www.pwc.com

Information security breaches survey

Technical report

April 2012

infosecurity EUROPE

BIS Department for Business Innovation & Skills

pwc

Survey carried out by:

Infosecurity Europe, celebrating 17 years at the heart of the industry in 2012, is Europe's number one Information Security event. Featuring over 300 exhibitors, the most diverse range of new products and services, an unrivalled education programme and visitors from every segment of the industry, it is the most important date in the calendar for Information Security professionals across Europe. Organised by Reed Exhibitions, the world's largest tradeshow organiser, Infosecurity Europe is one of four Infosecurity events around the world with events also running in Belgium, Netherlands and Russia. To register to visit or for further information please visit www.infosec.co.uk

This report was launched at Infosecurity Europe on 24 April 2012 at Earl's Court, London.

Reed Exhibitions is the world's leading events organizer, with over 500 events in 39 countries. In 2011 Reed brought together six million active event participants from around the world generating billions of dollars in business. Today Reed events are held throughout the Americas, Europe, the Middle East, Asia Pacific and Africa and organized by 33 fully staffed offices. Reed Exhibitions serves 44 industry sectors with trade and consumer events and is part of the Reed Elsevier Group plc, a world-leading publisher and information provider and a FTSE 100 company. www.reedexpo.com

Results analysed and report written by:

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

Our security practice, spanning across our global network, has more than 30 years experience, with over 200 information security professionals in the UK and 3,500 globally. Our integrated approach recognises the multi-faceted nature of information security and draws on specialists in process improvement, value management, change management, human resources, forensics, risk, and our own legal firm. PwC has gained an international reputation for its technical expertise and strong security skills in strategy, design, implementation and assessment services, and as such, was recognised as a leader in the Information Security And IT Risk Consulting field by Forrester Wave.

In association with:

Infosecurity Europe and PricewaterhouseCoopers LLP would like to thank the department for Business, Innovation and Skills (BIS) for their support and for allowing us to draw on past ISBS survey questionnaires and findings, so that we could analyse trends over the years.

The Department for Business, Innovation and Skills is making a difference by supporting sustained growth and higher skills across the economy.

BIS: working together for growth

www.bis.gov.uk

Introduction

This is the latest of the series of Information Security Breaches Surveys, carried out every couple of years since the early 1990s. Infosecurity Europe carried out the survey, and PwC analysed the results and wrote the report. The department for Business, Innovation and Skills supported the survey.

This year's results show that security breaches remain at historically high levels, costing UK plc billions of pounds every year. A big driver of this is the continuing escalation of cyber-attacks. The number of significant hacking attacks on large organisations has doubled over the last two years. We're also seeing many data protection breaches, data loss events and computer frauds, particularly in organisations that haven't invested in staff education. Most serious breaches result from failings in a combination of people, process and technology; it's important to invest in all three aspects.

Yet, organisations are struggling to target their security expenditure. There's also some evidence of complacency setting in among large organisations. The key challenge is to evaluate and communicate the business benefits from investing in security controls. Otherwise, organisations end up paying more overall; the cost of dealing with breaches and of the knee-jerk responses afterwards usually outweighs the cost of prevention.

It's clear that the business environment is anything but static. Social networks are growing in importance to business, and companies are rapidly opening up their systems to smart phones and tablets. Security controls are lagging behind the rate of technology adoption. Unsurprisingly, most respondents expect the number of security breaches to increase in the future.

As always, this report would be impossible without many people giving their time to work on it. Above all, we'd like to thank the survey respondents – this survey is very comprehensive and we recognise the commitment they've shown in completing it. Considerable time and effort has also been donated by the survey team at Infosecurity Europe and the data analysis and report writing team, especially Mark Sowerby, at PwC. Finally, we thank the independent reviewers who have, as always, provided insight and helped us ensure this report is balanced and focused on the most important findings.

Survey approach

In total, 447 organisations completed the survey during February-March 2012, on a self-select basis. The number of respondents by size is comparable with the 2010 survey (giving a margin of error on quoted statistics of +/-6% at 95% confidence for large organisations and +/-8% for small and medium-sized ones). As in the past, we have presented the results for large and small organisations separately, and explained in the text any differences seen for medium-sized ones. The 2008 and earlier surveys quoted overall statistics based on a weighted average; these were virtually identical to the results for small businesses.

Respondents came from all industry sectors. Compared with previous years, more were from business management and executive directors, though the majority of respondents continue to be either information security professionals or IT staff.

As with any survey of this kind, we would not necessarily expect every respondent to know the answers to every question. For presentation of percentages, we have consistently stripped out the Don't Knows. If the proportion of Don't Knows was significant, we refer to this in the text.

Introduction and methodology

Chris Potter
Information Security Partner

Grant Waterfall
IT Risk Assurance Partner

Figure 1: How many staff did each respondent employ in the UK?

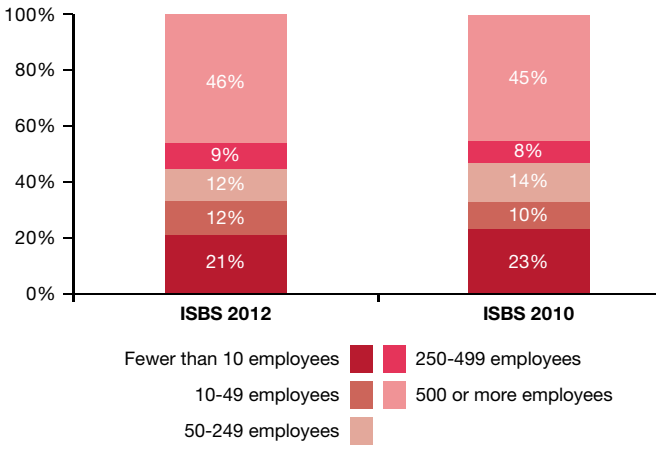
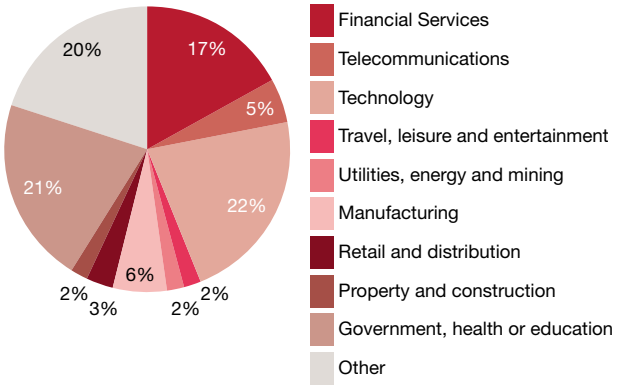


Figure 2: In what sector was each respondent's main business activity?



Executive summary

Increase in cyber-threats keeps cost of breaches high

The vast majority of respondents had a security breach in the last year:

93%	of large organisations
76%	of small businesses

The main cause is an increase in the number of cyber-attacks, especially for large organisations:

54	is the median number of significant attacks by an unauthorised outsider on each large organisation in the last year (twice the level seen in 2010)
15%	of small businesses were hit by denial of service attacks in the last year
15%	of large organisations detected hackers had successfully penetrated their network in the last year

As a result, the cost to UK plc of security breaches remains high, while down somewhat on 2010 levels:

£15k - £30k	is the average cost of a small business's worst security breach of the year
£110k - £250k	is the average cost of a large organisation's worst security breach of the year
Billions	is the total cost to UK plc of security breaches in the last year

It's not just about technology – people are vital too

Most serious security breaches are due to multiple failings in people, processes and technology. Computer frauds, data losses and regulatory breaches (together with hacking attacks) were most likely to result in a very serious breach.

45%	of large organisations breached data protection laws in the last year (and this happened at least once a day at one in ten of them)
18%	of organisations affected by infringement of data protection laws had an effective contingency plan in place
20%	of small businesses lost confidential data (and 80% of these breaches were serious)
19%	of large organisations suffered from staff carrying out computer fraud

The root cause is often a failure to invest in educating staff about security risks, often only recognised after the event:

44%	of large organisations carried out additional staff training after their worst security breach of the year (and 38% changed their policies and procedures)
26%	of organisations with a security policy believe their staff have a very good understanding of it
75%	of organisations where the security policy was poorly understood had staff-related breaches
54%	of small businesses don't have any programme for educating their staff about security risks

Controls are not keeping pace with business changes

The Internet continues to facilitate more sophisticated business relationships:

73%	of respondents have outsourced business processes over the Internet
38%	of large organisations ensure that data held by external providers is encrypted
56%	of small businesses don't carry out any checks of their external providers' security (and rely instead on contracts and contingency plans)

Social networks have become more important over the last two years:

52%	of small businesses depend on social networking sites (up from 32% in 2010)
8%	of small businesses monitor what staff have posted on those sites

Organisations are rapidly opening up their systems to access via mobile devices:

75%	of large businesses allow staff to use smart phones and tablets to connect to their systems
39%	ensure that data on these smart phones and tablets is encrypted
34%	of small businesses allow smart phones and tablets to connect to their systems but haven't done anything to mitigate the security risks

The challenge is to spend money wisely

On average, organisations continue to spend a significant amount on their security defences, as they expect the assault from breaches to continue:

8%	of IT budget is the average amount respondents spent on information security
50%	of large organisations expect to spend more on security next year (versus only 14% who expect to spend less)
67%	of large organisations expect more security breaches next year (versus only 12% who expect fewer)

However, there are some signs of complacency in some large organisations:

12%	say senior management give a low priority to security
20%	spend less than 1% of IT budget on information security

A root cause is that it is hard to measure the business benefits from spending money on security defences. Investing in security can end up losing out against other competing business priorities. Worse still, it's easy to spend money on the wrong things.

80%	of large organisations don't evaluate return on investment on their security expenditure
58%	of small businesses don't try to evaluate the effectiveness of their security expenditure at all

Security strategy and controls

Figure 3: How high a priority is information security to top management or director groups?

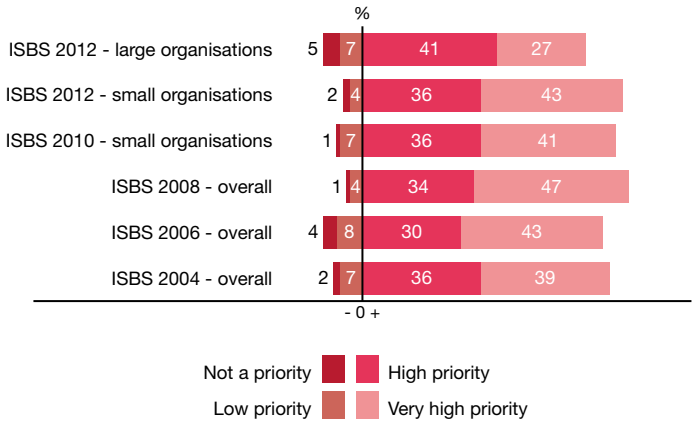


Figure 4: What is the main driver for information security expenditure?

