the way in recognising information as a risk to be managed. This has led some in the industry to rank it alongside credit risk and market risk in importance. Now experts like Malcolm Marshall, a partner at KPMG, see other industries catching up. Organisations in sectors as diverse as property and oil and gas are beginning to recognise information as another corporate risk to be managed, prompted by the perceived value of information and the elevated risks to it.

The level of seniority the topic demands internally is likewise on the increase, pushed up the corporate agenda by media attention of high-profile cyber-attacks and personal experience of cyber-crime. Mr Marshall even sees non-executive directors on the board paying attention to it these days. A potential concern here is that senior managers may have a tendency to focus on the latest cyber-attack or data breach. This could mean companies overlook or downplay other risks, as well as the evolving risk landscape.

"The perception is that hacking—somebody coming in from outside and getting company data—is still far and away the biggest risk that people think about," says Mr Marshall. "A small number of organisations are beginning to think more holistically: data and information underlines almost every risk they face and their ability to harness that information and manage it, or destroy it at the right time, is at the core of good risk management."

Chief information security officers (CISOs) and other information risk managers should seize the opportunity presented by this elevated board-level interest—along with any additional resources it brings—to shape the discussion at senior level and spread the importance of managing information risk across the business, all the while remaining wary of the pressures to focus on high-profile hacking incidents, which can lead to the disproportionate allocation of resources.

The starting point for many will be creating a comprehensive view of information risk across the business, as clearly there remains plenty of room to improve here. Only a minority (45%) of respondents to our survey believe that their company has a single view of information risk across the enterprise, falling to a low of only one in three CEOs (33%).

Controlled speed

The role of information risk management, in the first instance, is to identify the valuable information that an organisation holds, calculate the level of risk to that information, understand how such risks would affect the business, and on that basis prioritise certain information and risks. All of this should happen before the information security team is brought in to put the mitigation measures in place, in line with available resources.

As the value of information and the nature of risks evolve, managers should put in place rules, procedures and processes to monitor and control information and information risk across the organisation on an ongoing basis. In the era of big, borderless data, establishing these types

of governance procedures must now include the richly connected "ecosystem" of customers and suppliers.

"Information risk management is not something you do once, it is a living process," says Stefan Fenz, a researcher at the Vienna University of Technology. "You may do the big work only once, the inventory and the calculations, but then you have to rerun it yearly or half-yearly to see how the threat landscape has changed, as by then your assets may have a different importance to an attacker or yourself."

> "Information risk management is not something you do once, it is a living process."
>
> *Stefan Fenz, researcher, Vienna University of Technology*

Yet the purpose of identifying, assessing and prioritising information and risks should not be solely defensive, focused on protecting against information loss. Rather, the role of effective information risk management is to understand the risk appetite of the organisation and implement controls proportionate with it. The controls should be proportionate with the perceived value of the information to the organisation and with the organisation's need to use the information in the business.

This includes overcoming uncertainty about how certain data can be used, which can be more of a stumbling block than controls. For example, the marketing department may be wary of using certain information because they do not know if doing so would violate privacy laws. The information risk team's role is to dispel that uncertainty by advising on policy, regulations and laws and helping the business get the most from their data within those boundaries. "It is very rare for a security organisation to just say no," says Gram Ludlow. "As a profession, we are well beyond that. But there is still a lot of fear and uncertainty in the business."

Paul van Kessel, the head of global IT risk and assurance at EY, another professional services firm, likens effective information risk management to the brakes on a car. The common perception of breaks may be to slow down a car, but to Mr van Kessel having brakes on a car allows it to be driven faster. Others share his view. "It's about enabling, not restricting," says Mark Jones, director of information technology security, compliance and governance at Heathrow Airport Holdings. "We spend a lot of time at Heathrow doing just that: making sure that we're enabling the business to do things through good control rather than restricting them."

Still, there is considerable work to be done. In our survey, nearly two-thirds (62%) of respondents in the IT function believe that information risk management is making their company less agile.

Getting off the ground

Heathrow Airport Holdings, formerly British Airports Authority, runs four British airports, as well as Heathrow Express, the rail network between Heathrow Airport and Paddington station in London. When the company started designing and deploying new IT services on the Heathrow Express to enhance the customer experience, Mr Jones and his team were involved in the process, advising on potential risks and the security technologies to mitigate them.

"Information risk management teams need to be involved in the detail," says Mr Jones. "They need to know the particular information risks associated with each business investment that is made, and they need to give clear, prescriptive advice that balances protection of information assets with organisational agility."

Steve Durbin of the Information Security Forum has observed this closer integration with the business taking place at other organisations. "Some of the higher-profile CISOs and security people I am aware of today talk about not having a security strategy and not having a security budget; they talk about being aligned completely with the business strategy and about receiving funding from business projects," he says.

Yet if information risk management is to be truly aligned with the business there remains some work to be done. Currently over half (56%) of respondents say that all major business decisions

currently feature a discussion about information risk, but this is misleading. Nearly three-quarters (73%) of respondents in the IT function say this, but only 42% of CEOs state the same. This suggests that information risk teams are being left out of some of the most significant business decisions.

Breaking out of the IT silo

Before information risk management can move closer to the business in a meaningful way, certain views, responsibilities and approaches need to be overhauled—starting with the legacy role of the IT function, which at many organisations is firmly entrenched. There is a widespread belief in IT's effectiveness in tackling risks to information. Kamlesh Bajaj, the CEO of the Data Security Council of India, believes that 80-85% of information risk can be mitigated by "simple hygiene factors", such as updating operating systems, applying patches to software and keeping the anti-virus software up to date.

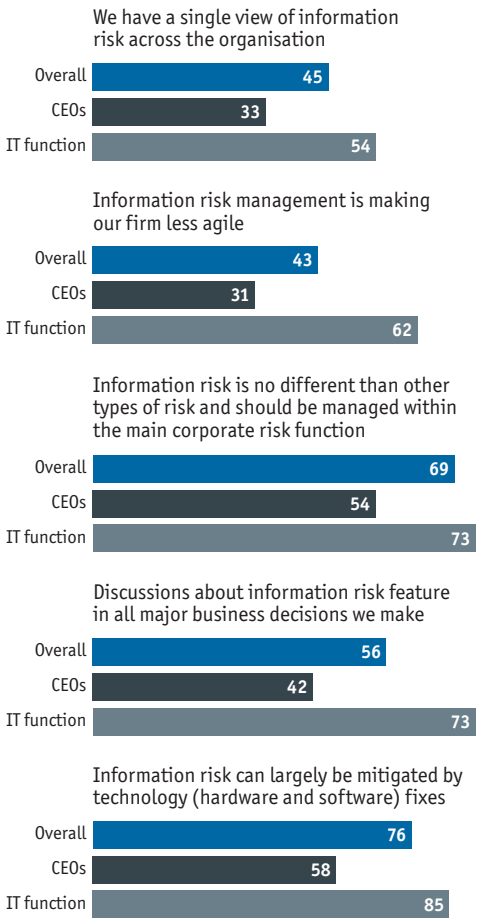
The respondents to our survey are equally sanguine about IT's ability to protect information: three-quarters (76%) of respondents believe that information risk can largely be mitigated by hardware and software fixes, although this view is noticeably more prevalent among respondents from the IT function (85%) than among CEOs (58%). The danger here is that a lot of what passes for information risk management today is really information security. It is a function operating in the IT department, and it relies heavily on technology to mitigate risks (firewalls, demilitarised zones, patching).

Clearly the approach to information risk management is heavily influenced by the person or department given responsibility for overseeing it. There is no single senior management position with primary oversight of information risk management at the majority of companies, but it is most common for the chief information officer (CIO) to take charge among the firms in our survey (26%). Some professionals and experts warn that many of the people occupying these roles are more chief IT officers than true CIOs (a further 13% of companies have the IT director in charge of information risk).

Chart 4: View from the top

To what extent do you agree with the following statements:

(% of respondents who agree)



Source: Economist Intelligence Unit survey, August 2013.

Chris Sutherland, the CISO at BMO Financial Group, would like to see the responsible individual sit outside of a technology department altogether. "We very specifically do not report inside the technology groups: you will never be successful as a chief information security officer if you're in the CIO's office because, frankly, your priorities compete," says Mr Sutherland.

There are indications, nonetheless, that the prevailing IT-centric view of information risk is

> [Y]ou will never be successful as a chief information security officer if you're in the CIO's office...
>
> *Chris Sutherland, chief information security officer, BMO Financial Group*

beginning to change: 69% of respondents to our survey say that information risk is no different to other types of risk and should be managed within the main corporate risk function. (Practitioners like Amar Singh, the CISO of a FTSE 100 company, would like to see the information risk manager given a seat on the main corporate risk board.) This figure rises to 73% among respondents in the IT function but falls to 54% among CEOs, suggesting the need for a change in viewpoint is most pressing at the very top of organisations.

Control, delete: Keeping data can be costly

Retaining information that has little potential value, and after the legal requirement for storing it has passed, can cause unnecessary risks. Yet fewer than half of the respondents in the survey say that their organisation is strict about deleting information that is no longer required.

