infosecurity EUROPE

PRICEWATERHOUSECOOPERS

Information Security Breaches Survey 2010

technical report

Commissioned by:

This report was commissioned by Infosecurity Europe and launched at Infosecurity Europe on 28 April 2010 at Earl's Court, London.

Infosecurity Europe, celebrating 15 years at the heart of the industry in 2010, 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 five 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

Reed Exhibitions is the world's leading events organiser, with over 2,500 employees in 35 offices serving 44 industries worldwide. We organise a wide range of events, including trade and consumer exhibitions, conferences and meetings. We organise over 440 events in 36 countries. Over 6 million active event participants attended our events in 2009. We are part of Reed Elsevier Group plc, a FTSE-100 company and world-leading publisher and information provider. For further information, please visit www.reedexpo.com

Written by:

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services to build public trust and enhance value for our clients and their stakeholders. More than 163,000 people in 151 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

Our security global practice has more than 30 years experience, with over 200 information security professionals in our OneSecurity UK network, and 3,500 globally in 151 countries. 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 2009.

"PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) or, as the context requires, the PricewaterhouseCoopers global network or other member firms in the network, each of which is a separate and independent legal entity.

Acknowledgement:

Infosecurity Europe and PricewaterhouseCoopers LLP would like to thank the department for Business, Innovation and Skills (BIS) 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 (BIS) is building a dynamic and competitive UK economy by: creating the conditions for business success; promoting innovation, enterprise and science; and giving everyone the skills and opportunities to succeed. To achieve this it will foster world-class universities and promote an open global economy. BIS - Investing in our future. For further information, see www.bis.gov.uk.

Introduction

Since the early 1990s, every couple of years the department for Business, Innovation and Skills (and its predecessor departments, the DTI and BERR) has commissioned a survey on information security practices and incidents in the UK. The most recent such survey was carried out by PwC and published in April 2008. BIS has decided not to fund further surveys, although the benefits of such information gathering is being reviewed within Government. However, recognising the value of the survey results to the information security community and their continuing support, BIS has agreed that Infosecurity Europe and PwC can carry out this survey in 2010.

This year's survey results show that the business environment is changing rapidly. Social networks and software as a service have moved Internet use beyond websites and email, creating new vulnerabilities. Criminals are also adapting their techniques and cybercrime is becoming more common. After falling for the last few years, the cost of security breaches appears to be rising fast. The most dramatic growth is in external attacks which have trebled since 2008.

So has the improvement reported in 2008 given way to complacency? Has the economic downturn reduced expenditure on controls? The short answer is 'no'. More complex threats have emerged over the last two years. Technical controls are no longer, in isolation, enough to protect organisations. A combination of people, technology and process is now required. To succeed in today's environment, organisations need to think several moves ahead of the criminals. Staff and customers need to be more aware of security threats. Collaborative working practices offer real opportunities, but create a demand for assurance across the supply chain.

The survey has, once again, benefitted from the independent reviewers who have worked with us. Their different perspectives and points of view have helped ensure the survey is balanced and focused on the most important findings. We thank all the reviewers for their time and insight. We would also like to thank all the respondents who collectively donated several man-weeks of time to make this report possible.

Survey approach

For the first time, ISBS 2010 was completed online on a self select basis, similar to other security surveys around the world. The respondents were typically security professionals. In total, 539 organisations responded. The number of large respondents is comparable with previous surveys (giving a margin of error of +/-6% at 95% confidence). There were, however, fewer small and medium-sized respondents (giving a margin of error of +/-8%); in addition, the self select basis is likely to have biased the respondents towards the subset of SMEs that have access to security professionals. As in the past, we have presented the results for large and small organisations, and explained in the text any differences seen in the medium-sized organisations.

Respondents came from all industry sectors. Compared with previous years, more came from the public sector (roughly a quarter), reflecting the increasing focus on security in the wake of the HMRC incident.

To enable trend analysis with previous surveys, most of the questions asked were the same as in the past. However, to reflect the changing nature of electronic commerce, we added some new questions in the areas of data loss prevention, virtualisation and social networking.

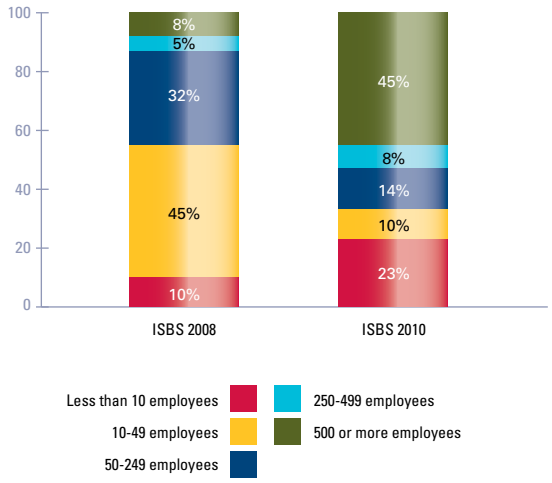
As with any survey of this kind, we would not necessarily expect every respondent to know the answers to every question. For presentation of percentages, we have consistently stripped out the Don't Knows. If the proportion of Don't Knows was significant, we refer to this in the text.

Chris Potter
Information security assurance partner

Andrew Beard
Information security advisory director

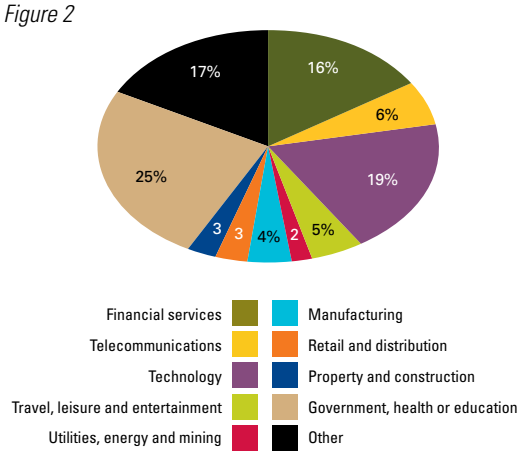
How many staff did each respondent employ in the UK?

Figure 1



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

Figure 2



Business change and media profile keep the focus on security

The business environment is changing rapidly. Organisations are becoming increasingly interconnected through the Internet. Social networks and externally hosted software services are moving Internet use beyond just websites and email. Wireless networks and Voice over IP telephony have now become mainstream.

34%	are critically dependent on externally hosted software services accessed over the Internet.
32%	consider use of social networking sites to be important to their business.
85% *(42%)*	use a wireless network.
47% *(17%)*	use Voice over IP telephony.

2008 comparatives shown in brackets.

Given the recession and the associated pressure on costs, one might have expected security expenditure to have dropped. In contrast, the amount small respondents are spending is the highest level ever recorded in this survey.

The changing environment, combined with the amount of media coverage, has kept security high on management's list of priorities.

77% *(81%)*	believe their senior management give a high or very high priority to information security.
90% *(94%)*	maintained or increased their security expenditure in the last year.
10% *(7%)*	of IT budget is spent by small respondents on their security, on average.

2008 comparatives shown in brackets.

Unfortunately, as in the past, security controls appear to be lagging behind the use of new technology.

New vulnerabilities are being exploited

The changing business environment is creating new vulnerabilities. Criminals are adapting their techniques exploiting the vulnerabilities; as a result cybercrime is becoming more common. After falling for the last few years, the number and cost of security breaches appears to be rising fast.

As in the past, large organisations (>250 staff) are the most likely to suffer security breaches. The number of breaches and the cost of individual incidents are up significantly on 2008 levels.

92% *(72%)*	of large respondents had a security incident in the last year.
45 *(15)*	is their average (median) number of breaches in the last year.
£280k - £690k *(£90k - £170k)*	is the average cost of a large respondent's worst incident of the year.

2008 comparatives shown in brackets.

Small organisations (<50 staff) are also suffering. Nearly twice as many respondents were affected as in 2008.

83% *(45%)*	of small respondents had a security incident in the last year.
14 *(6)*	is their average (median) number of breaches in the last year.
£27.5k - £55k *(£10k - £20k)*	is the average cost of a small respondent's worst incident of the year.

2008 comparatives shown in brackets.

An indicative estimate of the overall cost to the UK is in the order of several billion pounds a year. Respondents are pessimistic about the future, with only 16% expecting fewer security incidents next year.