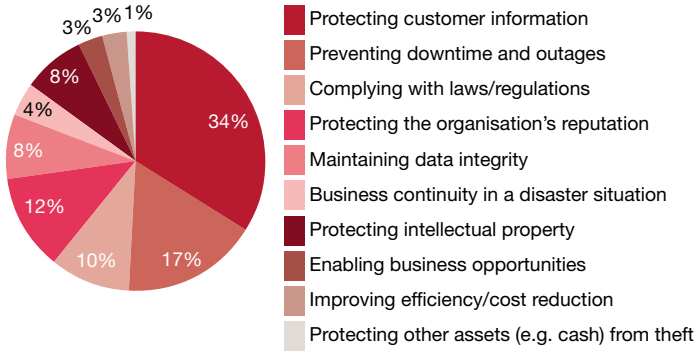
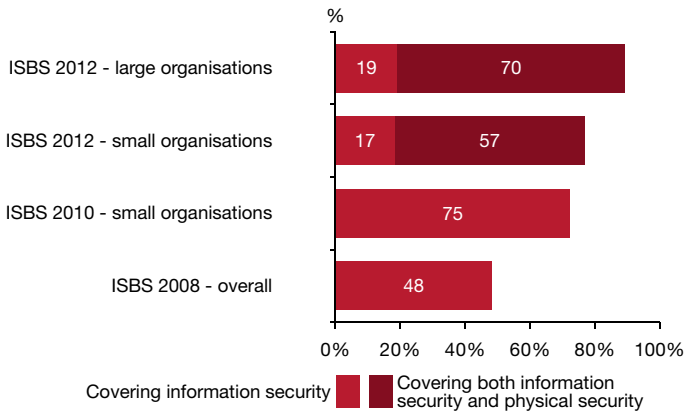


Figure 5: How many respondents carry out security risk assessments?



In 2008 and 2010, respondents were not asked about physical security

Attitudes to information security

Senior support is vital if staff are to manage security effectively. So, it is encouraging that three quarters of respondents believe security is a high or very high priority to their senior management. This is very consistent with the level seen two years ago. Nine out of ten executive directors think they give security a high priority, more than any other type of respondent. In contrast, one in eight IT and information security personnel feels security is a low priority. Often the priority that senior management believe they give to security gets lost in large organisations.

As in the past, there is significant industry variation. As expected, the financial services, government, utilities and technology sectors all give security a relatively high priority. However, the highest priority was reported by retail and distribution firms, twice as high as for property and construction companies. Following the trend first seen two years ago, small businesses are more likely to give security a high priority than large ones. Some respondents in large organisations were damning about the lack of priority they see and the impact this has.

A customer of a large telecoms provider suffered from multiple computer viruses on both its sites. The service provider's information security team raised this with their senior management who took the view that it was the customer's problem not theirs. As a result, only limited assistance was given, and the customer was still infected a year later. This was symptomatic of the low priority placed on security generally by the telecom company's senior management; their staff get no security awareness training and, as a result, the security policy is poorly understood.

The top four drivers for security expenditure are identical to those seen in 2010. The most common driver by a large margin is to protect customer information; this gap has increased substantially since 2008. Nine-tenths of these respondents feel that their organisation gives security a high or very high priority. Compliance with laws and regulations is particularly important in the government and finance sectors. Respondents that focus on efficiency and cost reduction were the most likely to report that security is a low priority.

Nine-tenths of large organisations now assess security risks; the number that don't has halved over the last two years. Most of them consider both physical and information security risks, reflecting how these have converged over the last decade. Almost every financial services provider conducts risk assessment. The weakest sector is property and construction, but even here only a quarter don't assess their security risks. There is a strong correlation between priority given to security and risk assessment; nine-tenths of companies where security is a high priority assess security risks, versus only three-fifths where security is a low priority.

A new question in this survey asked how respondents evaluate security threats. Most organisations are using multiple sources. The most common are discussions with senior management (66%), internal security experts (61%) and guidance from industry bodies (52%). Half of organisations use alerts from government and intelligence services; a similar proportion base their threat analysis on news media reports. Roughly 45% consult security product vendors and external security consultants.

Changing environment

Remotely hosted services can save on the expensive outlay for servers, licences, and maintenance, particularly for small businesses. In a time of cost constraint and given the industry hype, we might have expected a big increase in these services. Instead, the use of cloud computing hasn't changed much since 2010. Roughly three-quarters of respondents are using at least one such service.

Website, email and payment service provision remain the most commonly used services. This is particularly the case for small businesses, where more than half of websites are external and two-fifths use a hosted email solution; in contrast, only 14% of large organisations use an externally hosted email service. Small businesses are also more likely to use online office software and externally hosted finance solutions.

There is a trend towards data storage on the cloud; a quarter of small businesses now use online data stores, principally for backup purposes. This contrasts with only one in ten large organisations. On the other hand, large organisations are the most likely to be using externally hosted services innovatively to drive their business; one in five are using cloud computing solutions other than those listed.

47% of organisations with externally hosted services believe these are critical to their business; in contrast, only 6% report that they aren't important. This hasn't changed much since two years ago. Three-quarters of leisure companies and three-fifths of retailers have externally hosted services that are business critical. Half of organisations of national importance (e.g. financial services, telecommunications and utilities) critically depend on them. Overall, small businesses are just as likely to have critical externally hosted services as large ones.

The confidentiality of data stored on the Internet also hasn't changed much since 2010. Around a quarter of large organisations and one-fifth of small ones have extremely confidential data hosted on the Internet. Over 80% of manufacturing, leisure, retail and financial firms have confidential data on the Internet.

In contrast, social networking has become much more important to organisations since the last survey; one in seven believe social networking is very important to their business, with very little variation between different sizes of company. Only half of respondents now believe social networking sites aren't important to their business. This does vary considerably by sector. The travel, leisure and entertainment sector is most affected, with nine-tenths saying social networks are very important; in contrast, two-thirds of finance institutions and only four-fifths of manufacturers think these sites are unimportant. As organisations find more ways to exploit social networking, its importance is likely to increase and penetrate into the other sectors.

One further area where there has been a dramatic change over the last two years has been the growth of smart phones and tablet computers. 82% of respondents allow such devices to connect to their systems remotely. As confidential data is increasingly stored on them, the chance of data breaches increases.

A large financial services provider had a computer with confidential data stolen in a riot in Egypt. It took several man-weeks of activity to make sure that the confidential data was not misused. After the event, the firm invested in additional staff training to make sure similar breaches didn't happen again.

Figure 6: Which business processes have respondents outsourced to external providers over the internet?

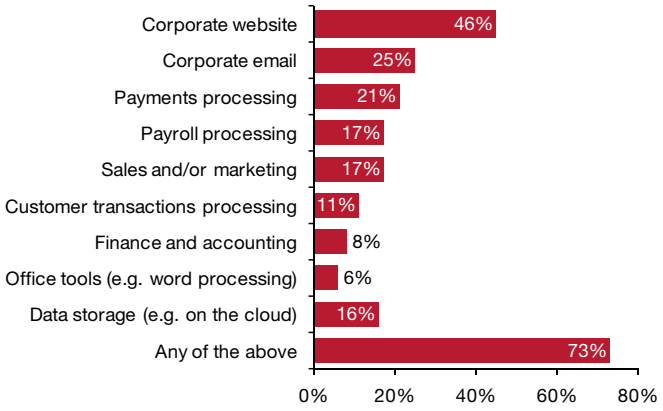


Figure 7: How confidential is the data that respondents store on the Internet?

Figure 8: How important is the use of social networking sites to the organisation?

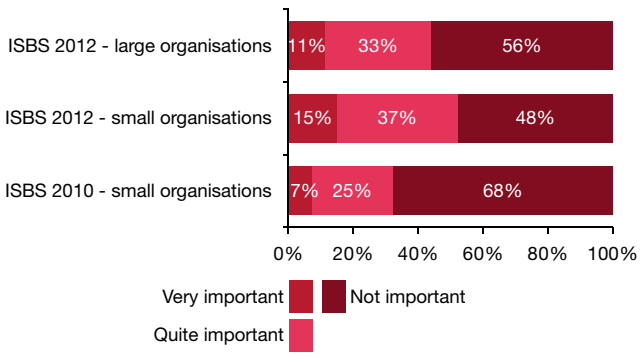


Figure 9: How many respondents have a formally documented information security policy?

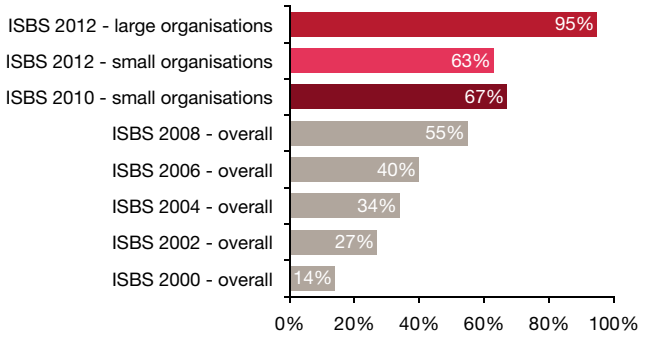


Figure 10: How do respondents ensure staff are aware of security threats?

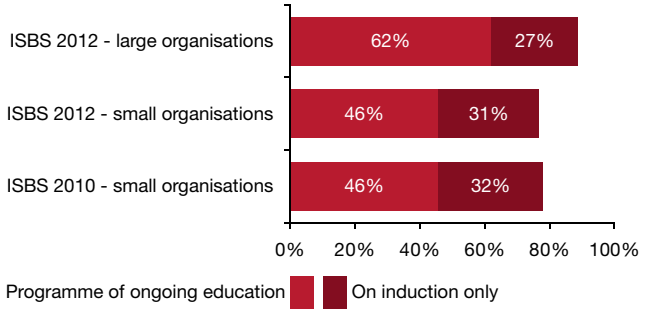
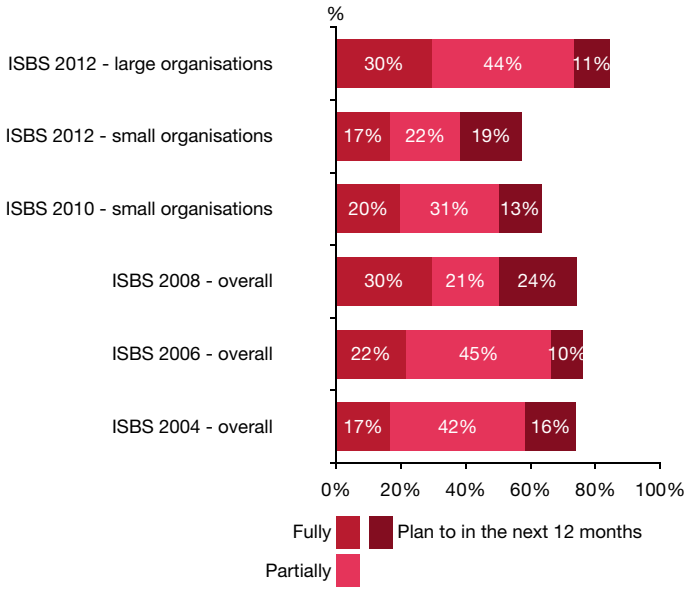


Figure 11: How many respondents have implemented ISO 27001?



Security culture

Setting out an organisation's approach to security is essential to ensure staff know what risks to look out for, how to handle data appropriately and what to do if a breach occurs. The last decade has seen a steady rise in the use of written security policies; for small businesses, this now seems to have reached a plateau, with about two-thirds having a formal policy. In contrast, almost all large organisations have a security policy. One in seven organisations that give a high or very high priority to security haven't written down their policy; most of these are small businesses that rely on word of mouth instead, but only a third think their staff fully understand this informal security policy.