A study by IDC, a technology analysis firm, found that just 0.5% of the world's data is ever analysed.[2] Other studies have found that 90% of corporate data is never used.[3] "Holding data when there is not a specific business need just creates unnecessary risk," says Jim Routh, the chief information security officer at Aetna, a health insurance firm. "It's much more efficient to eliminate the probability of that risk by purging data."

Mr Routh says there is no one-size-fits-all model for data retention and destruction in the financial services industry. US regulators require records to be kept for periods ranging from 30 days to seven years. "There are all kinds of requirements to destroy information within specific timeframes," says Mr Routh. "It's really a balancing act between meeting regulatory requirements and keeping raw data for analysis within a specific timeframe."

Judging from our survey, companies in Europe, the Middle East and Africa are less strict about deleting data than their peers in North America and Asia-Pacific, although this may soon change—at least in Europe. The General Data Protection Regulation (GDPR), a planned EU law on data protection set to come into effect in 2016, mandates that personal data has to be deleted when a person withdraws consent for an organisation to hold it, or the data is no longer necessary and there is no legitimate reason for an organisation to keep it. Based on current drafting, breach of the GDPR could result in significant fines.

Meanwhile, data storage is perhaps more expensive than some might imagine. Malcolm Marshall, a partner at KPMG, says that firms often believe that the cost of working out which data can be deleted is greater than the cost of buying more storage. In the "big data" era, however, when petabytes of information are stored, one of Mr Marshall's clients has amassed a "vast amount" of unstructured data that is costing US$60m a year to store, prompting the company to begin the process of deciding which information can be safely destroyed.

[2] John Gantz and David Reinsel. The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, December 2012, IDC.

[3] Leung AW, Pasupathy S, Goodson G, et al. Measurement and Analysis of Large-Scale Network File System Workloads. Proceedings of the 2008 USENIX Annual Technical Conference, Boston, MA, June 2008.

3 Protecting the crown jewels

It is widely accepted by practitioners and experts alike that companies should not try to protect all information nor eliminate all risks. The reasons for this include the availability of company resources and the futility of the exercise—given enduring human fallibility and the growing sophistication of cyber attackers. There are also strategic considerations: not all information is of equal importance to the businesses, nor is all data required to be protected by legislation. Thus, a critical element of information risk management is determining which information is most valuable to the business.

Amar Singh says his approach is to concentrate all effort, spend and technology in protecting the "crown jewels" and any peripheral valuables that would cause the most harm to the organisation. Here harm could mean loss of business, cessation of business because of punitive regulatory fines, or irreparable damage to the brand and reputation. "The rest of the assets must be tagged and bagged as low-risk, low-impact," he says. "It's not good enough for organisations to say: everything is crown jewels for us."

The crown jewels—often referred to as "mission-critical" information—will be different in every organisation. Some of that information will be obvious, ranging from proprietary information to consumer data about addresses and credit cards—essentially the information that cyber-criminals are trying to get their hands on. Other critical information can be less obvious, making it important, say experts, to secure involvement in the process of senior executives who understand the business.

After all, senior managers on the business-side may have different attitudes from IT about what information is important. Malcolm Marshall of KPMG gives an example of an IT team at an energy company that prioritised particular innovations and mergers and acquisitions (M&A) data. The board, meanwhile, valued the data that could raise employee safety standards and reduce deaths. This realisation resulted in the company looking at risks in new areas.

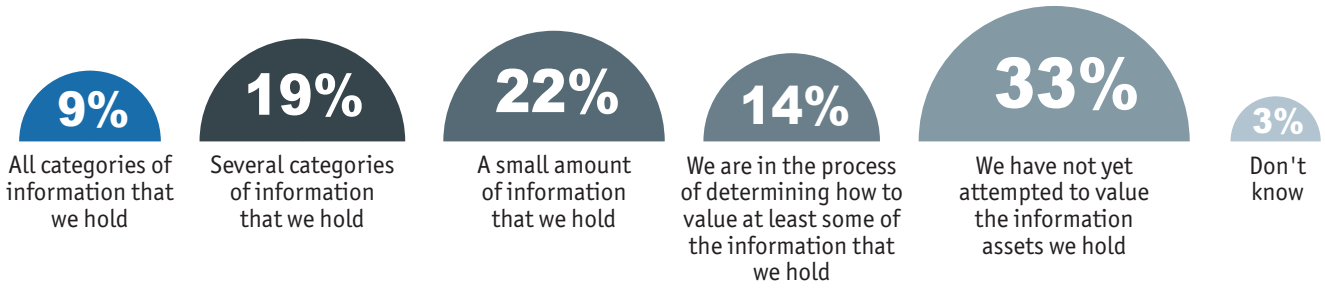
Taking this type of qualitative approach to determining mission-critical information is considered to be the easier option for companies. An alternative quantitative method growing in popularity is to attribute a monetary figure to information. There are clear merits in knowing the exact value of certain information assets—for example it can draw attention to the most high-value information and facilitate an objective analysis of which information to put the most protection around—but the challenge of doing so should not be underestimated.

Money talks

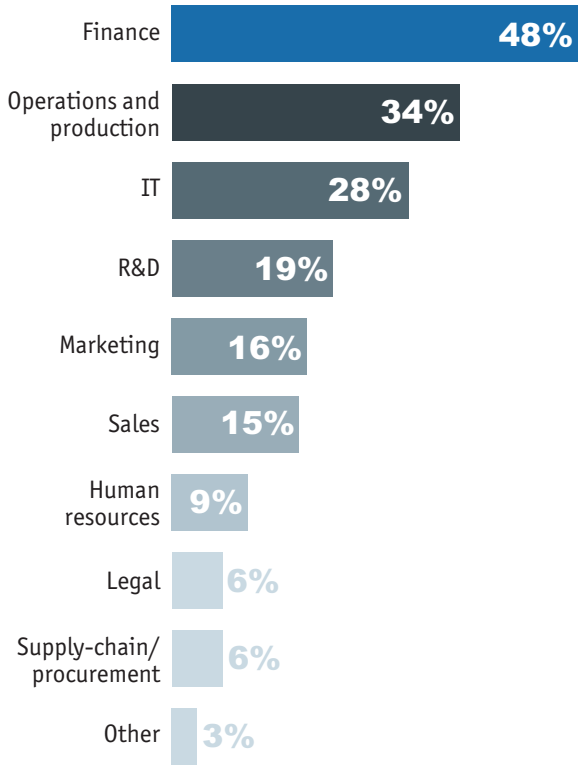
The recognition of information as a business asset, sometimes referred to as "infonomics", is still in its infancy, but our survey reveals that the majority of firms will soon be treating information in this way. Half (51%) of respondents have already assigned a value to at least a small amount of information, while a further 14% are moving in this direction. Gram Ludlow, an information risk expert, says that he has seen a few firms attempt it, but it is a very complex system and it tends not to last. "It doesn't work for a large, complex organisation,"

Chart 5: Infonomics

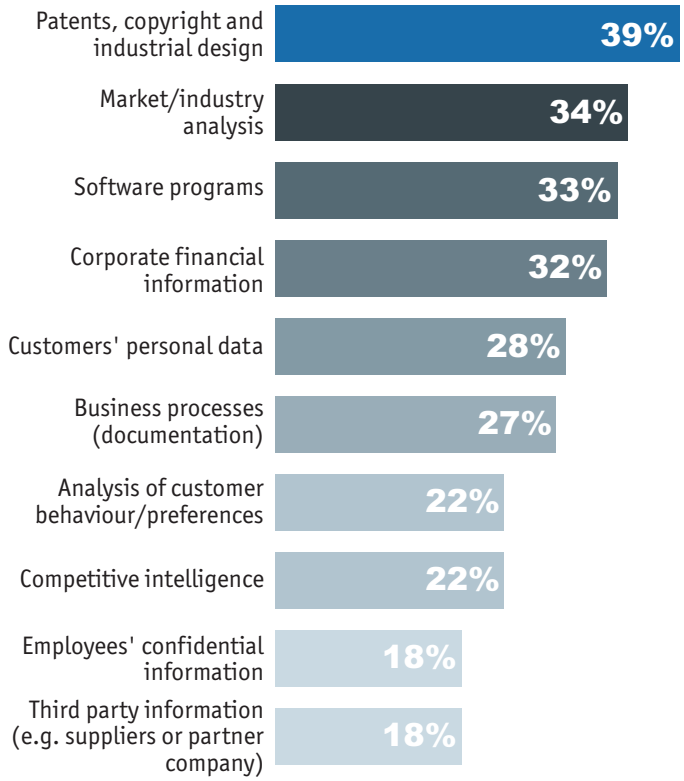
To what extent has your organisation attributed a monetary value to the information it holds
(% of respondents)



Departments with most mission-critical information
(% of respondents)



Types of information most likely to be assigned a monetary value
(% of respondents)



Source: Economist Intelligence Unit survey, August 2013.

he says. "In a large company, there is too much data, it's too spread out, or there are too many data sources to maintain a strict system."