New threats increase the demand for assurance

A new wave of Internet worms (such as Conficker) has taken over PCs, which are then used to send spam or attack other organisations. Malicious software probes the defences or organisations and opens doors for hackers to extract confidential data.

62% *(21%)*	of large respondents were infected by a virus or malicious software in the last year.
61% *(31%)*	of large respondents have detected a significant attempt to break into their network in the last year.
15% *(13%)*	of large respondents have detected actual penetration by an unauthorised outsider into their network in the last year.
25% *(11%)*	of large respondents have suffered a denial of service attack in the last year.

2008 comparatives shown in brackets.

Small respondents report similar rises in external attacks. For example, three times as many of them were infected by viruses as in 2008.

These attacks are creating a demand for assurance across the supply chain. Mandatory security requirements are becoming more common. More organisations need to comply with standards such as PCI and government minimum measures. However, at the moment, organisations do not appear well prepared to meet the wider demands for assurance. In particular, organisations that use third party services often do not demand the same level of assurance that their customers are demanding from them.

68%	of large respondents have been asked by their customers to demonstrate their compliance with security standards.
61%	of large respondents ensure their contracts with third party providers include security provisions.
27%	of large respondents obtain reports from third party providers on security breaches that affect their data.
17%	of respondents with highly confidential data at an external provider ensure that data is encrypted.

Effective threat protection requires the right security behaviour

The rise in incidents is due to the more complex threats that have emerged over the last two years. Technical controls are no longer, in isolation, enough to protect organisations. A combination of people, technology and process is now required.

This is particularly the case for large respondents who have experienced increasing numbers of serious confidentiality breaches.

46%	of large respondents had staff lose or leak confidential data.
45%	of confidentiality breaches were very serious or extremely serious (compared with only 15% of other types of breaches).

It is encouraging that the number of organisations with a formal security policy is higher than ever. However, a security policy is only useful if staff understand and apply its contents. Getting the message out across a large organisation is a big challenge. Only one in five believe their policy is well understood.

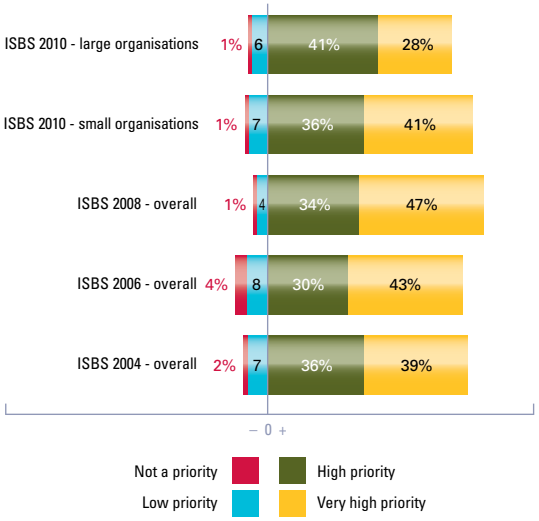
90% *(88%)*	of large respondents have a formally documented security policy.
68% *(65%)*	of large respondents have implemented ISO 27001 (partially or fully).
52% *(26%)*	of large respondents provide staff with ongoing education on security.
30%	of large respondents believe responsibilities for data ownership and protection are very clear.
19%	of large respondents monitor what their staff post on social networking sites.

2008 comparatives shown in brackets.

Given the rising level of breaches seen in the survey it is more critical than ever that organisations raise security awareness among all their staff. Business needs to become an effective first line of defence, not just a victim of the growing cybercrime threat.

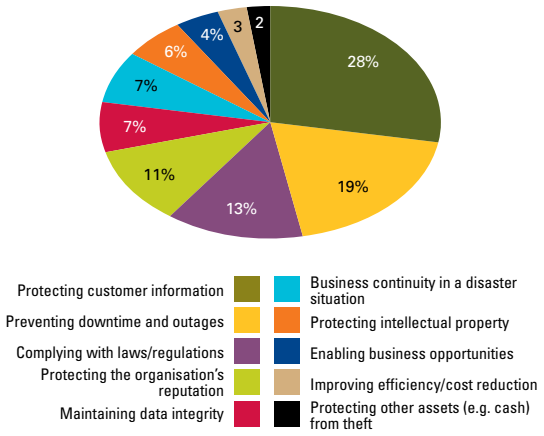
How high a priority is information security to top management or director groups?

Figure 3



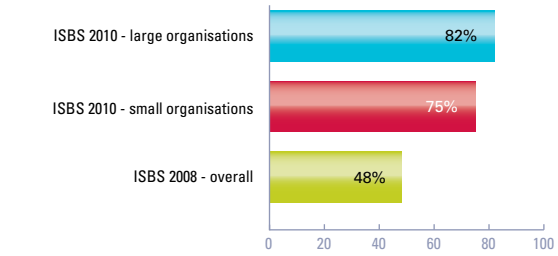
What is the main driver for information security expenditure?

Figure 4



How many respondents carry out security risk assessment?

Figure 5



Attitudes to information security

The need to set the tone at the top is a common cry from information security professionals. 77% of top management give a high or very high priority to security, similar to levels seen over the last decade. For the first time, small respondents report security is a higher priority than large respondents.

Government, financial services and technology organisations assign the highest the priority to security; they are twice as likely to assign a high priority as the worst sector, property and construction. Retailers are another outlier, with over a quarter indicating that their security is a low priority.

Protecting customer information remains the most important driver for security. Preventing downtime and outages has increased in relative importance, perhaps in the wake of the recent wave of Internet worm attacks. Protecting the organisation's reputation and maintaining data integrity have, in contrast, fallen somewhat in relative importance.

For one in eight organisations, complying with laws and regulations is now the biggest driver of expenditure. In the financial services and government sectors it was the second highest driver after protecting customer information. In contrast, compliance with regulation appears highly unlikely to drive security in the retail and manufacturing sector. Small organisations also are much less influenced by compliance than large ones.

Organisations that hold critical or confidential information with third party providers are particularly concerned with protection of customer information. This was also the case with organisations whose senior management place a very high priority on security. In contrast, organisations that place a low priority on security tend to be most concerned with preventing downtime and outages.

Organisations are more likely to perform risk assessments than in previous years. This is probably due to increased awareness of risk-based standards, such as ISO 27001. Four-fifths of large organisations have assessed security risks in the last year. Small companies are not far behind, but a quarter still base their priorities on perception, rather than formal risk assessment.

The utilities sector is most likely to have a completed a risk assessment; over 90% had done so. Other sectors with high levels of oversight and regulation (e.g. financial services, telecoms and government) are also more likely to have completed a risk assessment. This contrasts with the property and construction sector, where nearly half the respondents had not performed one.

Some of the drivers for security expenditure are more risk informed than others. Organisations that had assessed their security risks were twice as likely to consider protecting customer information or the organisation's reputation most important. Organisations that had not were twice as likely to consider protecting other assets from theft or business continuity in a disaster their most important driver.

Some organisations are not converting senior management support for information security into action. One in seven organisations that give a high priority to security do not have a formally documented information security policy. Even when it is a very high priority, 8% do not have a policy.

An increasing trend is the convergence of physical and information security management. Whereas in the past physical assets needed the bulk of protection effort, today information assets demand at least equal attention.

Changing environment

The rate of adoption of newer technologies has accelerated over the last two years. As a result, most respondents now use wireless networking, remote access and Voice over IP telephony (VoIP).

85% of small respondents use wireless networks, more than double the use in 2008. Perhaps because they have already invested heavily in dedicated fixed wire technology, slightly fewer large organisations have wireless networks. Organisations in the technology and communications sectors are most likely to make use of wireless networking. Financial services seem to be the late adopters; only half using the technology.

The number of organisations providing staff with remote access to their systems has increased; nine-tenths of large companies now do this. Utilities, telecoms and financial services companies are most likely to allow remote access; retailers are least likely.

VoIP adoption has accelerated, with adoption rates up three times on 2008. Telecoms and financial services tend to be early adopters, while retail and leisure companies appear the slowest to implement VoIP.

Virtualisation appears widely adopted, especially among large organisations. The lack of standard definition for virtualisation may, however, partially account for the high apparent adoption rates. The early adopters are telecoms and utilities, while very few retailers have deployed this technology. Some respondents reported issues with its implementation.

A physical server was corrupted during its virtualisation. The server was rebuilt from backup, but service levels were compromised for several hours.