Possession of a security policy by itself does not prevent breaches; staff need to understand it and put it into practice. Only 26% of respondents with a security policy believe their staff have a very good understanding of it; 21% think the level of staff understanding is poor.

Three-fifths of large organisations invest in a programme of security awareness training, up by 10% on 2010 levels; less than half of small businesses, however, do this. The survey results indicate a clear payback from this investment; 36% of organisations that have an ongoing programme feel their staff have a very good understanding of policy, versus only 13% of those that train on induction only and 9% of those that do nothing. Similarly, only 10% of organisations with an ongoing programme feel their staff have a poor understanding, versus 36% of those that train on induction and 49% of those that do nothing. There is some industry variation, with the property and construction sector least mature. Sometimes, it takes a breach before companies train their staff.

Routine security monitoring at a large public body in Northern Ireland picked up an employee using confidential data for personal reasons. There was a contingency plan to handle such events. As a result, despite the breach being widely reported in the media, the investigation took only a few weeks and resulted in disciplinary and legal action. Following the breach, additional staff training took place.

IT staff at a large financial services provider were testing a system change. Unfortunately, they were not aware of data protection rules and so used a copy of live data in a test environment that had weak access controls. The security team picked this up by accident and then rolled out additional staff training to make sure it didn't happen again.

ISO 27001 adoption rates appear similar to 2010; a quarter of respondents have completely implemented it, but a similar number haven't and don't plan to. Large organisations are twice as likely to implement ISO27001 as small ones. Adoption rates are highest in the IT and telecoms sectors (two-fifths report full compliance) and lowest among retailers and property companies.

90% of large organisations have prepared in advance for an incident, and half also have a response team in place. Small businesses are less well prepared; only 40% have contingency plans.

The accounting system for a small technology company in the Midlands became corrupted. There was no contingency plan in place; as a result, it took several days to recover the system. After the incident, the company developed contingency plans as well as changing its technology configuration and processes.

Investing in security

Putting a precise figure on the amount spent on security is difficult, since different organisations classify their expenditure differently. In many, security may not have a separate budget. This survey has historically used % of IT budget as a guide to the level of investment in security.

The average respondent now spends roughly 8% of their IT budget on security, roughly the same level as in 2010. Medium-sized companies spend on average slightly more than small or large ones, at 10% of IT budget. As in the past, there is a strong correlation between the priority that senior management put on security and expenditure; if security is a very high priority, average spend is 11% of IT budget, more than twice the amount spent when security is a low priority.

Organisations that suffered a very serious breach during the year spent on average 6.5% of their IT budget on security, slightly below the overall average. Given that most of them took many steps after the breach to tighten up their security, this suggests that the amount they had spent before the breach was low and had left them exposed. In many cases, this appears to have been a false economy.

A small public body in the South-East accidentally came across staff infringing the law. The technical configuration of the body's systems was not up to date, which had enabled the breach. It took more than a month to deal with the breach with several man-weeks of effort and several hundred thousand pounds worth of cost. The contingency plan for dealing with such breaches proved ineffective and so was updated after the event.

Roughly one in eight organisations now spend less than 1% of IT budget on security; this compares with one in five in 2008. A fifth of large organisations spend less than 1%, consistent with the pattern seen in 2010; this is probably due to the size of IT budgets in very large organisations.

Despite the prolonged economic slowdown, most organisations have spent more on security this year than in the previous one. Most large organisations expect this trend to continue, but small businesses are more likely to keep their expenditure steady in the next year.

There's a large regional variation; three-fifths of organisations in the North West of England and Northern Ireland have increased their security expenditure. In contrast, a third of those in Wales have decreased their security spending.

The 2010 survey showed that more than one half of government respondents were increasing their security spend, with only 6% reducing it. But this year's results show that spending has slowed down in this sector. The biggest spenders on security are now financial services, telecoms and manufacturing, all at around 10% of IT budget on average.

The companies that are most concerned about the future appear to be spending the least to protect themselves. Three quarters of respondents that aren't confident that they can detect the latest generation of attacks are not increasing their security budgets. Security skills appear to be a limiting factor; eight out of ten organisations that are not at all confident of getting the appropriate skilled security people have not increased what they spend on security.

Figure 12: How is information security expenditure changing?

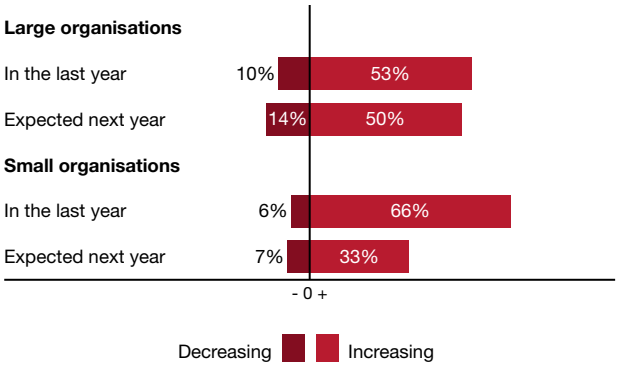


Figure 13: What percentage of IT budget was spent on information security, if any?

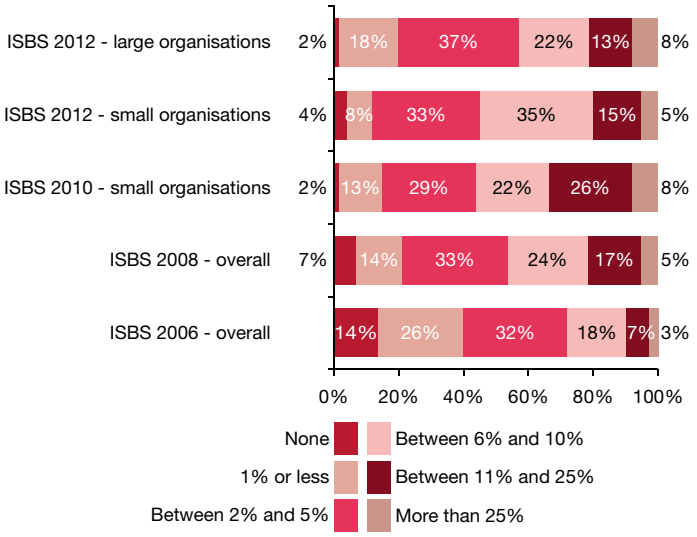


Figure 14: Which sectors spend most on security?

Average rate of increase (net number of companies reporting increase)	Average current security spend (as % of IT spend)		
	Below average (less than 6%)	Average (6% to 8%)	Above average (more than 8%)
High (more than +50%)	Travel, leisure and entertainment		Telecomm-unications
Average (between +30% and +50%)	Retail and distribution	Utilities, energy and mining	Financial services, Technology, Manufacturing
Low (less than +30%)	Property and construction	Government, health or education	

Figure 15: How do respondents measure the effectiveness of their security expenditure?

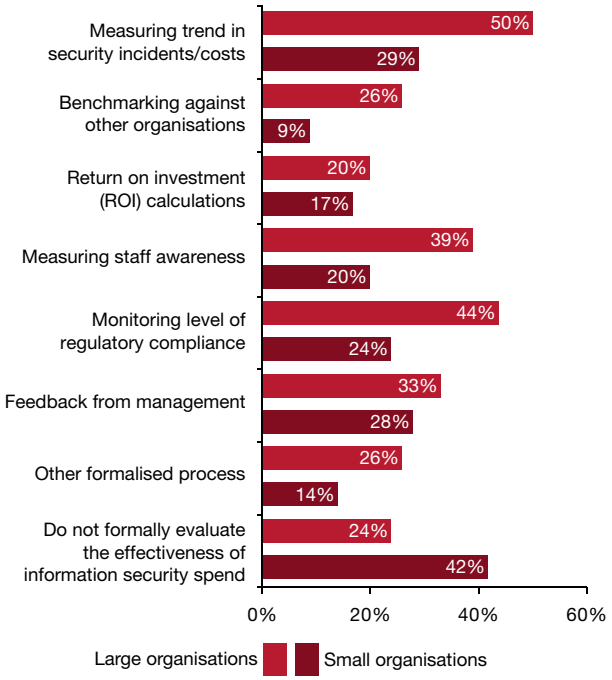
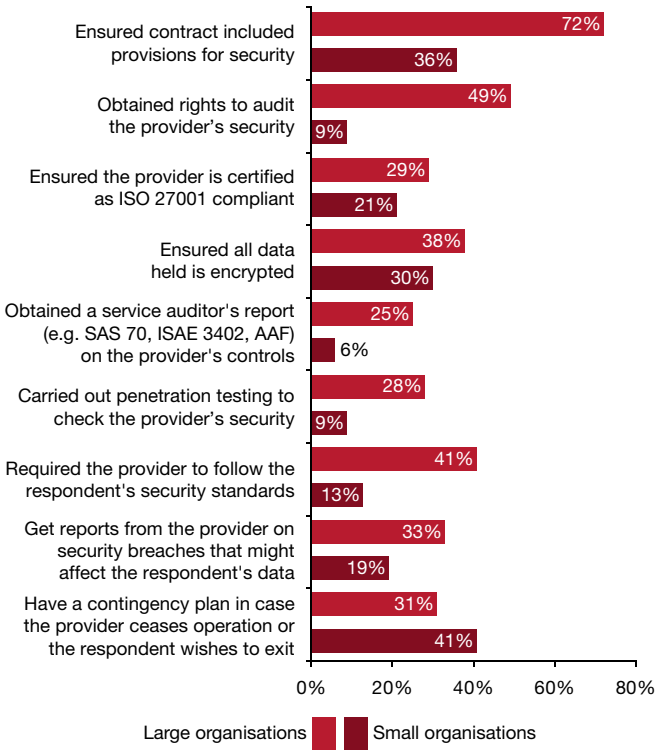


Figure 16: What steps have respondents that use externally hosted services taken to obtain comfort over the external provider's security?



Evaluating spend effectiveness

Given the general economic environment, most companies are tightly controlling their costs. This means it's very important to ensure money spent on security is spent wisely. Yet, a quarter of large organisations and nearly half of small businesses don't measure how effective their security spend is. The worst sectors are property, utilities and manufacturing.

Among those that try to measure the effectiveness of security, trend analysis of the number of security incidents or incident costs is the most common measure employed. Gathering feedback from management is also popular, particularly in small businesses. However, more than half of large organisations and two-thirds of small ones are not carrying out these basic measures.

More sophisticated measures are relatively rare. Only a quarter of large organisations benchmark themselves against others. Over the last decade, organisations haven't made much progress in treating security as an investment rather than an overhead. Only one in five try to calculate return on investment on their security expenditure; this is fewer than in 2006 when we last asked this question and is close to the levels seen in 2002. Worryingly, given the number of data breaches reported, less than half of large organisations and only a quarter of small ones are actively measuring their regulatory compliance.

Demand for assurance

Two-thirds of respondents now have significant outsourced services. Almost all of them take steps to gain assurance over their provider's security. Large organisations have got better at ensuring contracts contain security provisions and audit rights. Small businesses appear heavily dependent on changing provider if there are issues. A fifth of organisations that outsource critical data think that data ownership isn't clear, making it hard to ensure end-to-end security.