Marcus Alldrick of Lloyd's of London agrees that it is "very difficult" to put precise values on information. "We look at thresholds and we we ask, Where does [the value] come within this range and what causes the value to the company?" Mr Alldrick and his team then evaluate what a breach or accidental loss of data would cost. "Everything is protected by a baseline level of control and then depending on the value of the information in terms of availability, integrity and confidentiality, we place additional controls on top of that," he says.

As a measure of the difficulty of valuing data, among firms in the survey that have attempted this, the largest number have attributed a monetary value to only a small amount of information. The majority of respondents believe that the most mission-critical information resides in the finance department, yet when organisations put a value on information it is usually on patents, copyright and industrial design. There are some obvious reasons for this—for instance, the fleeting nature of much corporate financial information. Finance data for a pending merger or acquisition may be very valuable at the time, but quickly loses most of its value once the deal has been done; whereas patents and trade secrets tend to hold their value for much longer—in the case of the recipe for Coca-Cola, 127 years.[4]

Arming the guardians and the doormen

A parallel activity to identifying this mission-critical information is controlling access to it. Creating a culture of awareness is a crucial part of managing information risk, which should span all levels of an organisation. Stefan Fenz of the Vienna University of Technology advises companies to include literally every employee in the process, from the cleaning personnel to the CEO. For Mr Singh, this involves identifying, protecting and educating what he calls the "guardians and the doormen who have access to these jewels".

Employees are generally considered the biggest risk to information, but fully 57% of respondents believe the importance of protecting information is mainly discussed only at senior levels and has not filtered down to lower levels of the organisation. Attempts to create this culture of awareness by means of a tick-box exercise needs to be avoided.

"Most organisations still use the awareness approach where they put someone in front of a machine and require him or her to go through a boring 5-10-minute computer presentation, following which they confirm and tick a box that they understand what they have just seen," says Mr Singh. "This is then reported as 'we have delivered training'. This will often be a compliance exercise rather than proper education."

The tactic used by Mr Singh is to engage employees on a personal level. "If I can help you, the end-user, protect and secure your personal cyber-life, then you will use that same knowledge and awareness and apply it to the corporate cyberspace," he says. Some experts like Mr Fenz recommend randomly testing personnel—tests that could range from sending fake e-mails and making fake telephone calls to external actors turning up at offices with a fake story and dressed in disguise.

The logistics firm FedEx makes all new hires attend an "InfoSec 101" course, and all employees are required to re-sit the course annually. FedEx's "enterprise security awareness programme" includes e-newsletters and publications, targeted awareness campaigns for high-risk groups, "road show cyber-security sessions" and an annual cyber-security conference at the firm's headquarters. "A key strategy of the overall programme is educating employees on current threats and providing practical security tips they can apply both at work and home," says Denise Wood, the CISO at FedEx. "We also partner with operating companies to deliver information through their existing channels."

Of course, no amount of training or testing will stop an employee occasionally leaving their smartphone or laptop in a public place, so technology can provide a solution in these circumstances, such as remotely wiping sensitive information. Likewise, employees can be prevented from accidentally introducing a virus to the corporate network, or deliberately stealing a contacts database, by blocking the USB ports on their desktop. By the same token, companies should be mindful of relying solely on technology to fix a risk that is still highly susceptible to human behaviour. "Deploying more security

"A key strategy of the overall programme is educating employees on current threats and providing practical security tips they can apply both at work and home."

Denise Wood, chief information security officer, FedEx

[4] http://www.dailymail.co.uk/news/article-2402603/A-formula-success-How-famous-food-drink-brands-boast-secret-recipes-despite-changing-way-things.html [Accessed September 16th 2013]

technology for the sake of deploying technology is a folly," says Mr Singh.

Assessing the supply chain

Ten years ago, most organisations had a simple process for handling information: data entered a company and it was put into a database controlled by that company. Nowadays the governance of information risk routinely goes beyond the organisation, stretching into the supply chain as well. When TNT Express ships products for Apple, it has to look as if Apple shipped the device, not TNT, says Phil Cracknell, the CISO of the logistics company. "So their databases are in our hands and we have to look after them as well as we look after our own." The type of information sharing and risk transference that this implies means that organisations need a level of assurance that partners are going to protect data as well as they do, if not better.

Organisations can apply for an international standard of best practice in this area (the ISO 27001), but most of the firms interviewed for this report such as TNT Express have their own minimum information handling standard that partners must meet. "It is your responsibility to ensure any third party which you deal with has the right coverage for data protection and looks after your data or your customer's data or your personal data to the right level," says Mr Cracknell. "Unless you actually check they do it right or have got some assurance from them, you're culpable."

The heavily regulated financial services industry has to be particularly vigilant in this regard. BMO Financial Group has a team dedicated to performing supplier risk assessments. The risk ranking of the supplier depends on the kind of information that will be shared and on the impact of an adverse event for BMO. "We either do site visits and on-site assessments, or we do a self-survey, or we're indifferent because it's not that big a deal," says Chris Sutherland, the firm's CISO in the US. "Conversely we also have a team that provides that information for other organisations that are assessing us." Either way, the bank has standard deliverables for each assessment.

Based on our survey, the majority (59%) of firms perform information risk assessments at least once a year. A further 29% say that they perform information risk assessments on a needs basis; this may include firms like BMO that perform a risk assessment each time they bring on board a new supplier or partner. However, this level of rigor is not the norm across the supply chain: over one-half (54%) of the respondents claim that suppliers rarely ask them about their information security policy or standards accreditation. This should be a note of caution for managers, since attackers are targeting smaller companies with less focus on information risk as a "back door" into larger organisations (see *Terror-bite: Small companies come under attack*).

4 Raising the standard

The single largest barrier to raising the status of information risk, as far as survey respondents are concerned, is a lack of understanding of the issues. Training—or the lack of it at senior level—is one aspect of this knowledge gap. Around one-third (34%) of senior executives—and over one-half of CEOs—say that they have not received training or instructions in how to protect information in the past year.

An even larger number, some two in five (41%) respondents, have not had training in the past 12 months on what to do after information has been lost or stolen, even though nearly half of organisations have experienced a loss of information in the past two years. Not surprisingly, the level of preparedness for loss of information among senior managers is generally low. Fewer than one in four respondents (23%) feel sufficiently prepared to take the lead in handling a breach. Levels of preparation are highest within the IT function but below average (15%) among CEOs.

Judging from our survey, there is a link between training and the level of preparedness for an actual loss of information. Those respondents who receive regular training are almost twice as likely to feel well prepared (45%) to deal with a breach as those who do not receive any training (23%). However, this 45% figure drops to 16% at those companies that have suffered a loss of information, which suggests that current education and training exercises are falling short of preparing senior managers for the real thing.

Talking in code

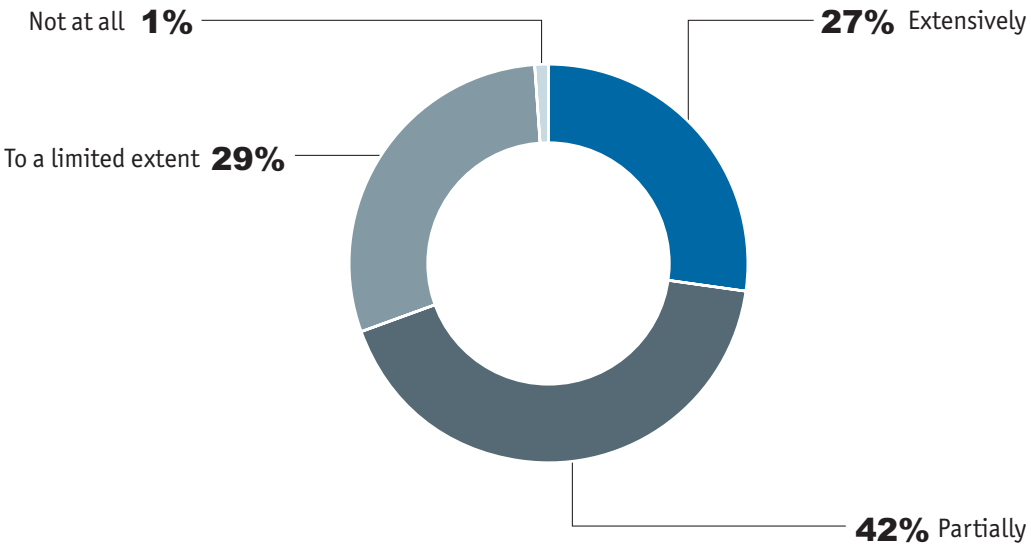
Besides educating senior executives, practitioners point to the need to improve day-to-day communications across the organisation. At board level, the discussion needs to be couched in terms of the business—where a lack of understanding can extend both ways. "The biggest area where we consistently fail is the language barrier," says Chris Sutherland of BMO Financial Group. "It's the geek-to-suit language. We spend all our time talking about exploits and bad guys and using industry buzz words, but we're not really talking about quantifiable business impact, and that's really what it's about."

This failure to communicate is evident when asking about the top barriers to raising information risk as a business priority. Among the CEOs in our survey, a lack of expertise or know-how within the organisation is a key barrier, second in importance only to a lack of understanding. By contrast, a lack of expertise comes near the bottom of the list of barriers cited by IT respondents; so to the extent that know-how does exist within an organisation it is not being spread around the business.