As organisations look to reduce the cost of their IT, providers are increasingly offering hosted business applications that are accessed over the Internet. These are collectively termed Software as a Service (SaaS), and form part of what is often referred to as cloud computing. Over three-quarters of organisations use externally hosted solutions; of these, 44% are entrusting critical services to third parties.

The most common externally hosted services are corporate websites and email, but nearly a quarter also use third parties for payment and payroll processing. All sectors are using externally hosted solutions, but government is least likely to release control of critical services.

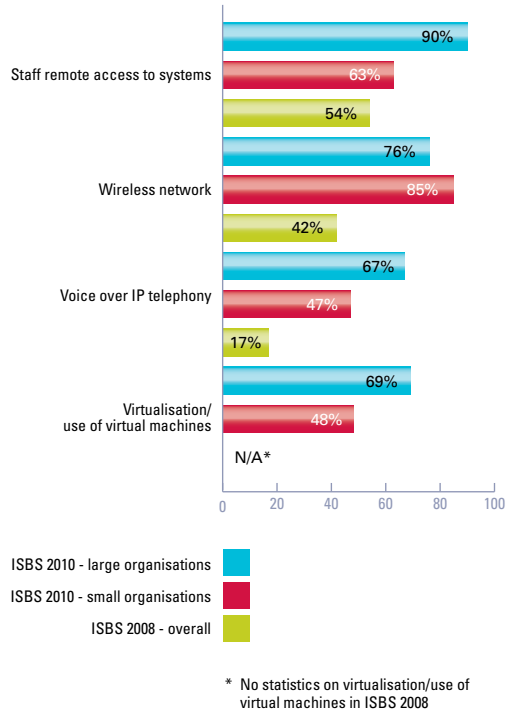
Social networking is also starting to change the way in which organisations conduct business. Traditionally organisations have tried to restrict and monitor recreational use of the Internet. That approach is now beginning to change; nearly a third of organisations now consider social networking to be important to their business. Travel and leisure companies are at the forefront of use of social networking; half of them consider it important to their business.

Putting all these trends together, organisations are becoming increasingly interconnected through the Internet. New services are extending electronic commerce beyond the first wave uses that have dominated the last decade, namely email and websites.

Previous survey results have shown that deployment of effective controls tends to lag behind the more rapid adoption of new technologies. The nature and number of incidents reported this year suggest this trend continues.

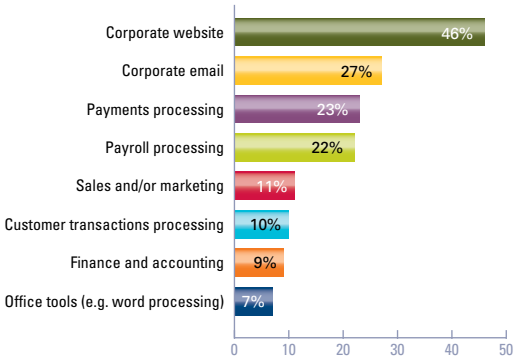
What technologies are respondents using to enable their business?

Figure 6



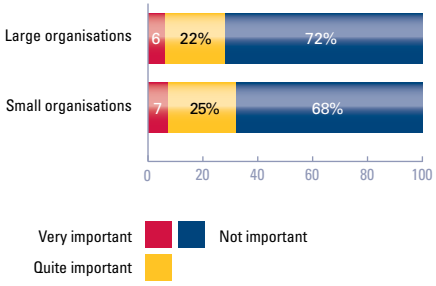
Which business processes have respondents outsourced to external providers over the Internet?

Figure 7



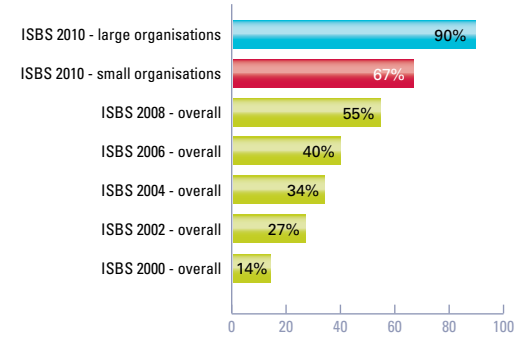
How important is the use of social networking sites to the respondents?

Figure 8



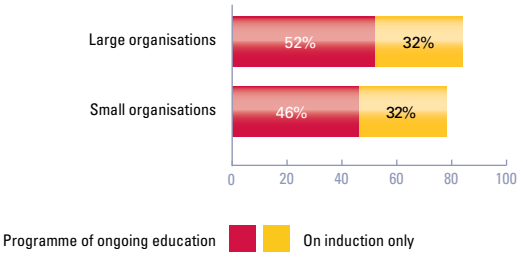
How many respondents have a formally documented information security policy?

Figure 9



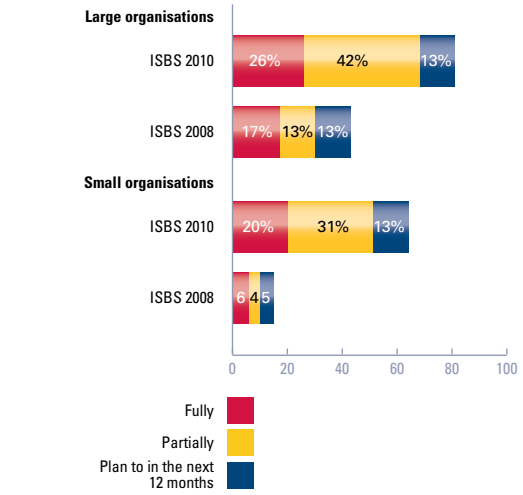
How do respondents ensure staff are aware of security threats?

Figure 10



How many respondents have implemented ISO 27001?

Figure 11



Security culture

The changing business environment increases the challenge of protecting information assets. Organisations cannot meet this challenge by technical controls alone. It is, therefore, encouraging that the number of organisations with a formal security policy is higher than ever.

Regulated sectors are the most likely to have documented their security policy. Utilities lead the way; nearly all of them have a defined and documented policy. The financial services and government sectors are close behind, with more than nine-tenths having a policy. Property and retail companies are least likely to have documented their policy.

More respondents than ever appear aware of the ISO 27001 information security standard. Two-thirds of large respondents have implemented ISO 27001 at least partially, double the level two years ago. As in the past, fewer small respondents have adopted the standard. The self-select basis of the sample this year means that the apparent increase for small respondents is unlikely to be representative of the population as a whole.

A security policy is only useful if staff understand and apply its contents. Small companies appear confident of this; more than half the respondents believe it is well understood, versus one in eight who feel staff understanding is poor. Getting the message out across a large organisation is a bigger challenge. Only one in five believe their policy is well understood, versus three-tenths who believe it is poorly understood.

There is a strong correlation between the importance senior management place on security and how well staff understand their security policy. Staff have a very or quite good understanding in more than nine-tenths of organisations that place a very high priority on security. In contrast, staff have a poor understanding in more than seven-tenths of organisations that give security a low priority.

Security policy is an important weapon in the information security armoury. However, on its own, it rarely improves staff awareness of the threats that organisations now face. It is often said that security is everyone's responsibility; a lack of awareness among staff, therefore, reduces the strength of the first line of defence.

Staff at a London educational institution replied to a phishing email. This resulted in spammers sending over 100,000 emails from the compromised accounts, and to the organisation's mail servers being blacklisted around the world.

Organisations know they need to raise awareness. Four-fifths include information security in their induction programme or as part of ongoing education. However, a third rely on induction alone to educate staff about security threats; a further fifth make no attempts to raise staff awareness. Financial services and telecoms companies are leading the way, while property companies are least likely to provide training.

Staff at a charity broke data protection laws; they were trying to be helpful on the phone but ended up giving out personal details that they were not authorised to provide.

Those organisations that invest in ongoing programmes of security education are rewarded by staff with a clearer understanding of security. They are three times as likely to have a well understood security policy as those organisations without any awareness initiatives; they in turn are five times as likely to have a poorly understood security policy. Induction training tends to increase the chance of having a quite well understood policy, but is insufficient to contribute to a good level of understanding.

Investing in security

Despite the economic downturn average spending on information security continues to grow. For small respondents average expenditure is now nearly 10% of IT budget; the highest level ever recorded by this survey. Average expenditure in large respondents remains at around 6% of IT budget, consistent with the levels seen in past surveys.