Weaknesses in a third party's security led to data corruption at a large financial services provider. The company's normal reconciliations detected the problem, but it took more than 100 man-days to fix it. The incident was caused by weaknesses in technical configuration, procedures and staff awareness, all of which were subsequently remediated.

Customers are increasingly asking respondents for assurance over security. The most common requirement is for compliance with a recognised standard such as ISO 27001, particularly in the financial sector. Meeting government-related standards is important for public bodies, utilities and telecoms. PCI DSS is most often requested for leisure companies, and independent service auditors' reports for the financial sector.

Old desktop computers from a large government body were diverted from the intended disposal company. After the audit that detected this, procedures were changed and monitoring of third parties' security stepped up.

Half of large organisations now give direct security awareness guidance to their customers (e.g. on their corporate website) and a third provide customers with security tools. The finance, government, telecoms and leisure sectors do this most.

A large government body suffered extensive adverse media coverage after gaps in their ISP's security enabled hackers to attack the body's website. After the breach, systems configuration, procedures and contingency plans were all updated; monitoring of third parties' security was also improved.

The personalisation challenge

Data ownership hasn't improved since the last survey. Only 35% of large organisations feel data ownership is very clear, and 26% of them think it isn't at all clear. As in 2010, this is less of an issue in small businesses, where 59% say it is very clear. Interestingly, 75% of executive directors believe data ownership is very clear, compared to only 31% of auditors.

What has changed since 2010 is the pressure on data security from increasing personalisation. Firstly, users are bringing their own smart phones and tablet computers to the office and taking sensitive data home. Secondly, companies are now much more dependent on the relatively anarchic information flows within social networks. Above all, dependence on the Internet is at an all-time high, which organisations often find out the hard way.

Failure to keep technical configuration up to date led to continual Internet failure for more than a month at a small marketing business in East Anglia. It took several man-weeks of effort to fix the problem, after which the company developed a contingency plan to deal with any similar event in the future.

Simply blocking all staff Internet access is no longer viable; instead, organisations tend to restrict which staff have access and block inappropriate sites. As in the past, large organisations are more likely to do this than small ones. Given how important social networks have become, it's surprising how little the control techniques used have changed over the last two years. Large organisations (especially in financial services) rely on blocking social media sites, rather than monitoring their use. Half of small businesses don't even have basic web blocking and logging software.

Practice varies by sector. Only a third of telecoms providers restrict staff access, and the sector is a leader in logging what staff post on social networking sites. In contrast, property companies have relatively weak blocking and monitoring controls.

Routine security monitoring at a large public body detected staff leaking confidential data via social media. Staff were not aware of the data protection rules or the security risks associated with social networks. The organisation responded by running extra staff training.

Smart phones and tablet computers are often lost or stolen, with any data on them exposed. If not controlled, these devices can punch right through security defences. Yet, it's clear how important they have become; three-quarters of large organisations and three-fifths of small ones now allow them to connect to corporate systems.

Unfortunately, the implementation of controls has not kept up. Over half the small businesses with mobile device use haven't taken any steps to secure them. Only about half of the large organisations that allow corporate data onto mobile devices make sure it is strongly encrypted. Organisations that allow personally owned devices tend to have weaker controls than those that allow corporate devices only. Personalisation is creating new security threats, from both malicious software and data loss.

A large public body in the Midlands was infected by malicious software on removable media. Routine security monitoring picked up the infection and the malware removed quickly.

Another large government body had a very serious breach when thieves stole unencrypted computers and external hard drives from an employee's house. Following the incident, hard disk encryption was deployed and staff received training about the security risks.

Figure 17: How do respondents prevent staff misuse of the web and social networking sites?

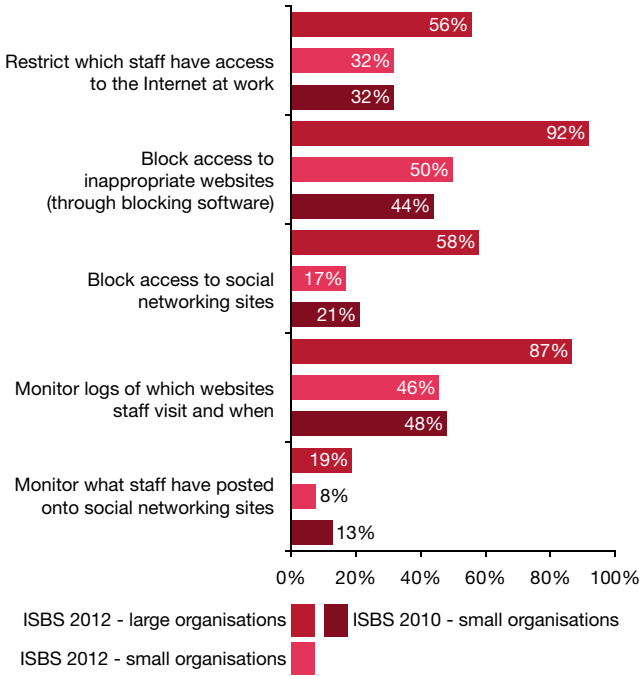
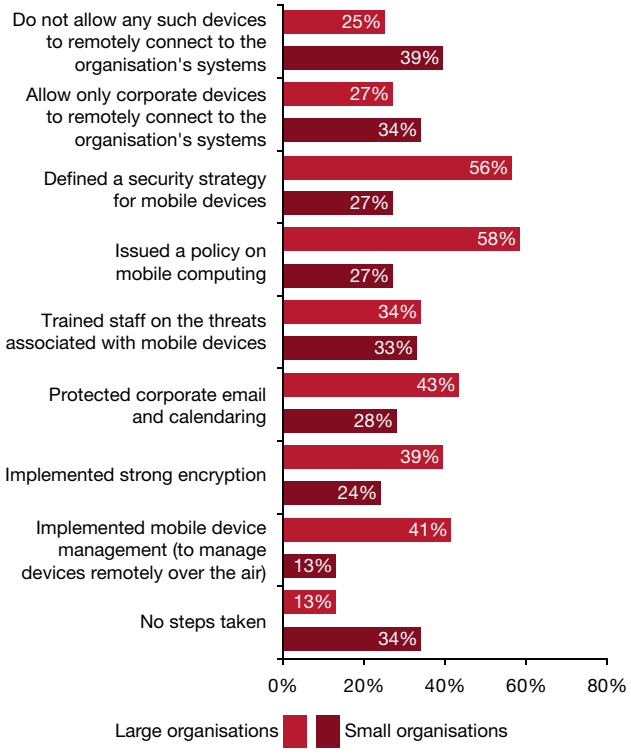


Figure 18: What steps have respondents taken to mitigate the risks associated with staff using smartphones or tablets?



Security breaches

Figure 19: In the last year, how many respondents had...

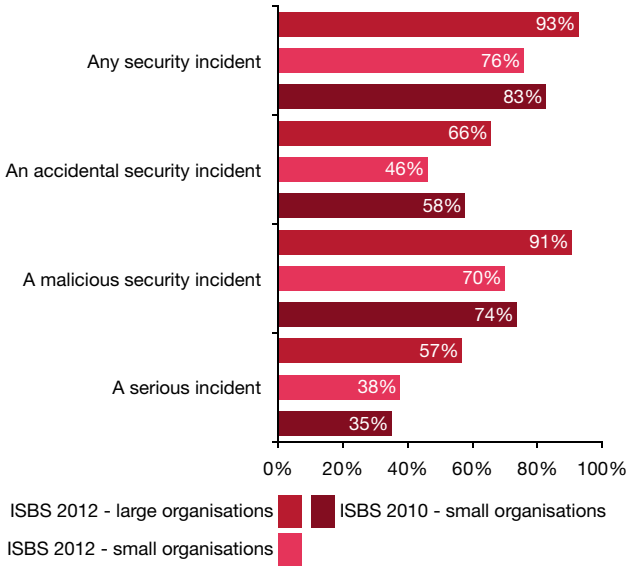
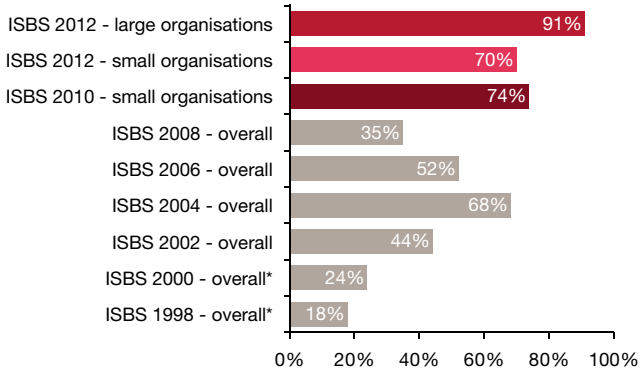
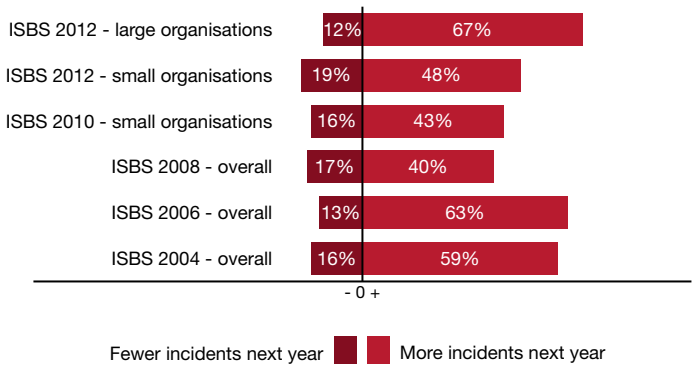


Figure 20: How many respondents had a malicious security incident in the last year?



The 1998 and 2000 DTI survey figures were based on the preceding two years rather than the last year.

Figure 21: What do respondents expect in the future?



Incidence of security breaches

The survey shows that the number of respondents reporting breaches remains at an all-time high. Nine tenths of large organisations reported malicious breaches, and two-thirds of them had a serious incident. Small businesses are not immune; three quarters of them reported a breach, and half of these were serious.

Large organisations are more visible to attackers, which increases the likelihood of an attack. They also have more staff and more staff-related breaches. This may explain why small businesses report fewer breaches than larger ones. However, it is also true that small businesses tend to have less mature controls, and so may not detect the more sophisticated attacks.

Malicious breaches affected a majority of respondents across all sectors. Property and utilities were least affected; two-thirds of them had a malicious breach. Financial services, leisure and public sector organisations were hit most.

Hackers attacked a large financial services provider's website, resulting in a major investigation lasting more than 100 man-days. After the breach, the company tightened up its procedures and the configuration of its systems.

Malicious breaches also affected all regions. Organisations in East Anglia reported fewest breaches, while Northern Ireland and the North-West were particularly hard hit.

Accidental security incidents also remain significant, with two-thirds of large organisations affected.

A large government body had systems problems for more than a month after a database failed to switch back cleanly from the disaster recovery site to the live environment. The technical configuration hadn't been kept up to date; as a result, the processes for switch-over failed. It took more than 100 man-days to fix the ensuing data issues.