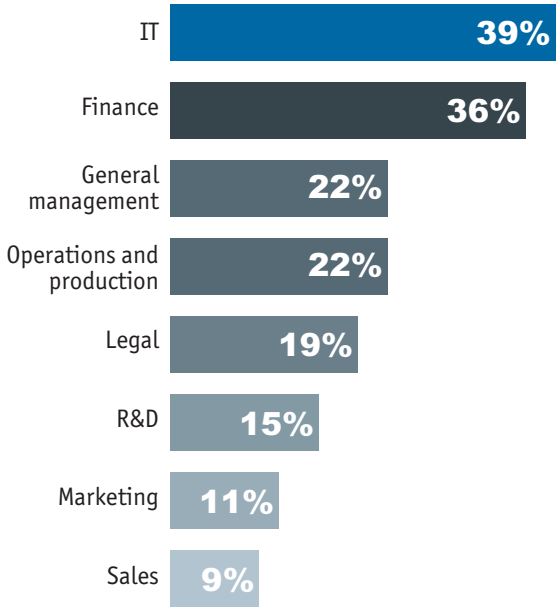
The impact of this communication failure can—in extreme cases—be severe. Mark Jones of Heathrow Airport Holdings cites examples where people who know a lot about information risk have sought and failed to influence the board because they lack understanding of the business. As a result, the board members have

Chart 6: Need to know basis

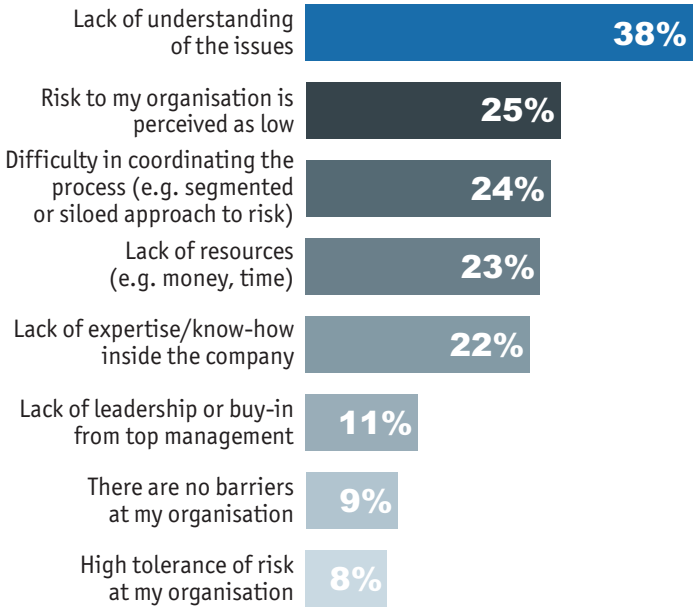
Q **To what extent are the concepts of information risk, and its management, known in your organisation?**
(% of respondents)



In which parts of the organisation is familiarity with information risk practices the greatest?
(% of respondents)



What are the biggest barriers to raising the status of information risk as a business priority at your organisation?
(% of respondents)



Source: Economist Intelligence Unit survey, August 2013.

refused investment and held back information risk programmes. Information risk professionals would clearly do well to note the areas where their opinions diverge from those of senior managers (see Chart 4).

What is more, this lack of understanding and poor communication extends across the business. Nearly one in three executives say that the concepts of information risk and its management are not well understood at their organisation. When these concepts are understood, it is mainly the IT function and finance that are in the know. Knowledge of information risk management is considered to be lowest in marketing, sales, human resources, and procurement—some of the functions being transformed by "big data".

"Departments like the marketing department are now collecting a tremendous amount of data and are becoming, behind IT, probably one of the largest generators of all kinds of data," says Amar Singh. This could be cause for concern to senior management when much of the data being handled is likely to be personal—the treatment of personal data is coming under closer regulatory control and the failure to protect it is attracting greater penalties, particularly in Europe.

One way to improve the situation is to try to encourage more directors and managers who have had business leadership experience to come into the field. "I would like to see more people in information risk management who have had P&L [profit and loss] responsibility," says Mr Jones. "Increasingly, executive management teams, operating boards, executive committees and main boards, are interested in information risk management, and when you're framing your argument to them, you are much more credible if the listener knows that you've come from a background where you understand the business imperative," he adds.

> "I would like to see more people in information risk management who have had P&L [profit and loss] responsibility."
>
> *Mark Jones, director, information technology security, compliance and governance, Heathrow*

Going beyond the law

When the General Data Protection Regulation (GDPR) comes into effect in 2016, the new EU law on data protection—as currently drafted—will include new rules requiring the mandatory deletion of personal data if an individual withdraws consent for an organisation to hold it. Fines for non-compliance with the GDPR such as losing identifiable personal data can be up to 2% of annual global revenue, up from a previous ceiling of €500,000.[5]

Marcus Alldrick of Lloyd's of London is in favour of increased regulation because he believes it will make organisations aware of their responsibility to protect the personal information they store and process, and it will stimulate them to think more about effective information risk management. In its current form, the proposed European rules include the mandatory reporting of data breaches within 24 hours of becoming aware that they have occurred.

"Some would argue it's a bad thing," says Mr Alldrick. "From our standpoint, it's a good thing—as long as it is fair, reasonable and pragmatic—because it increases transparency, and also because we get to understand more as an insurance industry about the types of attacks, the business impact that the attacks have, and so forth. We will be able to scope and price our policies more effectively because we are seeing an increase in cyber-risk-related insurance."

On balance, the majority (62%) of respondents to our survey are looking to government to take a greater lead in the area of risk management. Support here does not necessarily mean drafting new legislation, however. An even larger number (68%) of respondents believe the regional differences in legislation around data protection and privacy make the management of information risk more difficult, so a standardisation effort would be welcome, particularly for multinationals.

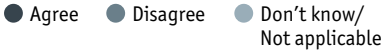
The involvement of government in information risk management extends to more than just drafting laws. In the UK, for example, the government has invested £650m in a national cyber-security programme. One of the

[5] http://www.bbc.co.uk/news/uk-22338204 [Accessed September 20th 2013]

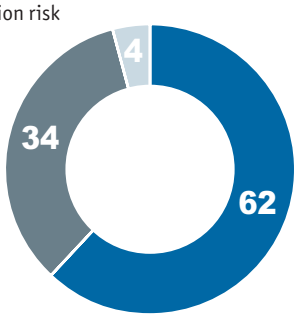
Chart 7: Ministry of information

To what extent do you agree with the following statements:

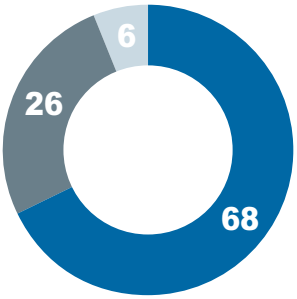
(% of respondents)



Governments need to take a more active lead in information risk



Regional differences in legislation/rules (around data protection and privacy) make the management of information risk more difficult



Source: Economist Intelligence Unit survey, August 2013.

achievements of the programme is the launch of the Cyber Security Information Sharing Partnership (CISP)—an arrangement with industry to share information and intelligence on cyber-security threats. Similarly, the UK security services recently sent a letter to every chairman of a FTSE 350 company to raise awareness of information risks at the boardroom level.

"The government and the regulators are really promoting communication, co-operation and collaboration," says Mr Alldrick. "We are seeing and we are involved in more information sharing which is to the benefit of our industry, to other industries and to society as a whole."

Still, not all collaboration needs to be government-led. At Brown University, David Sherry shares information about the latest threats with the other Ivy League universities, as well as affiliated schools in New England. "There's a lot of talking amongst the security groups," says Mr Sherry. "I came from financial services where sharing threat information was not common. We didn't share with our competitors."

Nor should industry wait for government to write the rule book on information risk. Legislation can play an important role in information risk mitigation, particularly around cyber-attacks, but ultimately it will only ever be a partial solution because technological innovation will always move faster than governments. Just as the EU's Data Protection Directive was wrong-footed by the arrival of social media, cloud computing and globalisation, so the GDPR—which will supersede the Data Protection Directive—is likely to be wrong-footed by the arrival of yet more disruptive technologies.

Conclusion

Just as firms are beginning to grasp the value of information as an asset, new business trends are taking information outside of the organisation, making it increasingly vulnerable to theft, loss and damage. The perceived value of information and the increased sophistication of attacks on this asset have elevated the importance of information risk management at a senior level across industries. Yet there is a disconnect between the value executives attribute to information and the level of protection across the business.

Nearly three-quarters of respondents to our survey say that the concepts of information risk management are, at best, partially understood at their organisation, and the majority of organisations do not have a single view of information risk across the organisation. The cause of this gap is not a lack of senior management buy-in. Rather it is a lack of understanding of the issues, caused by the failure of information risk professionals to communicate in a common language familiar to the business.

The survey shows that information risk managers often sit within the IT function. One of the dangers of this approach is that information risk is perceived as an IT issue, and one that can be fixed by technology alone. Although a certain baseline of technology is vital to protecting the information assets, it is not the entire solution. Employees are still the weakest chink in the information risk management armour, and only robust education and a strong culture of risk awareness will strengthen this defence.