Information security expenditure is not always allocated to IT budgets and organisations differ in their interpretations of what constitutes security spending. For these reasons, benchmarking in this area should be considered indicative rather than conclusive.

Regardless of where security expenditure is allocated, most respondents have spent more this year than last. Nearly half of all large organisations have increased information security spending in the last year; in contrast, only 11% have spent less. Three times as many small respondents have increased their expenditure as have cut back. It is encouraging that companies are not taking a short term view on the security costs, despite the depth of the recession over the last year.

Security expenditure appears to be rising across all industry sectors, but the increase is highest in government; more than half in this sector have increased expenditure and only 6% have reduced their spending. This level of investment reflects high profile incidents in the last two years and subsequent Cabinet Office mandatory minimum security measures.

Organisations also seem to spend more in response to serious security incidents. Three-fifths of respondents that had suffered an extremely serious incident increased their security spending. Among those that had not suffered a serious incident, just over a third increased their expenditure. The seriousness of incidents experienced appears to have less impact on decisions taken to reduce security expenditure.

The priorities set by senior management clearly influence expenditure. Where they assign a very high priority to information security, respondents spend 13% of their IT budget on security; this is three times the amount spent by those with a low priority on security. Respondents that have carried out risk assessments spend more on security (8% of IT budget) than those that have not (5% on average). These gaps have widened since 2008.

As in 2008, the average expenditure figures disguise a wide range of responses. Roughly one in seven respondents spend less than 1% of their IT budget on information security, down from one in five in 2008. At the other end of the scale, one in twelve spend more than 25% of their IT budget on security, up from one in twenty in 2008.

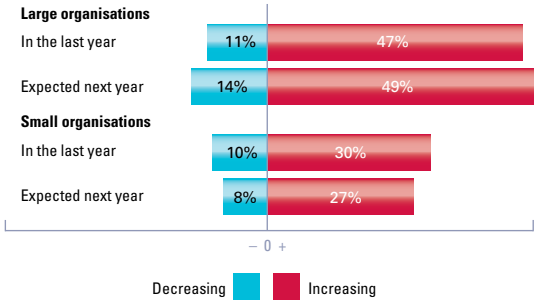
There is a strong correlation between past and future expenditure. Two-thirds of those who increased their expenditure last year plan to increase it again this year. This compares with only a quarter of those who reduced their expenditure last year.

Financial services organisations are most likely to spend more next year; in contrast, retailers are least likely to spend more next year. Even here though, few organisations are planning to reduce spending – the vast majority intend to maintain spending at current levels.

Three-fifths of respondents that expect more security incidents in the future plan to spend more in the next year. This compares with only one fifth of respondents who expect fewer incidents.

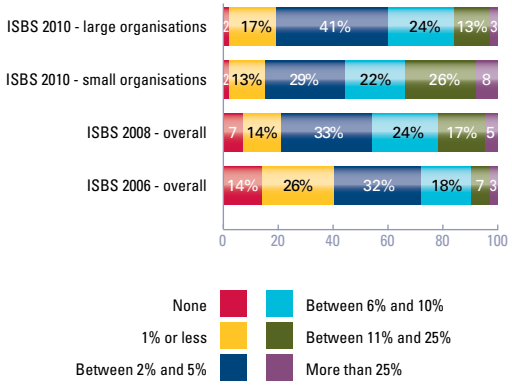
How is information security expenditure changing?

Figure 12



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

Figure 13



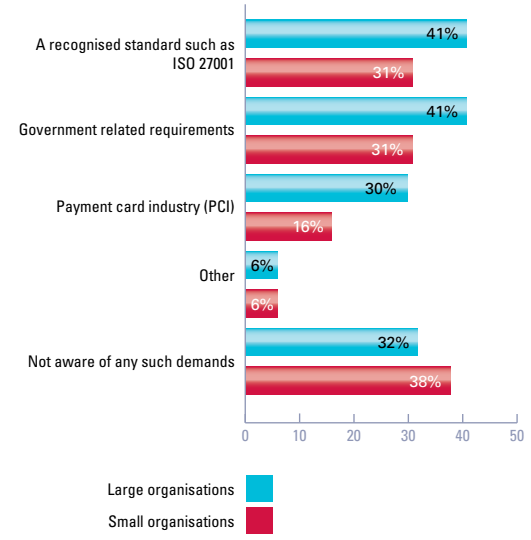
Which sectors spend most on security?

Figure 14

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 9%)	Above Average (more than 9%)
High (more than +40%)	-	Government, health or education	-
Average (between +20% and +40%)	Utilities, energy and mining	Financial services, Telecommunications Travel, leisure and entertainment, Retail and distribution, Other	Technology
Low (less than +20%)	Property and construction	Manufacturing	-

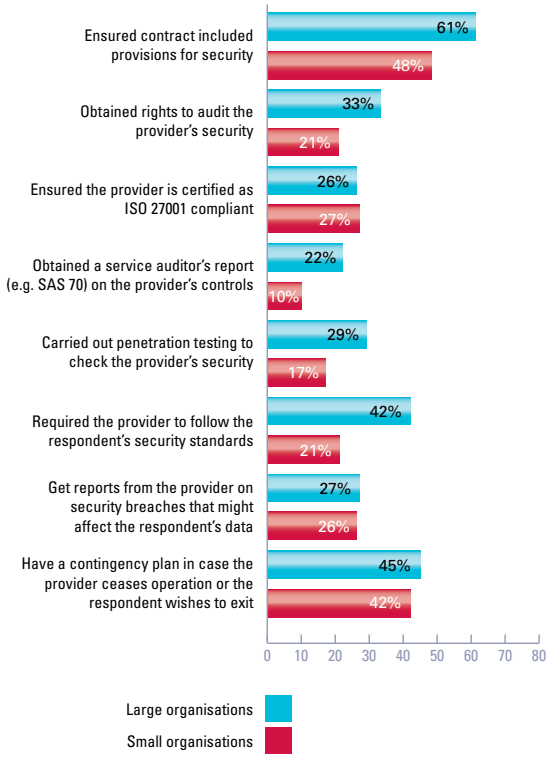
What standards or guidelines have respondents' customers required them to comply with?

Figure 15



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

Figure 16



Demand for assurance

The business environment has become increasingly inter-connected, with customer data being shared more and more across the supply chain. Three-quarters of respondents are now using externally hosted solutions for some part of their business. At the same time, customers are increasingly concerned about data protection. Organisations are increasingly required to demonstrate compliance with information security standards or guidelines.

An insurance company had outsourced some services to a third party. Unfortunately, staff at the service provider fraudulently created a policy to obtain money by deception.

ISO 27001 is becoming a common standard for compliance; two-fifths of large organisations have been asked by their customers to comply with the ISO. Demand is highest in the telecommunications sector, where two-thirds need to comply. Despite having their own sector specific standards, two-fifths of financial services and a third of government organisations are also being asked to comply with ISO 27001. The implication is that ISO 27001 is increasingly becoming the lingua franca for information security.

Requests for compliance with Payment Card Industry (PCI) security standards are also common. Demand is low in property, manufacturing and government organisations; elsewhere, it is spread evenly across business sectors. This reflects increasingly widespread adoption of online card payments.

Government related standards are, not surprisingly, most prevalent within public sector organisations; three-fifths have been asked to comply with government related standards. Half of all telecoms providers and two-fifths of technology companies have also been asked to comply. This reflects government's extensive use of third parties, in particular for computing and networking.

Other standards customers have requested include FSA guidelines, Sarbanes-Oxley or SAS 70 reporting, and US government standards (NIST 800-53). In addition, of course, companies need to comply with the Data Protection Act, and the compliance regime for this has recently been tightened.

A particular challenge organisations face when providing customers with assurance is data ownership. Responsibility for critical data ownership and protection is very clear in only 30% of large organisations; in 28%, it is very unclear.

Organisations are also taking action to gain comfort over security arrangements with their own external suppliers. The most basic discipline is to include security provisions in contracts with their external providers. It is, therefore, a concern that two-fifths of large organisations are failing to do this. There is some correlation between the confidentiality of information held by third parties with the inclusion of security clauses in contractual terms. However, a quarter of organisations whose external providers host highly confidential information do not have security provisions in their contracts.