We asked a new question this year about how organisations identified their most significant breach of the year. Routine security monitoring picked up a third, while a quarter were obvious from their impact (e.g. systems down, assets lost). Interestingly, 6% of organisations' worst security incidents were discovered by accident.

Our respondents remain pessimistic. Almost two-thirds of them expect the number of breaches to increase in the next year; this is four times as many as expect fewer incidents. No sector was optimistic, with financial services particularly concerned about the future.

Given this view of the future, it is vital to have the right skills available to prevent, detect and manage incidents. Respondents are more positive here. Two-thirds are confident that they will have access to the skills they will need over the next year. There is quite a wide industry variation here; property and leisure companies are least confident, while utilities and retailers are particularly confident. Interestingly, small and medium companies are twice as confident as large organisations; this suggests a skill shortage in complex IT environments.

Respondents are also, on balance, confident about the latest generation of attacks that are designed to evade standard protection tools; 50% are confident or very confident they will be able to detect them, 37% were unsure, while 13% were not confident. Again, there is significant industry variation; manufacturers, technology, telecoms and utilities are most confident, while property and financial services companies are least confident. Medium-sized companies are the most confident, twice as confident as large and small businesses.

Type of security incident

The number of respondents with system failure or data corruption was similar to our 2010 report. Two-thirds of large organisations and just under half of small organisations experienced such problems.

No industry sector appears immune from these incidents. Telecommunications, utilities and technology companies appear to have the most reliable systems. The public sector and travel, leisure and entertainment companies are most likely to have systems problems.

The number of respondents infected by malicious software was similar to the high levels reported in 2010; two-fifths of small businesses and three-fifths of larger companies reporting such breaches. This is close to the all-time peak, despite the amount organisations have spent on anti-virus protection. The arms race between malicious software writers and anti-virus providers shows no sign of abating.

The travel, leisure and entertainment sector was most likely to report virus infections, followed by telecommunications and manufacturing. As in the past, technology companies are the least likely to be infected, probably due to their high levels of past investment in security technology. Wales and Scotland had the most infections, while East Anglia and the Channel Islands reported the fewest.

In the 2010 report, fraud and theft rates had tripled compared to 2008, reflecting the recessionary environment. In 2012, fraud and theft remain at historically high levels. One ray of hope is that the average number of thefts for affected small organisations is half that of two years ago. Roughly three-fifths of manufacturers and retailers suffered from theft or fraud; in contrast, only a sixth of technology companies reported such breaches.

As in the past, large organisations were twice as likely to report staff-related incidents compared to smaller businesses. Despite most companies investing in security awareness training, the number of breaches caused by staff has not dropped over the last two years. No sector is immune, but property and construction companies were half as likely to have such breaches as manufacturers.

Outsider attacks have increased over the last two years, especially against large organisations; three quarters report being attacked, and the number of attacks against each has increased substantially. At least half of the respondents in every sector reported attacks, rising to three-quarters of travel and finance companies.

The trend in the average number of breaches suffered by affected organisations shows a marked contrast between small and large organisations. The mean number of breaches is now roughly one per day for small organisations, rising to ten per day for larger businesses. However, as always, the mean is distorted by a few respondents reporting hundreds of breaches per day, so the median tends to be a better measure. The median small business has roughly one breach per month, while the median large organisation has roughly one per week. Hacking attacks make up the largest single component.

Figure 22: What type of breaches did respondents suffer?

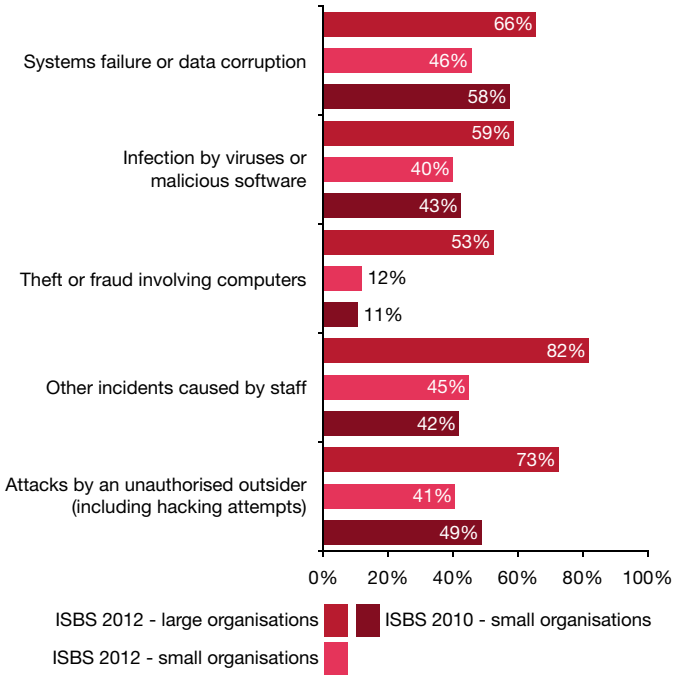


Figure 23: What is the median number of beaches suffered by the affected companies in the last year?

	Large organisations	Small organisations
Systems failure or data corruption	**3** (4)	**2** (2)
Infection by viruses or other malicious software	**3** (2)	**1** (1)
Theft or fraud involving computers	**5** (4)	**3** (8)
Other incidents caused by staff	**24** (20)	**8** (7)
Attacks by an unauthorised outsider (including hacking attempts)	**54** (28)	**8** (13)
Any security incident	**71** (45)	**11** (14)

Equivalent comparative statistics from ISBS 2010 are shown in brackets

Figure 24: What was the worst security incident faced by respondents?

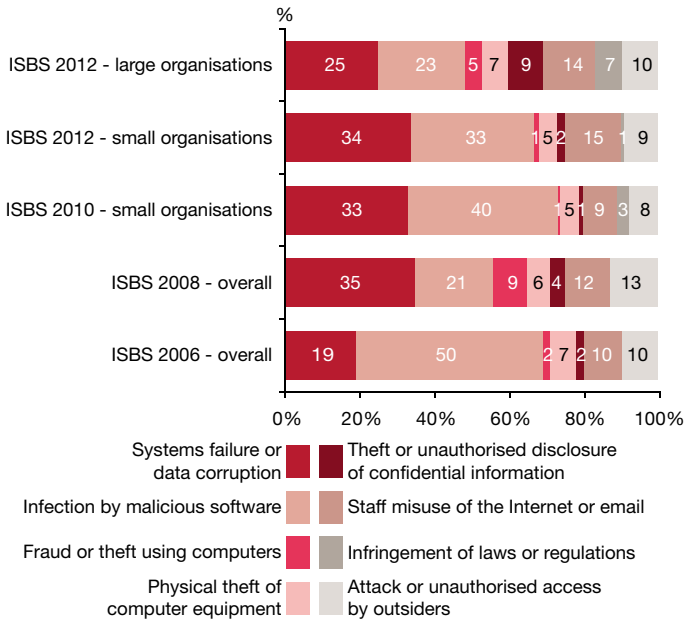
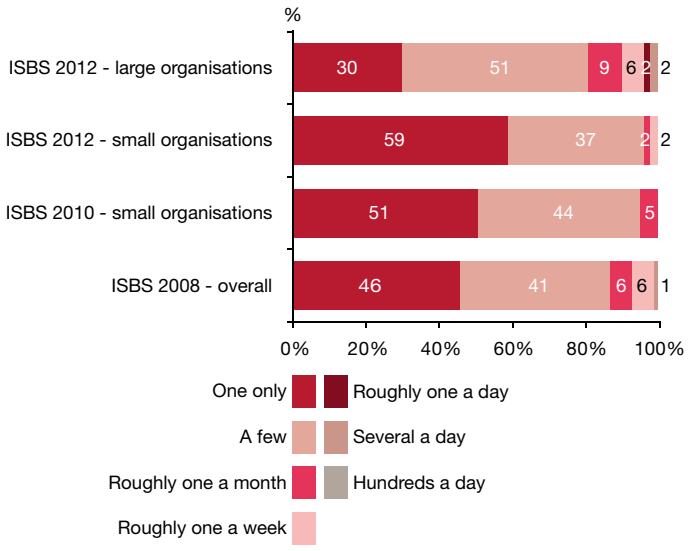


Figure 25: How many malicious software infections did the affected organisations suffer in the last year?



Infection by viruses and malicious software

The virus infection rate appears to have stabilised, but is still three times higher than in 2008. Two-fifths of small businesses were infected in 2011. Large organisations with more staff and computers continue to be much more susceptible to infection; two-thirds of them reported incidents.

The 2012 infections report showed a wide variety of different varieties of malicious software and attack routes. No single type dominated. Since 2010, we have not seen mass infections since 'Conficker', 'Nimda' and 'I Love You' were released into the wild. Instead, many of the existing viruses, such as 'SpyEye', have become more sophisticated. Virus writers continue to move their historic focus away from Windows computers onto other platforms such as mobile phones and Apple systems.

Weaknesses in their outsource provider's security and poorly configured technology led to a large law firm in London being infected by the 'Conficker' worm. This locked users out of their accounts and so caused very major disruption to the business. It took several days to disinfect the machines and restore normal service. After the breach, the firm implemented new security software and changed its processes to minimise future infections.

A PC at a large financial services firm was infected by a macro virus after an old document was retrieved from archive. The anti-virus software detected and fixed the virus quickly.

Virus writing has been an organised criminal activity for some time now. The Internet gives cyber criminals an international reach; there is an ongoing arms race between them and anti-virus providers. For example, the 'zbot' Trojan has repeatedly been upgraded and a variant is now reported to be capable of intercepting SMS messages.

Routine security monitoring at a medium-sized financial services provider uncovered that unprotected PCs had been infected by the 'qakbot' Trojan. Removing the infection caused very major disruption to the business for several days and took several man-weeks of effort.

Law enforcement authorities are now intervening more often in a more co-ordinated manner, such as the recent action against the 'DNSchanger' Trojan. Government warnings are becoming more common, helping a few respondents to identify infections.

A government warning led a military base to identify infection by malicious software. The malware had been specifically targeted at the organisation. The contingency plan wasn't effective, so it took more than 100 man-days to clean up the systems; there was also some adverse publicity. After the event, changes were made to systems configuration and contingency plans, and some extra security software was implemented.

Interestingly, virus infections occurred in 63% of organisations that don't provide staff with security awareness training, but in only 43% of those that have a programme of continual security awareness.

In a third of small organisations, virus infections were the source of their worst security incident of the year.

Staff at a small technology company in the North-West visited a website that should have been safe but had been infected by spoof antivirus software; it took four hours of effort to clean up the infected PC.

Systems failure and data corruption

Two-thirds of large organisations and half of small ones suffered from systems failure or data corruption. A third of the worst incidents in small businesses were due to this kind of problem.

The systems at a small letting agency in the South West failed, leading to very major disruption to its business for several weeks. A contingency plan was in place but wasn't effective. It took considerable effort to restore the systems. Following the incident, the agency changed the technical configuration of its systems to prevent similar problems in the future.

Hard drive failures and back-up failures were responsible for many incidents. In most cases, these could have been avoided if back-ups were verified.

A large government body suffered major business disruption for several weeks after its RAID storage failed and the back-ups also failed. A specialist disk expert had to be called in to recover and restore the data.