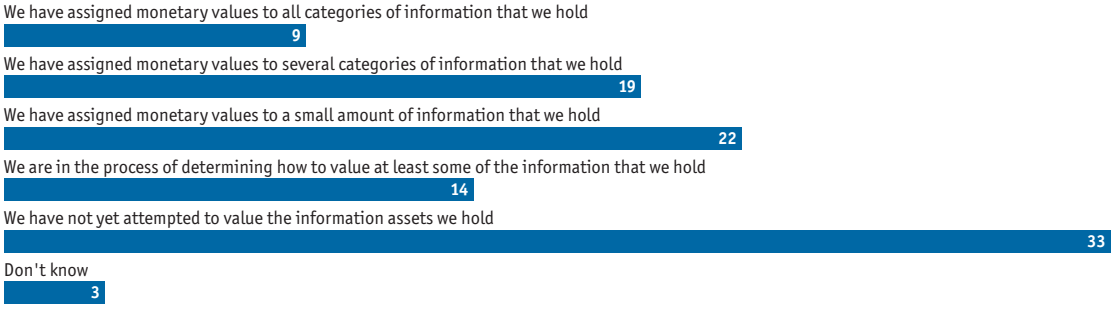
Information risk will never be eradicated, but it can be lessened to the extent that it matches the risk appetite of the organisation. The firms that are already achieving this tend to have information risk professionals who understand the business agenda and are embedded in project teams in the organisation. They do not just protect information, they also advise on how to get the most from this asset within the confines of regulation, legislation and the firm's own data protection policies. After all, if information really is the new oil, its full value will only be realised when it can flow freely and securely around an organisation's extended network.

Appendix

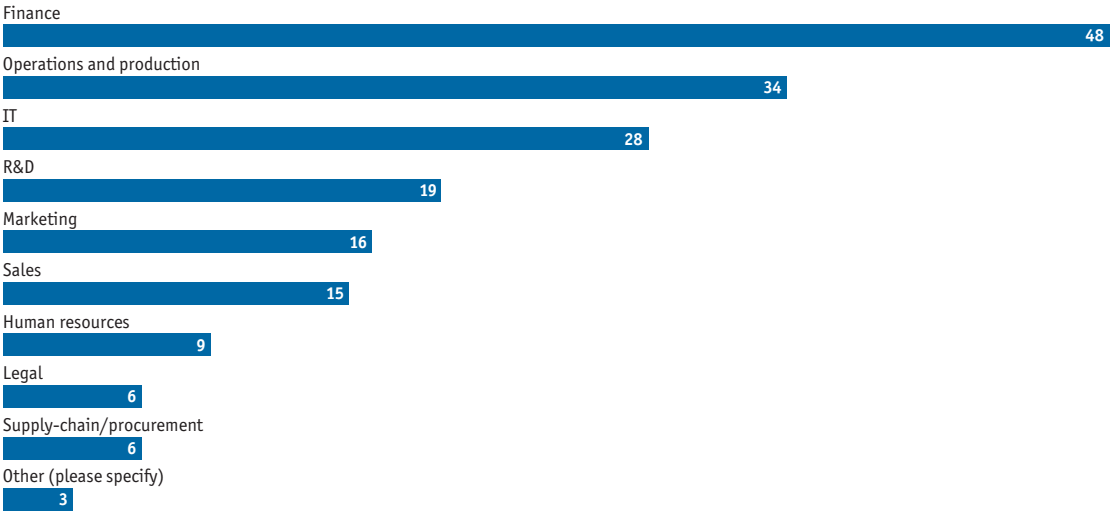
Survey results

In August 2013 The Economist Intelligence Unit conducted a global survey of 341 executives. Please note that not all answers add up to 100%, either because of rounding or because respondents were able to provide multiple answers to some questions.

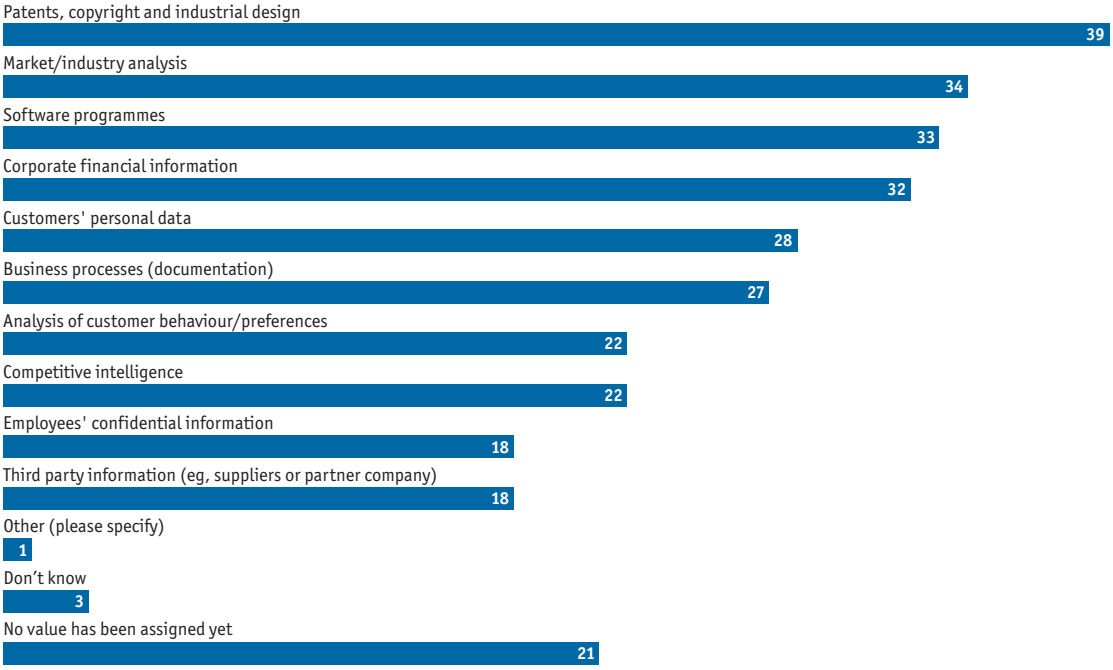
Which of the following statements best characterises your organisation's approach toward the valuation of its information?
(% respondents)



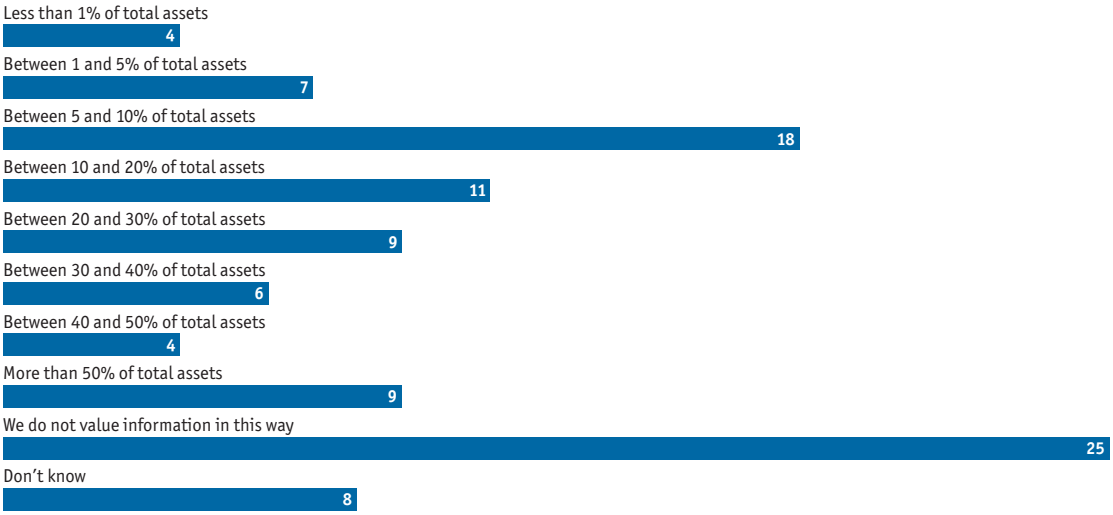
In which parts of your organisation does most mission-critical information reside? Select up to two.
(% respondents)



To the best of your knowledge, to which of the following types of information has a monetary value been assigned in your organisation? Select all that apply.
(% respondents)