A majority of respondents believe that their security has neither improved nor deteriorated as a result of using external services. A quarter believe it has improved, compared with only one in ten who believe it has deteriorated. Audit rights, ISO compliance, SAS 70 reports and breaches reporting appear to increase confidence levels the most. However, given these measures are not widely adopted, it seems likely that some organisations have a false sense of security. It is also a particular concern that the confidentiality and criticality of the service has little bearing on the measures adopted to ensure security and continuity.

Preventing data leakage

Data leakage has become an increasingly hot topic over the last two years. The response has been increasing adoption of strong authentication and encryption. Two factor authentication techniques are now in use for some systems at 74% of large respondents. Utilities, telecoms and financial services are the early adopters here.

In ISBS 2008, website transactions, wireless transmissions and staff remote access were normally encrypted. Since two years ago, there has been a big increase in hard disk encryption, particularly on laptops. USB encryption levels have also increased threefold compared with 2008. However, there remain a surprising number of organisations that are not enforcing these basic disciplines.

A charity infringed data protection laws when it disposed of an old computer without wiping the hard drive. The staff member concerned was blasé, saying he had deleted the files and trusted the person to whom he had sold the computer.

ISO 27001 and PCI appear more potent drivers for the use of encryption than government requirements. PCI, in particular, is driving more encryption of website transactions and sensitive data fields in databases. However, organisations that need to meet government requirements are more likely to encrypt data transfers and removable media. It seems that organisations will respond to specific requirements mandated by government; however, where requirements are less explicit, adoption of good practice is lower.

Technology companies are most likely to encrypt backups. This sector is often an early adopter of new techniques; the historical recovery challenges associated with encrypted backups are progressively being overcome.

A courier carrying a large financial services provider's backup tapes was robbed. This led to several man-weeks of investigation to check that the data had not been misused.

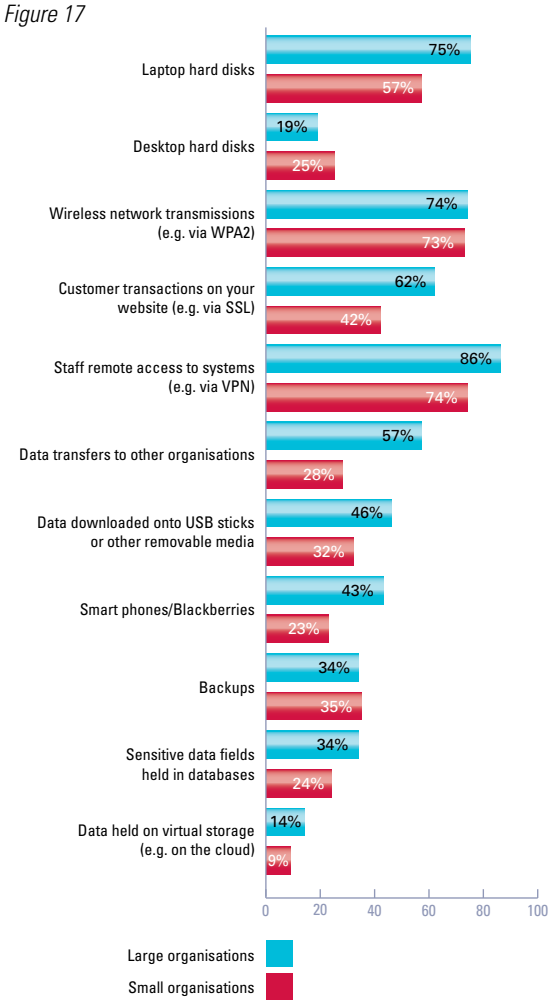
Very few organisations are encrypting data held on virtual storage, including the 'cloud'. Worryingly, only 17% of those with highly confidential data at external providers ensure that it is encrypted. Virtualisation and cloud computing seem to be set to follow the trend, established over the last decade, of controls lagging behind adoption of new technologies. Given the increased criticality and confidentiality of information held on virtual storage organisations need to respond quickly to close this control gap.

Staff postings to social networking sites pose a new data leakage risk. Yet, at the same time, social networking is increasingly important to businesses. Organisations are reassessing their approach to controlling staff access to the Internet. The trend, established between 2006 and 2008, of allowing more staff to access the Internet has been reversed. Nearly half of large organisations now restrict which staff can access the Internet; less than a third did so in 2008. Manufacturing and utilities organisations are most likely to restrict access; roughly seven-tenths do so. In contrast, less than a third of technology organisations restrict who can access the Internet.

Organisations want to allow effective use of the Internet, but reduce inappropriate use. Use of software to block access to inappropriate websites is slightly up on two years ago. Web access logging and monitoring is relatively static. Some sectors, such as financial services and telecoms, are close to full adoption; others, such as retail, lag behind. However, more sophisticated use is being made of these tools than in the past. Organisations are one and a half times as likely to monitor postings to social networking sites if social networking is considered very important to their business.

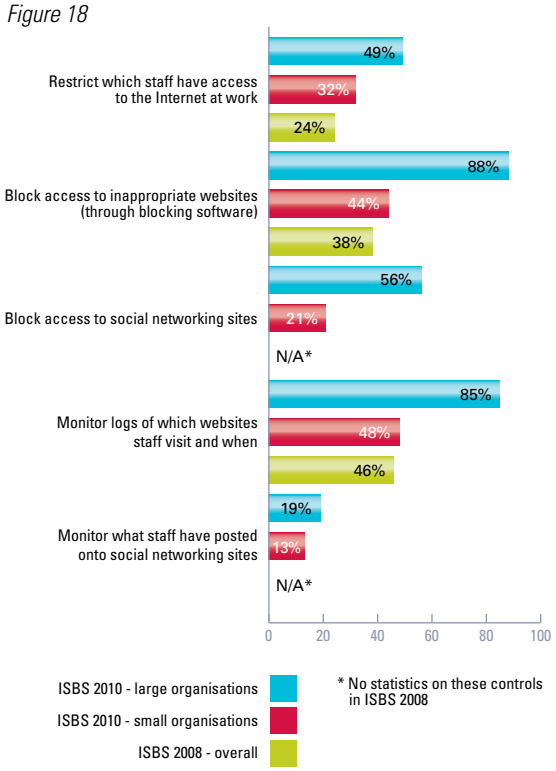
What data types do respondents encrypt?

Figure 17



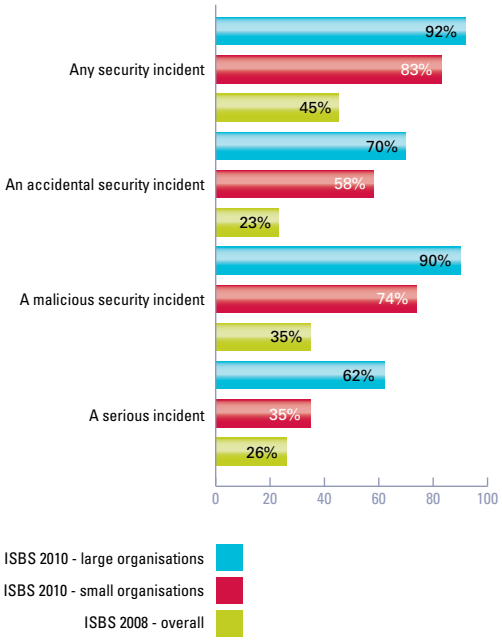
How many respondents prevent staff misuse of the web and social networking sites?

Figure 18



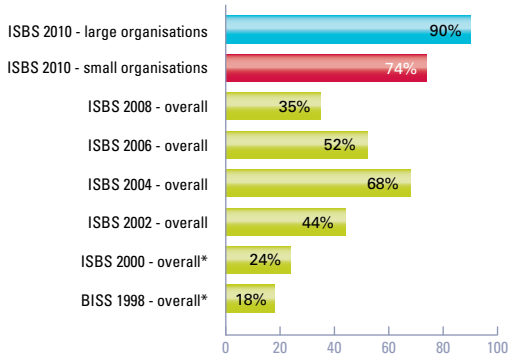
In the last year, how many respondents had...

Figure 19



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

Figure 20



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

What do respondents expect in the future?

Figure 21

Incidence of security breaches

After the peak in 2004, the last two ISBS surveys had shown a decline in the proportion of respondents that had a security breach. This year's results show a dramatic reversal of that trend. More respondents report a breach than in any previous ISBS survey over the last two decades.