While most of these incidents involved technology issues, people and processes were involved in those that were more serious. There is a correlation between these incidents and how well staff actually understood the security policy. Three-quarters of organisations whose security policy is poorly understood had problems, compared to only a third of those whose policy is well understood. Benefits flow from investing in staff awareness training; only half of respondents with an education programme suffered this type of breach, compared to two-thirds of those who don't train their staff.

Poor awareness of the security policy at a medium-sized media company led to staff accidentally deleting important data. It took several man-days to recover the data.

Six per cent of respondents reported staff sabotage, a similar level to 2010. Surprisingly, some large retailers and financial services firms reported this as a weekly occurrence.

Computer theft and fraud

Computer theft and fraud remain at high levels historically. The proportion of large organisations where staff used computer systems to carry out theft or fraud has doubled over the last two years; more than a third report such incidents. In small businesses, fraud is rarer, but is still several times more common than in 2008.

A small Scottish company suffered adverse media coverage after several thousand pounds were stolen by an employee. The root cause was inadequate staff vetting.

Physical theft of computers by outsiders remains a common cause of breaches. Increasing use of hard disk encryption is reducing the impact of these breaches. In addition, one in eight large companies have had intellectual property stolen by an outsider.

A large government organisation lost more than £500,000 through fraud after a targeted attack on its systems. The investigation took more than 100 man-days and there was some adverse media coverage. After the breach, the poorly designed processes that enabled the fraud were changed.

Figure 26: How many systems failures or data corruptions did the affected organisations suffer in the last year?

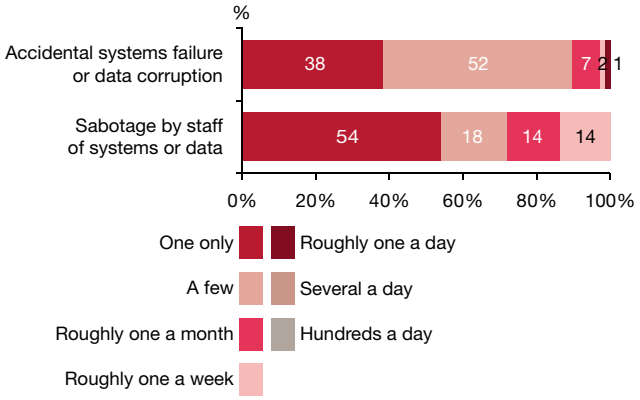


Figure 27: What type of theft and fraud did respondents suffer?

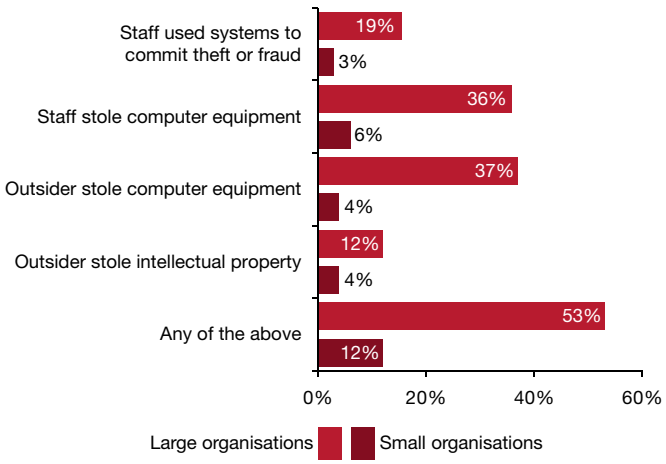


Figure 28: How serious were different types of incidents?

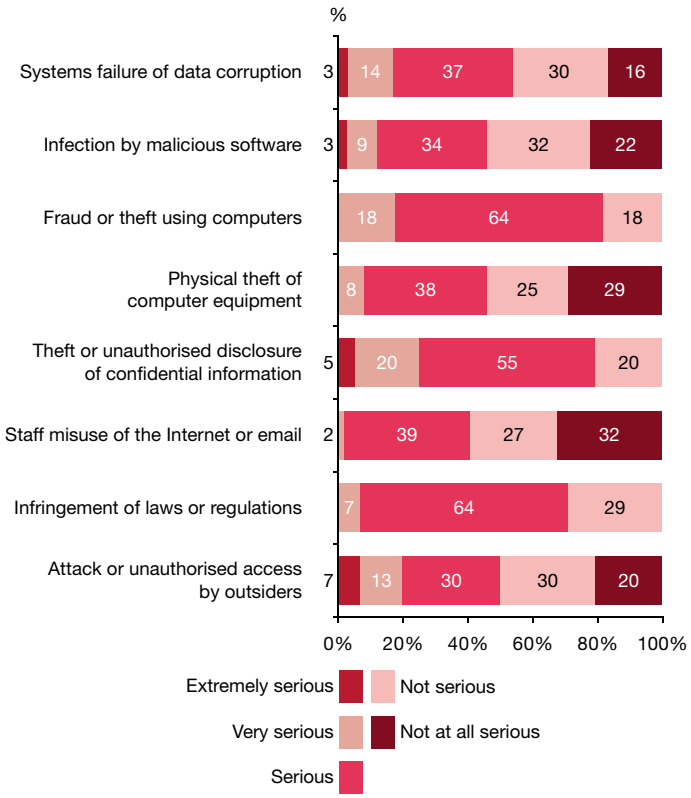


Figure 29: How many respondents had staff-related incidents?

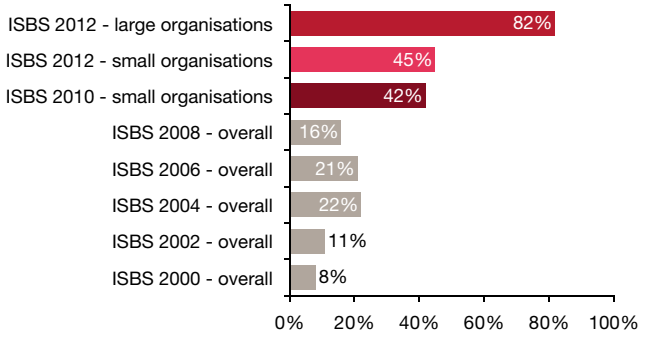


Figure 30: What type of staff-related incidents did respondents suffer?

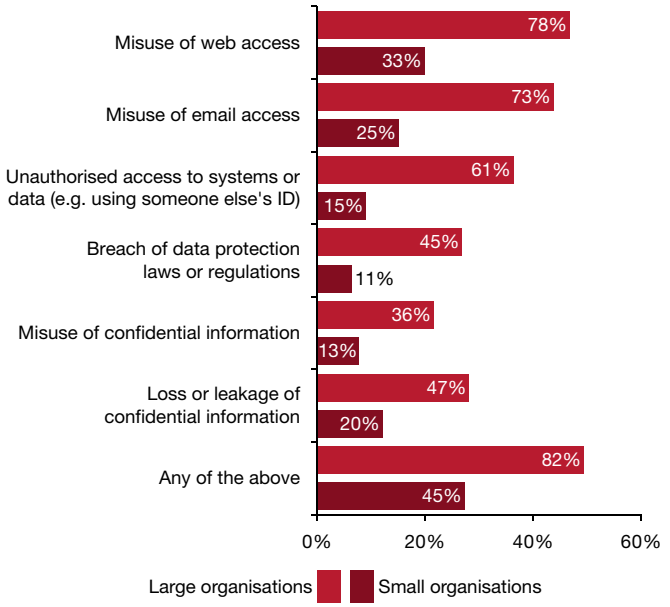
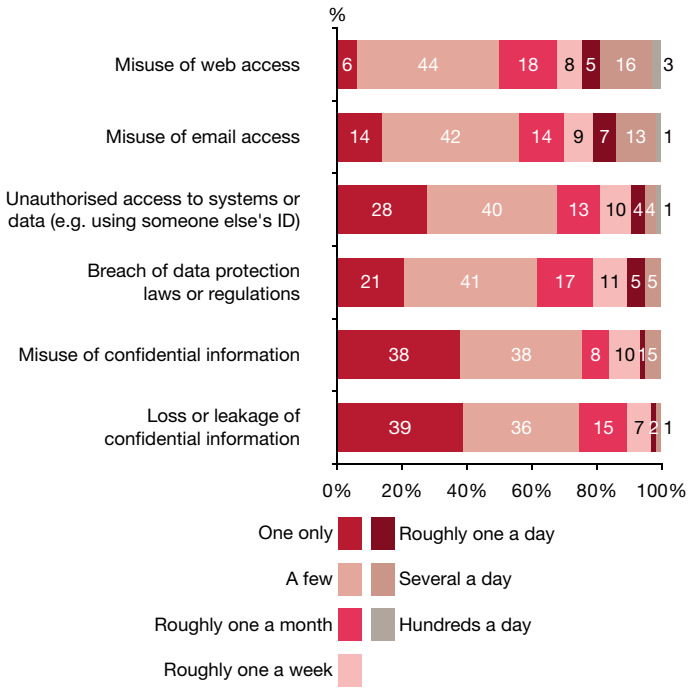


Figure 31: How many incidents did affected organisations have in the last year?



Other incidents caused by staff

Overall, breaches caused by staff were at a similar level to the 2010 survey, which was a substantial increase from 2008. As in the past, large organisations are much more likely to have these breaches than small ones. Four-fifths of large organisations reported such breaches compared to just under half of small businesses.

The biggest single contributor is staff misuse of the Internet and email. This occurred in three-quarters of large organisations and in a third of small ones. Unauthorised access to others' user accounts is at similar levels to two years ago.

Security awareness is a key factor here. Only three-tenths of organisations with a very well understood security policy reported misuse; this compares to four-fifths of those with a poorly understood policy.

Use of monitoring technology is now common, particularly in large organisations, where it detected more than two-thirds of the worst breaches of this kind. Respondents who monitor web usage were twice as likely to report staff misuse of the Internet as those who do not; it is likely, therefore, that the latter aren't identifying all their breaches.

Routine security monitoring at a large transport company picked up staff systematically distributing pornographic material. Disciplinary action followed.

Data protection breaches occurred in almost half of all large organisations; disappointingly, little if any progress has been made in this area since 2010. Clear data ownership appears to be a major factor here. Organisations with very clear data ownership were three times less likely to report a breach than those where data ownership is not clear. Few respondents reported large regulatory fines, but the costs of investigation and follow-up were often substantial.

Security monitoring at a large financial services provider detected some staff breaking the law. The resulting investigation took more than 100 man-days, but resulted in legal action being taken without damaging the firm's reputation. After the breach, the company made sure that the procedures in this area were completely clear to staff.

Staff accidentally lost confidential information at half of large organisations, and actively misused it at a third of them. However, this phenomenon affects small businesses too; one in five reported leakage of confidential data.

Routine control audits at a large financial services provider detected a data loss. Senior management had not placed enough priority on security, which led to poorly designed processes and poor staff awareness of security issues. Human error then caused the breach. It took more than 100 man-days and more than £500,000 to investigate and remediate the breach. There wasn't a contingency plan in place, but after the breach changes were made to policies, procedures and staff training.

Unauthorised access by outsiders

The survey results suggest that UK plc is under a relentless cyber attack. Seven tenths of large organisations have detected significant attempts to break into their networks, the highest level ever recorded in this survey. All sectors were affected. The number of individual attacks has roughly doubled; the median for large organisations is now one attack per week and the mean is ten per day. Attacks on Internet and telecoms traffic remain at four times the level seen in 2008, with the travel, leisure and entertainment sector particularly affected.