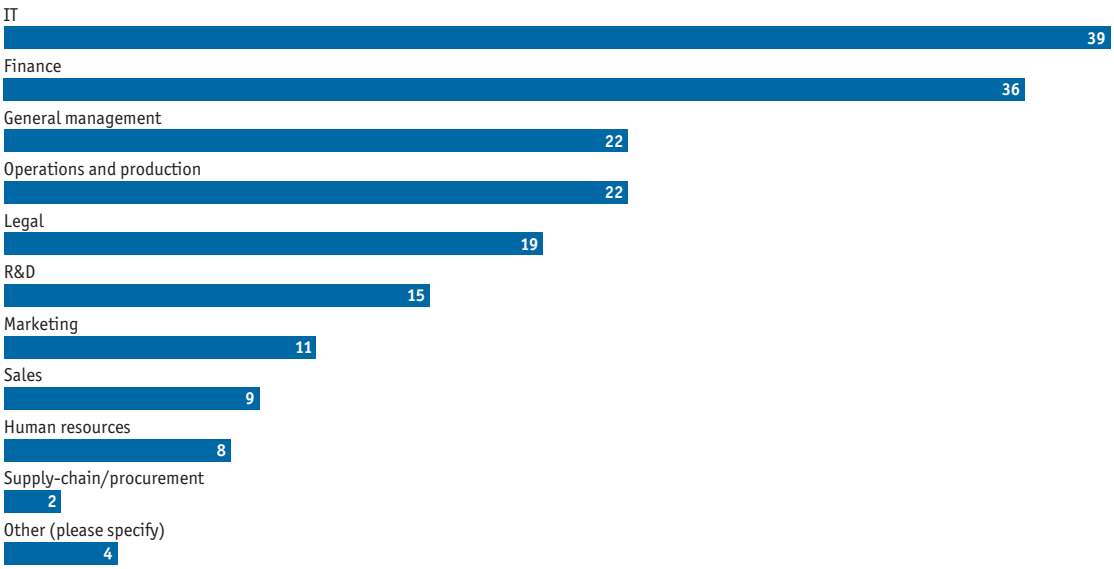


To the best of your knowledge, please estimate the value of information your organisation holds as a percentage of total assets?
(% respondents)

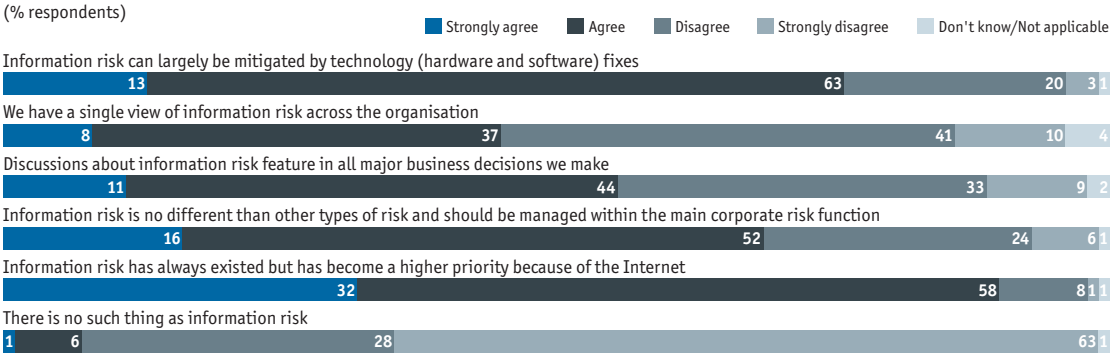


To what extent are the concepts of information risk, and its management, known in your organisation:
(% respondents)

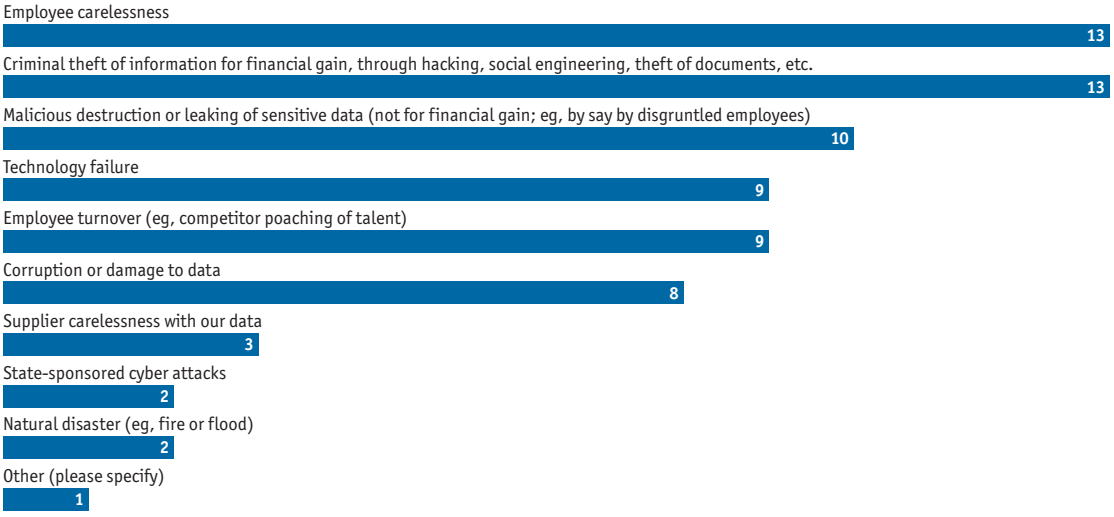
In which parts of the organisation is familiarity with information risk practices the greatest? Select up to two
(% respondents)



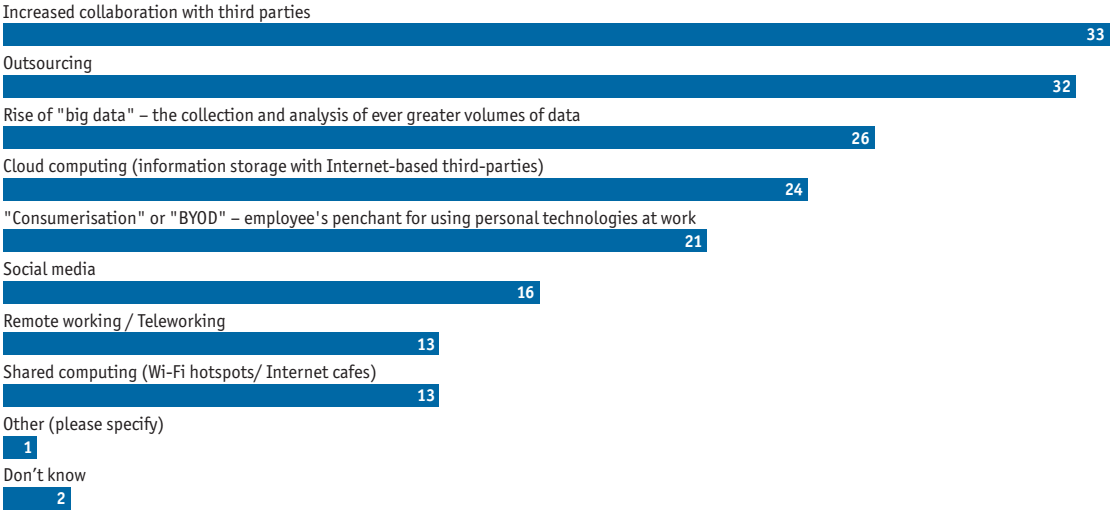
To what extent do you agree with the following statements?
(% respondents)



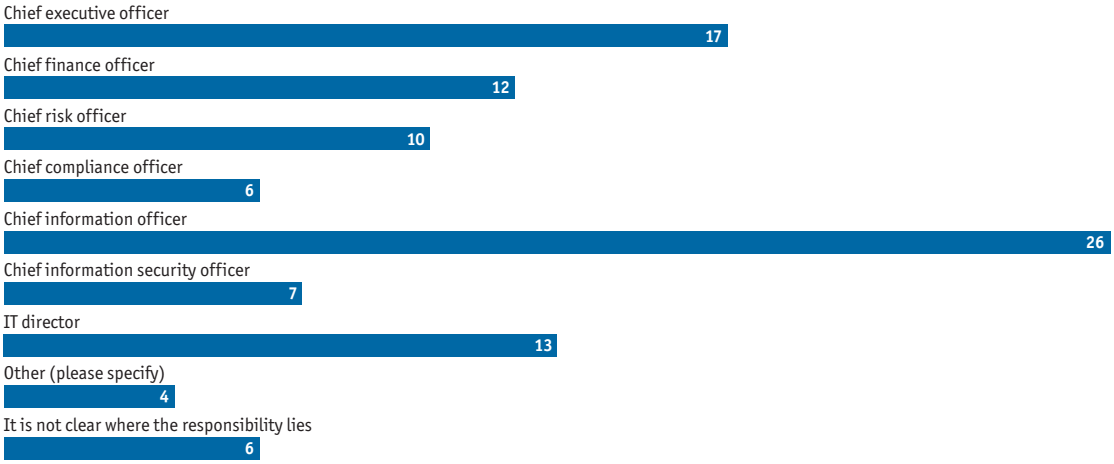
What are the main sources of risk facing your organisation's information? Select up to two
(% respondents)



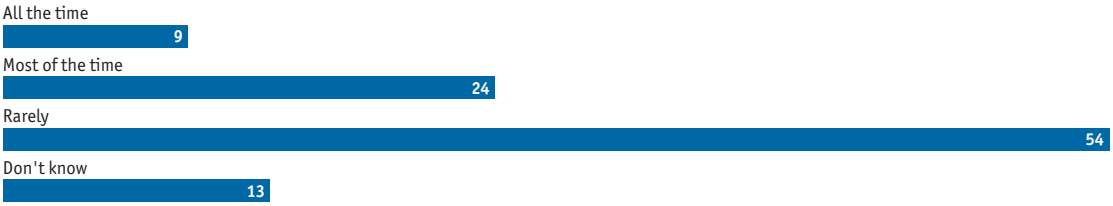
Which of the following business trends/technology developments are most likely to increase risks to your organisation's information? Select up to two
(% respondents)