There was less variation by industry sector than in previous years' surveys. Respondents from all sectors had a high incidence of security breaches. For example, every manufacturing respondent experienced a malicious security breach in the last year. Technology companies were least likely to have a malicious security breach, but even there three-quarters of respondents had a breach. There was also less variation by region than in the past. Wales had the highest incidence of breaches and Scotland the lowest. Interestingly, respondents whose senior management give a low priority to security report the highest incidence of breaches.

As always, there are many factors that could account for the increase in security breaches compared with two years ago. Two, in particular, are important to understand:

- As discussed in the ISBS 2008 report, previous breach statistics were probably under-reported due to weaknesses in the detective controls that would pick them up. This year's results show controls have improved; there is, therefore, likely to be less under-reporting this year;
- The survey sampling basis has changed between ISBS 2008 and ISBS 2010. This year's survey moved to the self-select basis used by most other security surveys around the world. Experience shows that self-select surveys tend to attract more responses from those who have been affected by security breaches. Extrapolation of the survey responses to the UK as a whole should, therefore, be treated with caution.

While these factors both suggest that the increase from 2008 may be exaggerated, it seems clear that the underlying trend is upwards. The nature of the incidents reported in this survey are different from those seen in previous surveys, with big rises in confidentiality and data protection breaches, hacking and denial of service attacks, and 'botnet' and spyware infections.

Large organisations are still likeliest to report security incidents. The reasons for this remain the same as in the past. Firstly, large organisations have more staff, so the likelihood of some internal misuse increases. Secondly, their size and typical presence on the Internet makes them a more attractive target for external attackers.

The average number of incidents per respondent is up significantly from two years ago. The mean number of breaches is now several a day (up from several per week). As in 2008, the median number of breaches (14 for small and 45 for large respondents) gives a more representative picture, since the mean is distorted by a small number of respondents with hundreds of breaches per day.

The number of serious security breaches is up somewhat compared with two years ago, particularly among large organisations. However, this rise is not as pronounced as the incidence of security breaches as a whole.

Respondents remain, on balance, pessimistic about what the future holds. Nearly three times as many respondents expect to have more security breaches next year as expect fewer breaches. Among large organisations this is more pronounced. Utilities and property companies are very pessimistic, while retailers are the most optimistic about the future.

Type of security incidents

The number of respondents experiencing systems failures and data corruptions has increased compared with two years ago. This is interesting, since for the last decade this has been fairly stable. It appears that the increasing dependency on systems and the rising complexity of their architecture is now causing problems. For instance, respondents that have implemented Voice over IP are more likely to have incidents than those that have not. Financial services providers, who tend to have messy legacy systems, are most likely to report problems. Telecom providers and utilities, where availability is critical, had fewest problems.

The most striking feature of ISBS 2008 was the decline in reported virus infections. This trend has dramatically reversed in this year's survey. Three times as many respondents had infections as two years ago; this trend was consistent across all sizes of respondent. The proportion of organisations with infections is now close to the 2004 peak, particularly among large respondents. However, compared with 2004, today's malicious software is much more likely to carry a malign payload.

Those sectors that have historically invested more heavily in security (technology, telecoms, financial services and utilities) were least likely to suffer a virus outbreak. Respondents in the manufacturing, travel, leisure and entertainment sectors were most likely to have an infection. The South-West reported fewest malicious software incidents, whereas the Midlands and Wales were the most affected regions.

Computer fraud and theft has tended in the past to impact only a tiny proportion of small businesses. This year, this has increased significantly, but it still remains relatively rare compared with other types of incident. Similarly, while the number of large organisations affected has risen somewhat, it has not risen as much as for other types of breach. Interestingly, fewer technology companies had equipment stolen than other sectors, perhaps because they understand their assets better. As in 2008, respondents from Wales were least likely to report thefts; in contrast, the theft rate in East Anglia appears to have risen significantly.

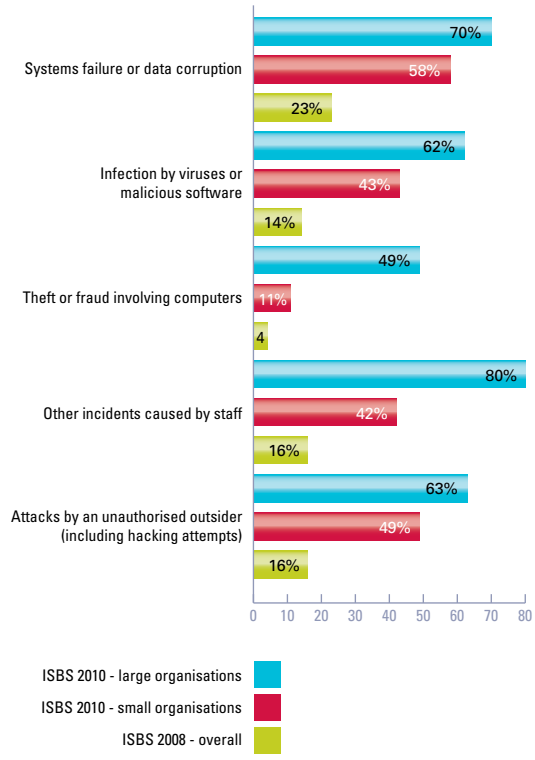
Other breaches caused by staff, whether by misuse of systems or unintentional data leaks, have always been more likely in large organisations than small ones. This trend has continued, though the gap has narrowed somewhat. Among large respondents, staff-related incidents were the most common type of breach reported. All sectors had staff-related breaches, though technology companies fared better than most; their staff, perhaps, inherently understand the security risks better. The extent to which staff understand the security policy has a big impact; organisations where this is poor appear more than twice as likely to have staff-related breaches as those where it is very good.

Attacks by unauthorised outsiders are also up markedly for all sizes of organisation. For instance, 63% of large respondents were attacked in the last year, compared with only 39% two years ago. Interestingly, fewer property and utility companies reported being attacked than average. The most attacked sectors included the usual suspects (financial services, government and telecoms), but also manufacturing and leisure. There was not much regional variation in attack pattern, though fewer respondents in the Midlands reported attacks than average.

While the average number of breaches suffered by affected organisations is up significantly compared with two years ago, this does vary by type of incident. The median number of virus outbreaks is down, while the number of other breaches has risen. Small organisations have seen a big jump in computer fraud and theft, perhaps reflecting the recessionary times. In contrast, the biggest rise for large respondents is in outsider attacks – cybercrime is currently one of the fastest growing areas of organised crime worldwide, and the survey results reflect this trend.

What type of breaches did respondents suffer?

Figure 22



What is the median number of breaches suffered by the affected organisations in the last year?

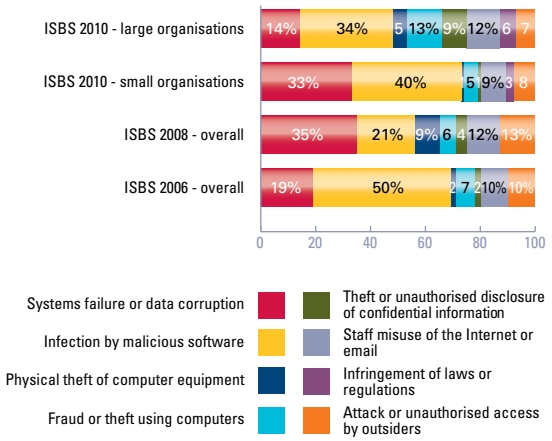
Figure 23

	Large organisations	Small organisations
Systems failure or data corruption	4 (3)	2 (1)
Infection by viruses or other malicious software	2 (3)	1 (2)
Theft or fraud involving computers	4 (2)	8 (1)
Other incidents caused by staff	20 (9)	7 (6)
Attacks by an unauthorised outsider (including hacking attempts)	28 (11)	13 (6)
Any security incident	45 (15)	14 (6)

Equivalent comparative statistics from ISBS 2008 are shown in brackets

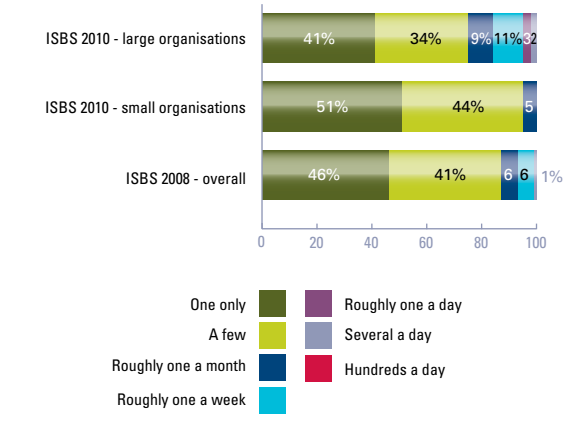
What was the worst security incident faced by respondents?