One in seven large organisations had been successfully hacked, again a historical high. These breaches are not isolated incidents. Most had detected hackers inside their systems several times during the year. Travel and telecoms companies were most affected; one in four had been penetrated. Since most businesses now share data with their business partners across the supply chain, this makes uncomfortable reading.

A government warning helped an English utility provider to detect that outside attackers were misusing its computer network. It took more than 100 man-days to clean up the network. After the breach, a major security programme took place, including staff training, changes to policies and procedures, deployment of new security software and increased monitoring of third parties' security.

Denial of service attacks are also common; they affected a third of large businesses and nearly half of all telecoms providers. These attacks typically disabled unprotected websites, but sometimes also affected email and IP telephony.

Attackers succeeded in overloading the internal systems at a large financial services provider by bombarding its website with automated quote requests. Insufficient priority had been placed on security in the design of the systems and processes. Fortunately, an effective contingency plan was in place; as a result, while there were some complaints from customers, the damage from the incident was minimised. It did, however, take more than 100 man-days of effort to change the systems and processes to prevent similar attacks in the future.

All sectors reported attackers on the Internet trying to impersonate them; financial services and government bodies were hit most, often reporting "phishing" attacks several times a day.

A government warning alerted a large utility firm to a spear-phishing attack; a foreign nation state was targeting senior management and asking them to divulge confidential data. The company responded by tightening up its technical configuration and training staff on the risks involved.

Customer impersonation and identity fraud remains high (up threefold from 2008) with all sectors affected. In a change since 2010, financial services have overtaken retail; manufacturing remains the least targeted sector. Criminals currently appear to find it easiest to make money by impersonating the customers of banks.

A new question for this survey was whether an outsider had stolen confidential data. Overall, one in eleven respondents reported positively; financial services and utilities providers were the worst affected.

Figure 32: How many respondents were attacked by an unauthorised outsider in the last year?

A high proportion of small organisations did not know whether they had been subject to attempts to break into their network or attacks on their traffic

Figure 33: How many incidents did affected organisations have in the last year?

Figure 34: How many respondents had a serious incident?

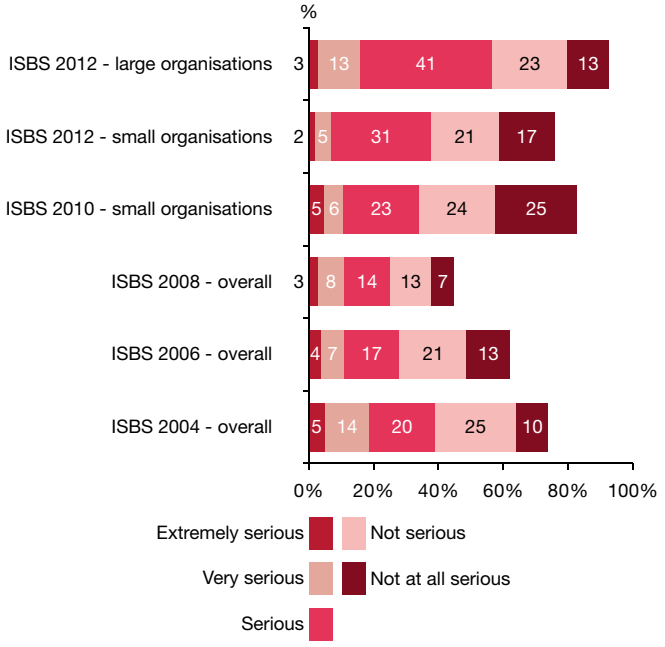
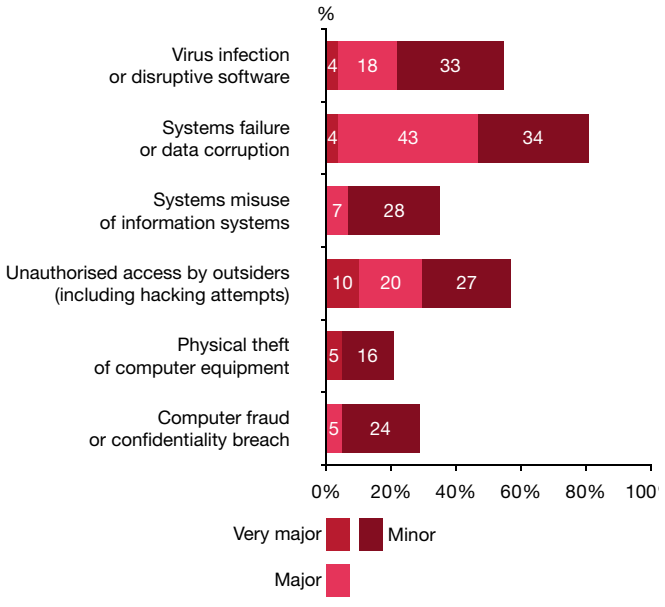


Figure 35: How much disruption to the business did the worst security incident cause?

	None	Less than a day	Between a day and a week	Between a week and a month	More than a month
Very major disruption	44%	1%	2%	1%	0%
Major disruption		8%	9%	2%	0%
Minor disruption		13%	6%	1%	1%
Insignificant disruption		10%	2%	0%	0%

Figure 36: Which incidents were most disruptive to business?



Impact of breaches

Security breaches can have many different types of impact. Direct costs, such as downtime and effort to remediate, are easy to estimate. Indirect costs are harder to determine; a business may be underperforming for many reasons, so any estimate of the reputational impact of a breach is approximate. This survey focuses on measuring the cost of an organisation's worst security breach of the year.

One way of measuring the impact of breaches is a subjective measure of their seriousness. On average, the seriousness of respondents' worst breach of the year has stayed roughly the same as in 2010. In large organisations, the average seriousness has dropped slightly; either they are getting better at reducing the impact or are becoming desensitised.

The most likely types of breach to be serious are loss of confidential data and computer fraud; hacking attacks are most likely to cause an extremely serious incident. In contrast, web misuse and virus infection often led to relatively minor incidents. Travel, leisure and entertainment companies are most likely to have suffered a serious security breach, while relatively few technology companies had one. Extremely serious breaches are most common in the public sector, utilities and retailers.

Business disruption

Downtime from respondents' worst breaches has slightly reduced, to 1-2 days on average. The biggest cause of downtime in 2010 was virus infection; this has fallen back in 2012, with systems failure cited as most likely to cause business disruption. This is not surprising since the last two years have not seen any new worms or virus epidemics on the Internet.

A small London-based financial services company's systems became unavailable for several days after an unknown operating system error caused data corruption. It took longer to fix the problem because there was no contingency plan, so the company put one in place once systems were restored.

External attacks against websites and Internet gateways were also significant. Roughly two thirds caused some disruption.

A small government body in the South-East suffered very major disruption for a day when its website was attacked. It took several man-days of effort to undo the damage.

In total, one in twenty of the worst security breaches led to business disruption for more than a week, with some continuing for more than a month.

Systems failures, hacking attacks and viruses were the main culprits. Interestingly, while regulatory breaches do not cause systems downtime, half of them disrupted business operations in their wake; the investigation distracted senior management and diverted resources from other activities.

A government warning helped a Scottish utility provider to detect deliberate misuse of customer records by a member of staff. The investigation took more than 100 man-days. Afterwards, the technical configuration was changed and additional staff training given.

Using the same basis as previous surveys, the cost of business disruption from the worst breach of the year appears to have roughly halved, to £7,000-£14,000 for small businesses and £60,000-£120,000 for large organisations. This is very similar to the levels seen in 2008.

Incidence response costs

The indirect cost of staff time responding to a breach can easily outweigh its direct cost. For some incidents (such as staff misuse), this time is primarily investigation of what went wrong; building up evidence to support disciplinary or legal proceedings can be particularly costly. For others (such as accidental systems failure), time tends to be spent restoring systems to operation and changing processes so that similar incidents do not recur.

Poorly designed technical configuration allowed staff at a small business in the South-West to misuse its systems. The resulting problem and investigation caused very major disruption for several days. The company didn't have a contingency plan in place; as a result, the breach diverted several man-weeks of effort and cost around £100,000. Legal action was taken against the staff involved.

The time spent to fix breaches was very similar to two years ago. In small businesses, three-fifths of breaches took less than one man-day to resolve; most of the rest needed between two and ten man-days effort and no incidents involved more than 50 man-days. The average cost of this time was £600-£1,500, plus a further £1,000-£3,000 in cash costs. In large organisations, the effort required to deal with breaches was much higher; one in ten breaches took more than 50 man-days to resolve, and only a quarter involved less than a man-day. Large organisations incurred £6,000-£13,000 in time costs, and £25,000-£40,000 in cash costs on average.

Failure to follow change control procedures led to several days of major disruption and customer complaints at a Scottish utility firm after the release of a new version of the booking system. An effective contingency plan was in place, but it still took several hundred thousand pounds and more than 100 man-days to get the systems back up and running. After the incident, procedures were tightened up and new release management software deployed.

Direct financial loss

Direct financial loss includes expenditure such as compensation, replacing stolen assets or fines. This remains rare; only a quarter of breaches involved any direct loss. However, a small number of breaches involved losses in the hundreds of thousands of pounds, including one at a small business. Computer theft and fraud was the biggest cause of direct financial loss. None of the incidents involving infringement of laws or regulations reported any direct financial loss; this suggests fines are not currently a major influence.

A large Internet Service Provider suffered a denial of service attack against an online store. The site was vulnerable because the technical configuration had not been kept up to date. It took several man-weeks of effort to deal with the attack, which caused several hundred thousand pounds of damage.

Indirect financial loss

Losses can also be indirect, for example through the loss of intellectual property or revenue leakage. These are difficult to assess; a competitor may be lucky or use stolen information, and the dip in share price may just be temporary. Unsurprisingly, very few respondents reported any indirect financial loss from their breaches. Human error appears to cause the breaches, with the largest indirect financial losses.

Damage to reputation

Reputation damage from security breaches was limited; three quarters of respondents kept knowledge of their worst incidents internal. However, this may change in the future if the European Union implements a European-wide breach notification directive. Public sector and financial services bodies attracted the worst media coverage, caused by hacking attacks and confidentiality breaches.

Figure 37: How much cash was lost or spent dealing with the worst security incident of the year?