Who is primarily responsible for information risk management at your organisation?
(% respondents)

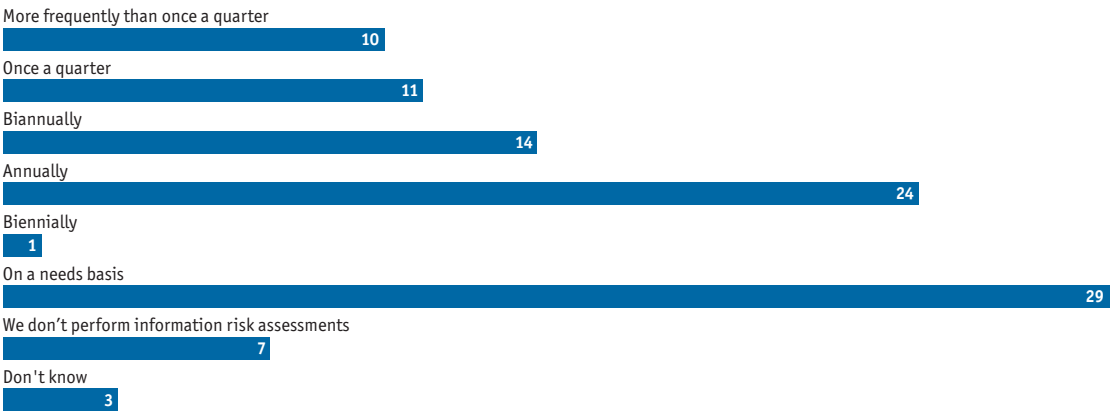


How often is your company asked about your information security policy or standards accreditation by suppliers?
(% respondents)



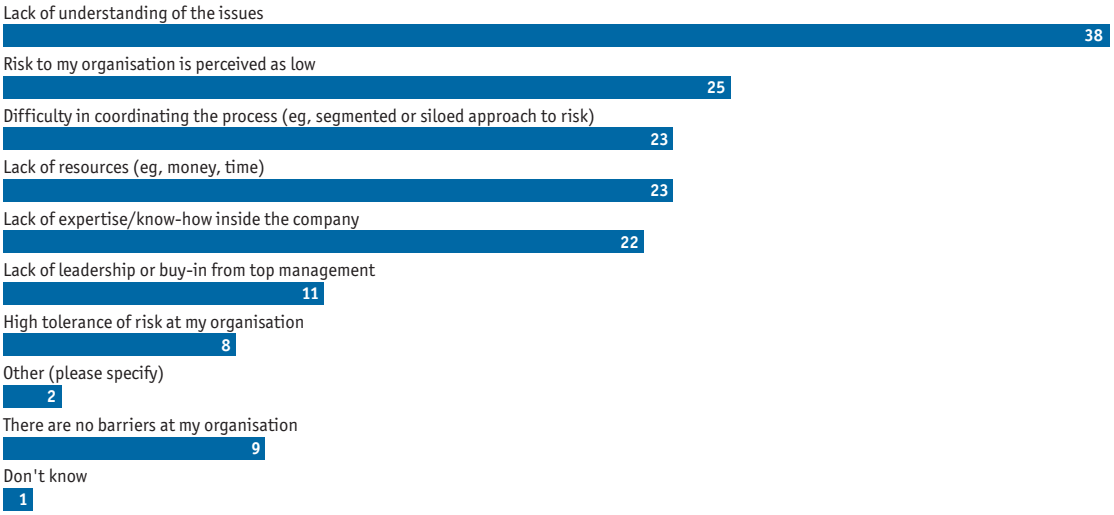
How often is your company asked about your information security policy or standards accreditation by major customers?
(% respondents)

How often does your organisation perform information risk assessments?
(% respondents)

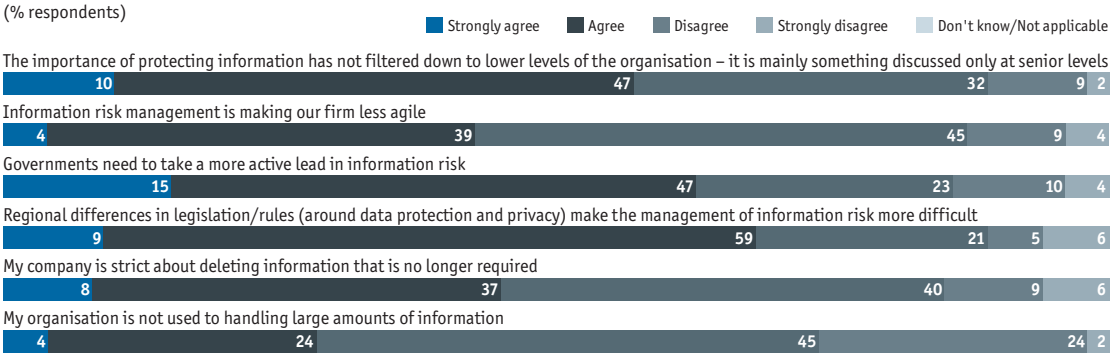


How much of a business priority is managing information risk at your organisation compared with your peers?
(% respondents)

What are the biggest barriers to raising the status of information risk as a business priority at your organisation?
Select up to two
(% respondents)



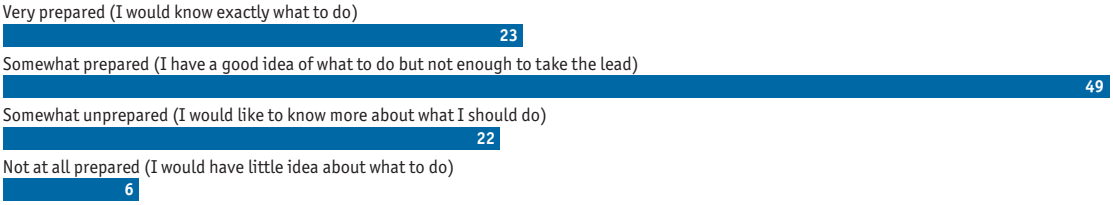
To what extent do you agree with the following statements?
(% respondents)



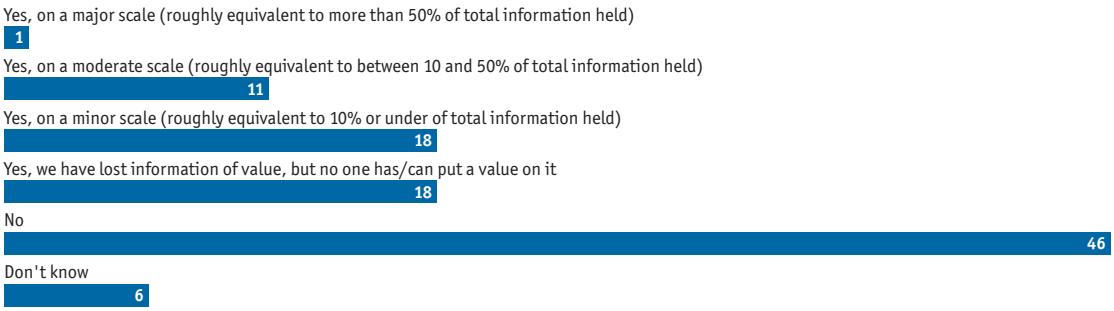
In the past year, how frequently have you received training or other instruction in how to protect information?
(% respondents)

In the past year, how frequently have you received training or other instruction in what to do should a loss or breach of information occur?
(% respondents)

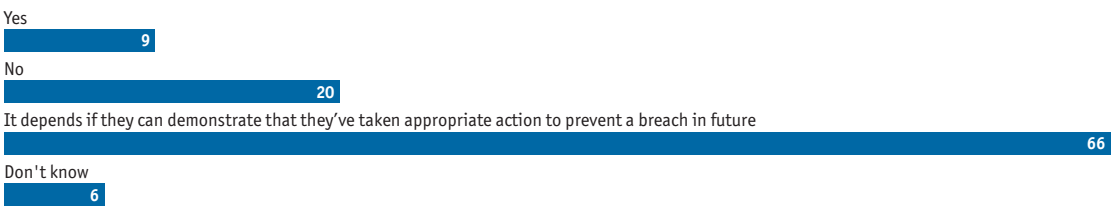
How prepared are you for a serious data breach or major loss of information at your organisation?
(% respondents)



Has your organisation experienced an information loss in the past two years?
(% respondents)