Figure 24



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

Figure 25



Infection by viruses and malicious software

After the steady decline in reported infections from the peak in 2004 to the last survey in 2008, the last couple of years have shown a new wave of incidents. 43% of small respondents had an outbreak in the last year, up threefold on two years ago. The picture among large respondents is no more encouraging; 62% were infected compared with only 21% in 2008.

A major contributor to this trend has been a new wave of Internet worms. Unlike the attacks of 2003-2004, these worms carry a sinister payload; infected machines can be controlled by the worm's creator to send spam or launch denial of service attacks (as part of a co-ordinated 'botnet'). The most significant of these over the last year has been the Conficker worm (also known as Downup, Downadup and Kido).

A large public sector body suffered very major disruption for several days following infection by the Conficker worm. Network traffic almost came to a halt and hundreds of accounts were locked. This in turn caused a spike in calls to the help desk. The disruption caused problems for customers and was picked up by the media. There was a contingency plan, but it proved ineffective, and more than £100,000 was spent cleaning up after the incident.

One of the things that has made Conficker so virulent is that it has several different ways in which it can attack an organisation. It targets vulnerabilities in server security and also spreads by infecting removable media devices. Once installed, it blocks access to anti-malware websites, disables automatic updates and kills any anti-malware processes.

A large charity was infected by the Conficker worm after it was brought in on an infected USB stick. The worm brought down the charity's systems for a day. Despite an effective contingency plan, it took significant effort to eliminate the infection and restore systems.

Largely as a result of these new worm attacks, 40% of small organisations reported that virus infection was their worst security incident of the year, twice as many as two years ago. Virus infection was the single biggest cause of worst incidents in all sizes of organisation.

A small IT consultancy was hit by a virus which took down its network for 12 hours. There was a contingency plan, but it proved ineffective, and it cost more than £10,000 to get the systems back up. The biggest impact, however, was probably the customer complaints.

While the botnet worms appear to have had the biggest impact over the last year, a large and increasing number of other new viruses, Trojans and spyware are bombarding organisations. Spyware such as the ZBOT family infects machines, then logs keystrokes and sends password details to cybercriminals. There is only a short time-lag between a new software service and a malicious exploit of it, as witnessed by Facebook and iPhone viruses.

A server at a public sector body was infected by spyware and had to be taken out of service for several days. This affected many key applications.

A dog breeder's computer system was infected by a Trojan. It sent rude messages to all their contacts, which was very embarrassing. It took more than a week to fix the problem.

Fake anti-virus software installed itself on a PC at a medium-sized law enforcement body. The organisation was unprepared for such a situation, and it took several man-days of effort to remove the malicious software.

Systems failure and data corruption

As in previous years, the single biggest cause of these incidents was hardware failure. Over a third of the worst problems arose from hardware faults. This is, however, down from 2006, when hardware was responsible for 61% of systems failures.

A hard disk failure on a server supporting a key application disrupted the operations of a medium-sized technology company for more than a month. The company had to resort to manual workarounds to support the failed business process. Unfortunately, this led to some customer complaints. In the end, it took several man-weeks of effort to restore service to normal.

Software bugs in applications or operating systems caused roughly a quarter of the worst problems, more than in the past. One reason is that systems are more complex and so inherently less stable; in addition, they also tend to be updated or patched more frequently than in the past.

A batch failure at a large financial services provider corrupted various downloads from other systems, causing the end of day batch process to fail. This caused very major disruption to the company for the next day, but was resolved on the following night.

Power outages or spikes accounted for about one in five of the worst problems. Often, companies had precautions (e.g. an Uninterruptable Power Supply) but these failed to operate.

A small company in London suffered a power spike in their building. Unfortunately, this took out not just their main server but also their backup server. The data was recovered using a specialist data recovery service, but this took several weeks and some records were permanently lost.

Network problems were the main cause of the remaining incidents. This was a particular issue if the organisation used Voice over IP telephony. Some had planned in advance their response to network failures, and this contingency planning generally paid off.

A small airline suffered major business disruption after its Voice over IP telephony failed. Fortunately, their contingency plan allowed them to restore service within a few hours.

Computer theft and fraud

Physical theft of computers remains the most common type of incident. Compared with two years ago, rates of theft, particularly by staff, have increased substantially. Large organisations are much more likely to have a breach of this kind than small ones.

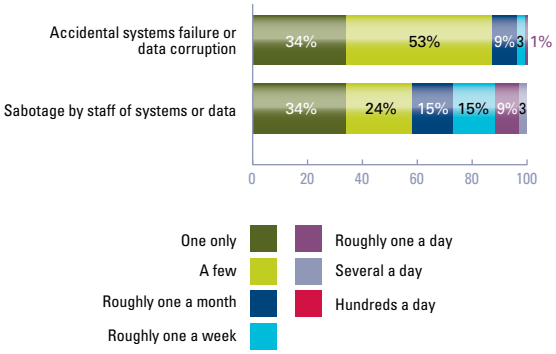
Thieves stole equipment worth more than £100,000 at a major telecommunications company. It cost even more than that to investigate the incident and remediate the controls so that it didn't happen again. Fortunately, an effective contingency plan meant that service was not interrupted.

A public sector body in the Midlands reported the theft of more than 50 laptops over a 12 month period. The main impact was the cash cost of replacing the hardware, but there was also some business disruption.

Computer fraud (or theft using computer systems) remains relatively rare. However, it has risen significantly since 2008, when only 1% of respondents reported such incidents. In addition, computer frauds are almost always serious in impact.

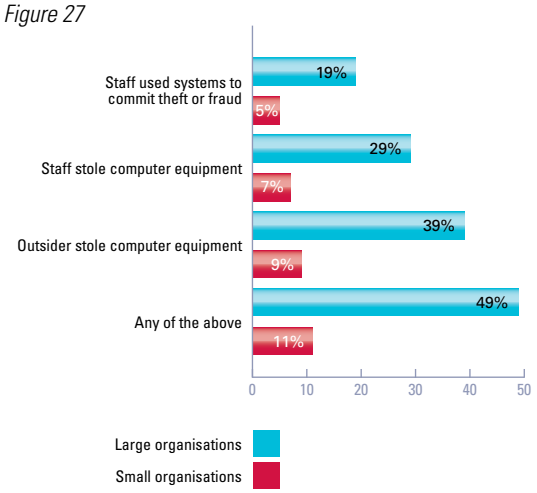
How many systems failures or data corruptions did the affected organisations suffer in the last year?

Figure 26



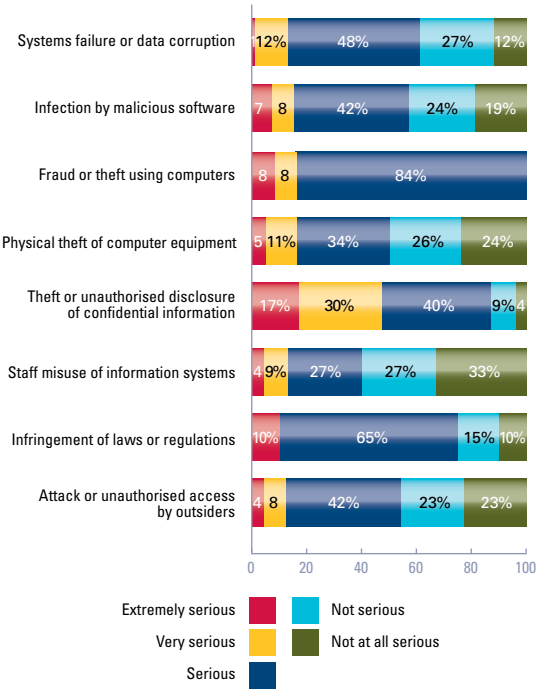
What type of theft and fraud did respondents suffer?