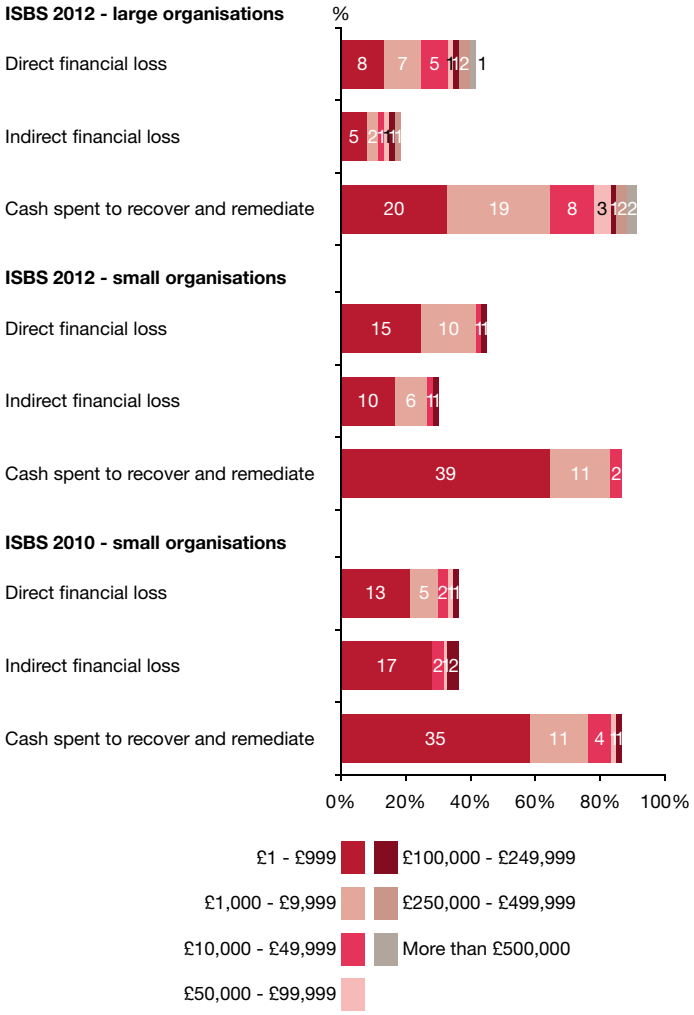


Figure 38: To what extent did the worst incident damage the reputation of the business?

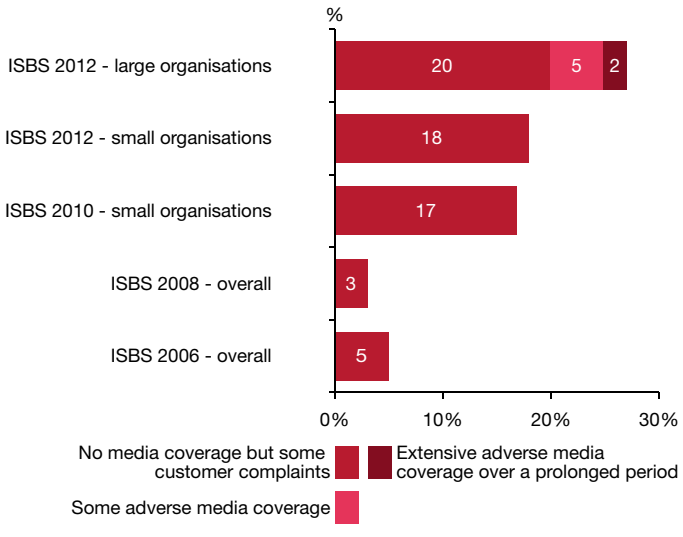


Figure 39: What was the overall cost of an organisation's worst incident in the last year?

	ISBS 2012 - small organisations	ISBS 2012 - large organisations
Business disruption	£7,000 - £14,000 over 1-2 days	£60,000 - £120,000 over 1-2 days
Time spent responding to incident	£600 - £1,500 2-5 man-days	£6,000 - £13,000 15-30 man-days
Direct cash spent responding to incident	£1,000 - £3,000	£25,000 - £40,000
Direct financial loss (e.g. loss of assets, fines, etc.)	£2,500 - £4,000	£13,000 - £22,000
Indirect financial loss (e.g. theft of intellectual property)	£4,000 - £7,000	£5,000 - £10,000
Damage to reputation	£100 - £1,000	£5,000 - £40,000
Total cost of worst incident on average	**£15,000 - £30,000**	**£110,000 - £250,000**
2010 comparative	£27,500 - £55,000	£280,000 - £690,000
2008 comparative	£10,000 - £20,000	£90,000 - £170,000

Figure 40: What type of security incidents do organisations plan for, and how effective are those contingency plans?

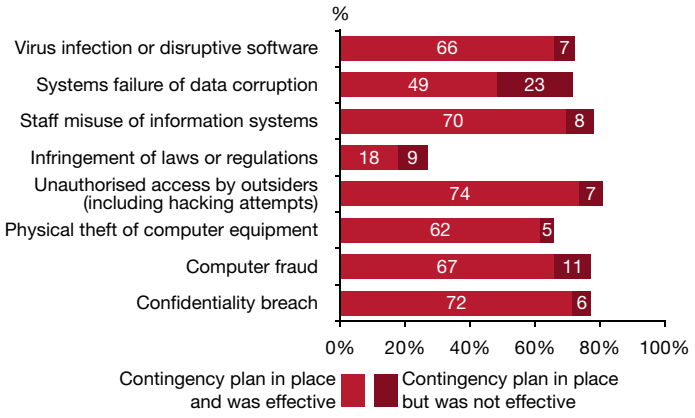


Figure 41: What steps did large organisations take after their worst security breach of the year?

A large telecoms provider suffered from extensive adverse media coverage over a prolonged period after poorly designed processes and technical configuration led to loss of confidential data. No contingency plan was in place to deal with this scenario. As a result, the incident cost more than £500,000 and took several man-months of effort to fix. After the breach, the company embarked on many security improvements, including staff training and vetting, changes to both technology and procedures, and legal and disciplinary action.

Total cost of incidents

The estimated average cost of respondents' worst incident of the year has reduced from 2010 levels towards the levels seen in 2008. For small businesses, the cost is roughly £15,000-£30,000; for large organisations, it's £110,000-£250,000.

Extrapolation of cost data across the whole of the UK should always be treated with caution, especially given the self-select nature of the survey. However, based on the number of breaches and the cost of the worst breaches, we estimate that the total cost of breaches has fallen somewhat from the 2010 peak, but is higher than 2008 levels (particularly for large organisations). Our best estimate of the total cost to UK plc is in the order of several billion pounds per annum.

Contingency planning

Overall, three quarters of respondents had contingency plans in place to deal with their worst incident of the year. This is similar to the levels seen in 2010, and there is little variation between large and small organisations. One blind spot appears to be infringement of laws and regulations, where only a quarter of affected organisations had a contingency plan.

Most contingency plans proved effective. The failure rate here was half that of two years ago. However, a third of contingency plans to deal with systems failure and data corruption didn't work, so frequent testing of plans in this area is prudent.

There is a strong correlation between the effectiveness of contingency plans and the seriousness of breaches. When contingency plans worked, less than half the incidents were serious; when the plans failed, four-fifths were serious.

A school in the Midlands suffered major disruption for several days after hackers targeted its website. There was a contingency plan for such breaches, but it proved ineffective. As a result, it took several man-weeks of effort to restore normal operations. After the breach, the school deployed additional security software.

A large financial services provider suffered extensive adverse media coverage after an attack on its website. The impact was minimised by an effective contingency plan. After the breach, improvements were made to technical configuration and procedures.

Steps taken after breaches varied with the nature of the incident. Additional staff training was most common after staff misuse or confidentiality breaches. Organisations tended to change configuration after systems failures, hacking attacks and virus infections. After the most serious breaches, organisations improved their processes and technology and also trained their people. This reinforces the evidence that the worst security breaches are due to failures in people, process and technology.

Independent reviewers

ASIS International is the largest organisation for security professionals, with more than 37,000 members worldwide including 750 in the UK. The UK Chapter runs dynamic seminars and training days throughout the year, publishes a quarterly newsletter containing articles from some of the country's leading security practitioners and acts as a voice for the security profession, representing members' views at the highest levels. For more information, see www.asis.org.uk

Our mission as **BCS**, The Chartered Institute for IT, is to enable the information society. We promote wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public. See www.bcs.org

Our vision is to be a world-class organisation for IT. Our 70,000 strong membership includes practitioners, businesses, academics and students in the UK and internationally. We deliver a range of professional development tools for practitioners and employees. A leading IT qualification body, we offer a range of widely recognised qualifications.

The Communications Management Association is the UK's premier membership organization supporting businesses delivering services online. It is part of the BCS. Please visit the web site for more information, www.thecma.com

EURIM - The Information Society Alliance *Informing policy for an economically competitive and socially inclusive network society.* EURIM brings together politicians, officials and industry (including professional bodies and trade associations) to help set the agenda for Internet and Information Society policy formation, consultation and scrutiny, remove regulatory and legislative barriers to UK competitiveness and secure value for money in the delivery of online public services. See www.eurim.org.uk

Eskenzi PR is the most respected PR and digital marketing agency in Europe that specialises in IT Security, with offices in the UK, France, Germany and USA. Eskenzi is a prolific, adventurous, creative agency that turns emerging companies into globally recognised industry leaders. For more information, see www.eskenzipr.com

Get Safe Online is a joint initiative between the Government, law enforcement, leading businesses and the public sector. Our aim is to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely and securely. See www.getsafeonline.org

ICAEW's IT Faculty provides products and services to help its members make the best possible use of IT. It represents chartered accountants' IT-related interests and expertise, contributes to IT-related public affairs and helps those in business to keep up to date with IT issues and developments. The faculty also works to further the study of the application of IT to business and accountancy, including the development of thought leadership and research. For more information about the IT Faculty please visit icaew.com/itfac

The **UK ISO/IEC 27001 User Group** is the UK Chapter of the International ISMS User Group. It exists to promote awareness of and share good practice in relation to ISO/IEC 27001 and information security management systems. For more information, see www.iso27001usergroup.co.uk

Information Systems Audit and Control Association (ISACA), is an international body that has been in existence since 1969 (with 100,000 international members). The London Chapter, (the first in the UK), was established in 1981, other UK Chapters now include Northern England, Central England, and Scotland, and there is also an Ireland Chapter. The London Chapter has over 2,500 members who come from a wide cross-section of business including the accountancy and information systems professions, central and local government, the banking, manufacturing and service sectors and academia. See www.isaca.org.uk

The Information Security Awareness Forum is an umbrella organisation of around 24 professional bodies. Members include the ISSA, BCS, IET, EURIM, CMA, Get Safe Online, (ISC)2, IISP and SASIG. The aim of the forum is to develop a co-ordinated cross-industry / cross-institution approach for delivering security awareness messages to large corporations, SMEs and individuals. See www.theisaf.org

The **ISF** is the world's leading authority on information risk management. A not-for-profit organisation, we supply authoritative opinion and guidance on all aspects of information security. We deliver practical solutions to overcome the wide-ranging security challenges that impact business information today. See www.securityforum.org/

The Information Systems Security Association (ISSA) is a not for profit, international organisation of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. See www.issa.org/

(ISC)² is the largest not-for-profit membership body of certified information security professionals worldwide, with over 80,000 members in more than 135 countries. Globally recognised as the Gold Standard, (ISC)² issues the CISSP and related concentrations, CSSLP, CAP, and SSCP credentials to qualifying candidates. More information is available at www.isc2.org.

IT Governance Ltd provides end-to-end cyber-security management solutions to help clients globally protect critical and sensitive information. We are the single source provider for comprehensive information, advice, books, tools, training and consultancy for information security, IT governance, risk management and compliance. Visit our website www.itgovernance.co.uk to learn more about our products and services.

The **Security Awareness Special Interest Group** (www.thesasig.com) is a subscription free quarterly networking forum open to those who have an interest in, or a responsbility for, raising awareness about security within their organisations.

www.pwc.com

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

Design: ML1-2012-03-01-11 49-VF