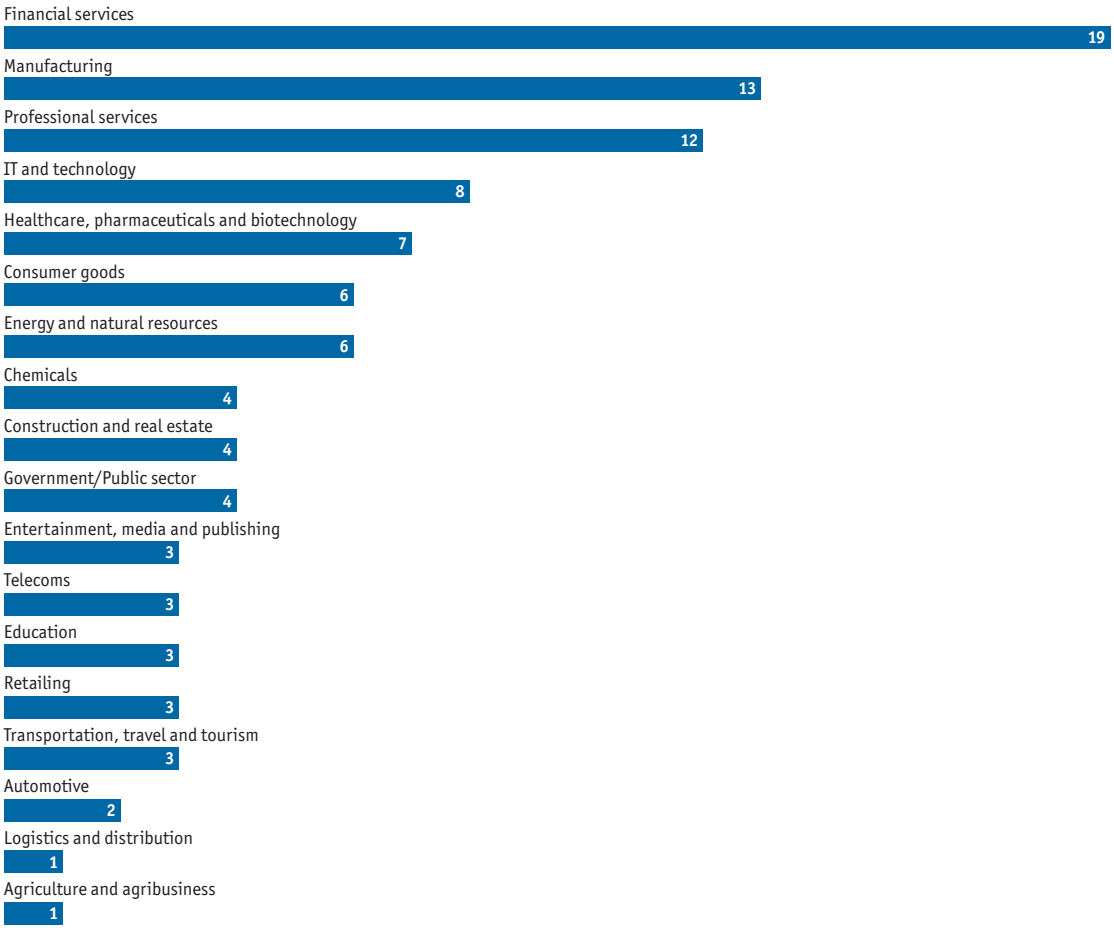


Would your organisation do business with an organisation that has suffered a serious data breach in the last year?
(% respondents)

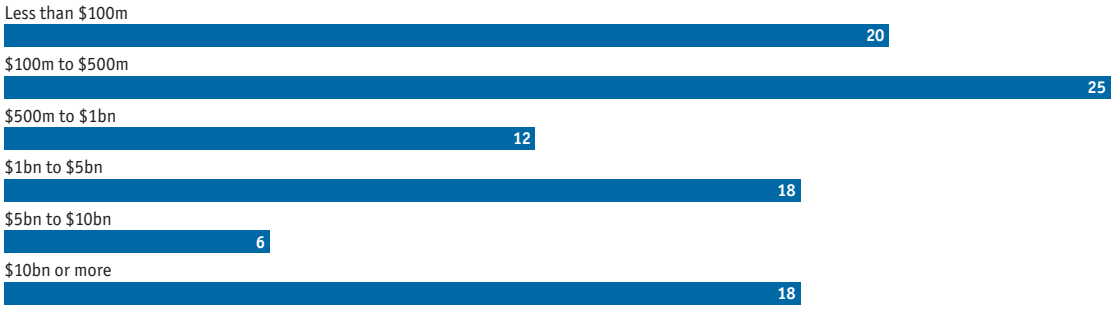


In which region are you personally located?
(% respondents)

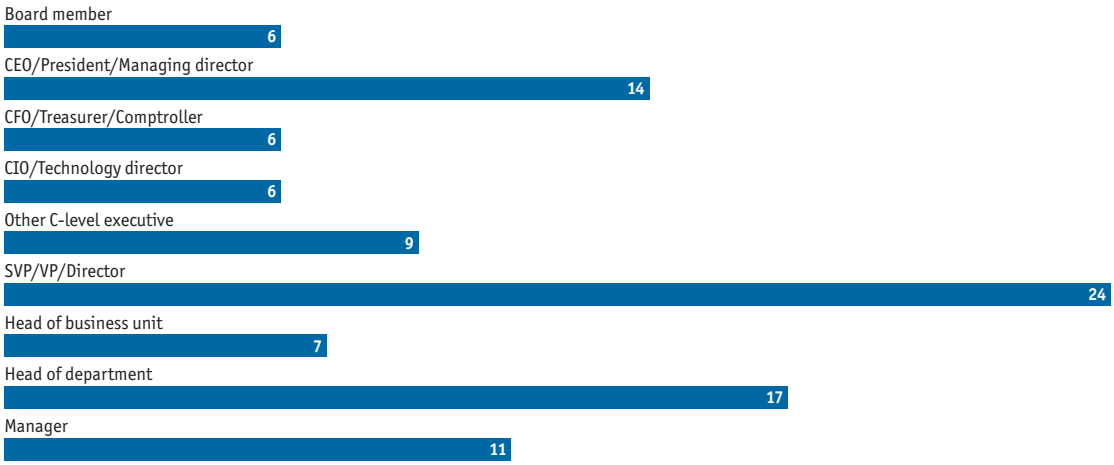
What is your primary industry?
(% respondents)



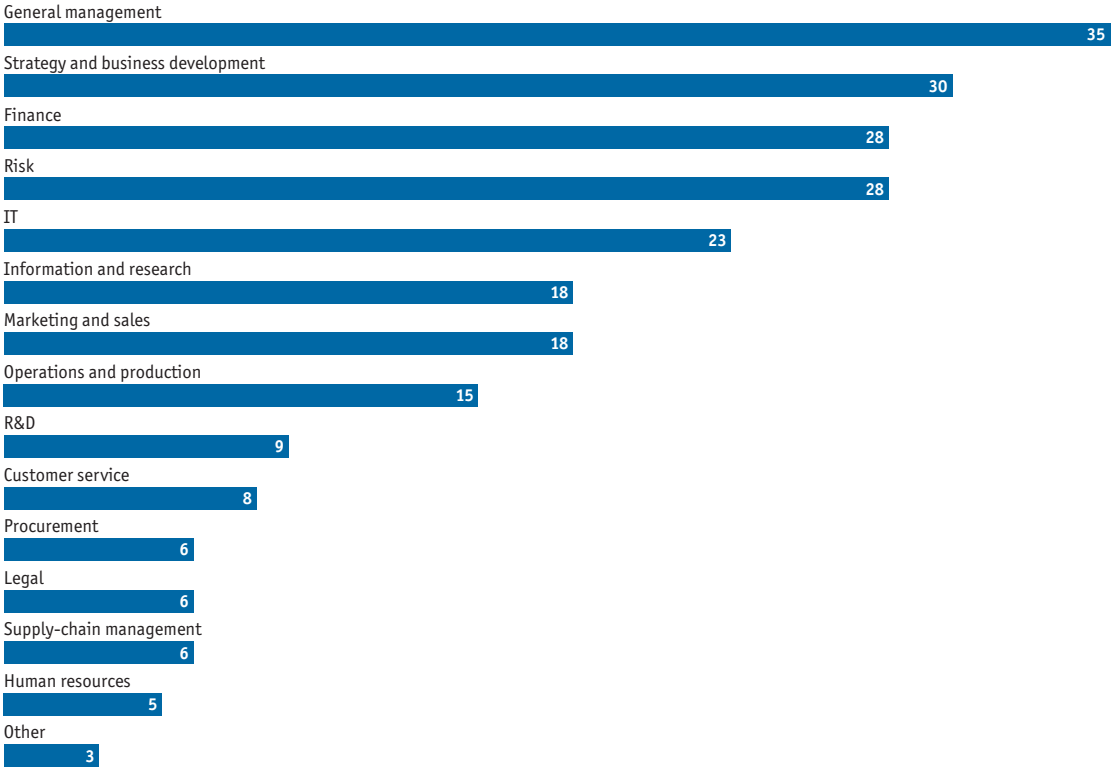
What are your organisation's global annual revenues in US dollars?
(% respondents)



Which of the following best describes your title?
(% respondents)



What are your main functional roles? Select all that apply
(% respondents)



With which of the following functions or practices are you familiar in your organisation? Select all that apply
(% respondents)

LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
E-mail: london@eiu.com

NEW YORK
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: newyork@eiu.com

HONG KONG
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

DUBAI
PO Box 450056
Office No 1301A
Thuraya Tower 2
Dubai Media City
United Arab Emirates
Tel: +971 4 433 4202
E-mail: dubai@eiu.com