Figure 27



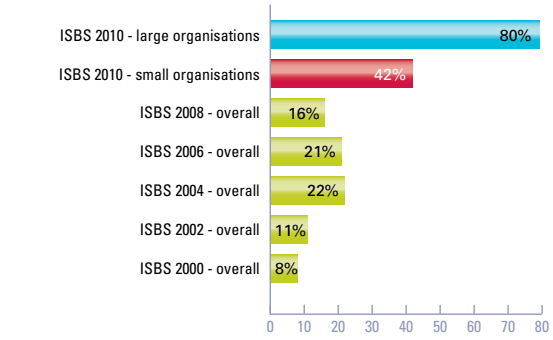
How serious were different types of incident?

Figure 28



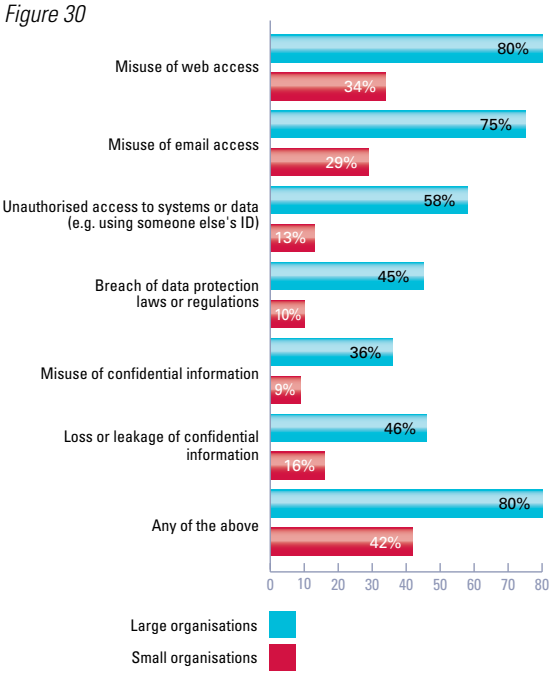
How many respondents had staff-related incidents?

Figure 29



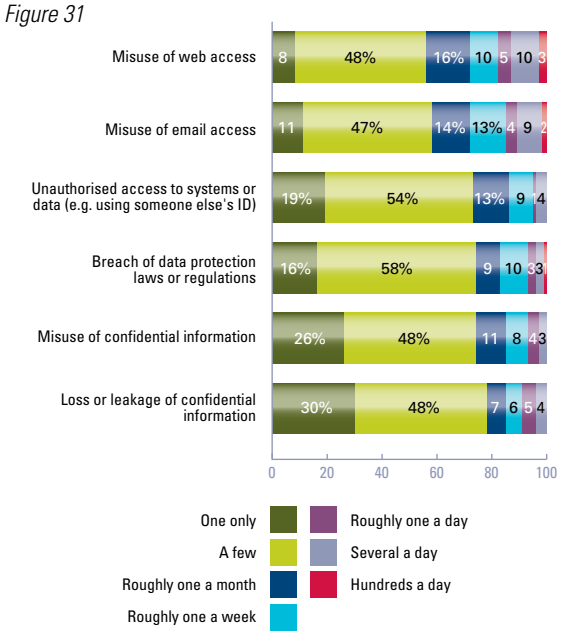
What type of staff-related incidents did respondents suffer?

Figure 30



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

Figure 31



Other incidents caused by staff

Staff misuse of the web and email remain the most common incidents. The number of respondents reporting breaches of this kind has roughly doubled since two years ago. It remains likely as well that, as in the past, these statistics are under-reported. Organisations that log and monitor staff web access are twice as likely to report breaches as those that do not; this suggests that those without logging may be missing some incidents.

Staff at a medium-sized public sector body in London viewed pornographic websites, which then infected systems with malicious software. The infections were cleaned up quickly, but the investigation of the incident cost more than £50,000. A contributing factor was the lack of any contingency plan.

There are also an increasing number of incidents involving peer-to-peer file-sharing using work computers. As well as breaching copyright, this can also have a big impact on the organisation's bandwidth for legitimate use of the Internet.

Staff at a firm in the defence sector used their Internet access to download and share illegal copies of films.

There continue to be incidents involving staff making excessive use of work computers for personal purposes. However, these tend to be less serious than in previous years.

Confidentiality and data protection breaches, while still less common than staff misuse of the web or email, have increased even more dramatically. In 2008, only 6% of large respondents (and 1% overall) reported such breaches. Now, nearly half of large respondents admit they have had a breach of this kind in the last year. A third of large respondents have suffered deliberate misuse of confidential data.

A large company providing services to the public sector was embarrassed when some of its customer data was stolen and sold to another company. Some customers complained. Because there was no contingency plan, it took several man-weeks of effort to respond to the breach and tighten up controls to prevent further incidents.

Temporary call centre staff at a large financial services provider stole customer details, but this was quickly discovered and dealt with.

More often, there is no malicious intent. Nearly twice as many small organisations lost confidential data accidentally through staff error as had confidential data stolen or misused.

A transport and logistics firm infringed data protection laws when customer data was used in system testing without the customers' consent or authorisation from the company's data controller.

When a confidentiality breach does occur, its impact is more likely to be serious than other types of security incident. 45% of confidentiality breaches were very serious or extremely serious, compared with only 15% of other incidents. Often, media interest results in reputational damage and the resultant investigation distracts senior management.

A confidentiality breach at a large public sector body resulted in some adverse media coverage. The contingency plan proved ineffective and it took more than 100 man-days to investigate and remediate the damage.

Unauthorised access by outsiders

One of the most shocking findings of ISBS 2008 was the jump in the number of large companies that had detected an outsider who had successfully penetrated into their network. The bad news this year is that these penetration rates have continued to climb. Twice as many respondents report having experienced a significant attempt by outsiders to break into their systems; roughly one in eight respondents overall had been successfully hacked. The root cause for most of the successful attacks was staff failing to set up or update their technical configuration correctly.

A large design and engineering consultancy lost its email services after an attacker compromised a server. Staff had failed to follow the security procedures when updating the firewall rules, and this allowed the brute force attack to succeed.

Human error when adding a firewall rule at a large financial services provider led to the perimeter firewalls being open to the Internet for a couple of days. The company's servers were taken over and used to send spam messages. This in turn resulted in the company's legitimate email being blacklisted and treated as spam.

A large technology company was attacked after a network infrastructure device was deployed with the default password and no port filtering between it and the Internet.

With the move to Voice over IP telephony, telecommunications traffic is now an attractive target for hackers. The number of respondents reporting attacks on their phone or network traffic is up fourfold on 2008.

It is not always technical configuration that causes problems. Social engineering, where outsiders get staff to reveal confidential information, remains an important risk. Phishing, where an electronic message or website asks people for their passwords, is up threefold on two years ago. It has also become more sophisticated and is now often highly targeted at specific individuals (known as 'spear-fishing').

Staff at a large financial services company were targeted by a sophisticated spear-phishing attack, where they were asked to download malicious software files from what appeared to be a company website. The attack appears to have been organised by a European criminal group.

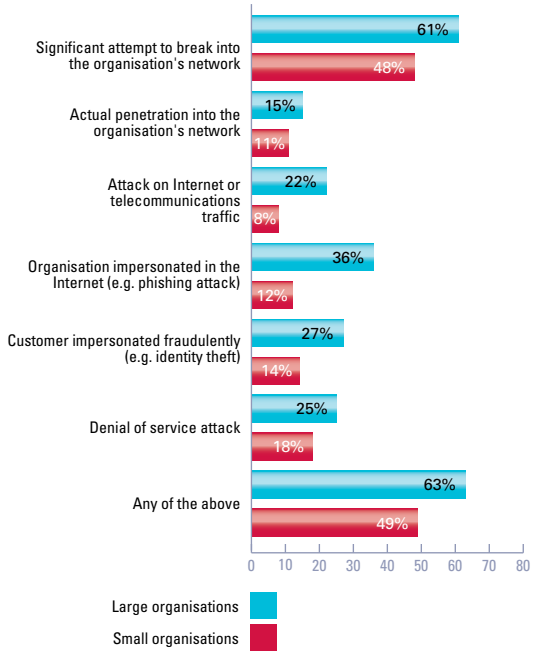
As a result, identity fraud, where criminals use harvested passwords to impersonate a customer and carry out fraudulent transactions, is increasing. A quarter of large respondents report such incidents, up threefold on 2008. The experience varies considerably by sector. Most exposed are retailers, where more than half of the respondents were affected. Financial services, particularly banks, also suffer. In contrast, very few manufacturing respondents report being targeted.

The rise of botnets has enabled criminals to launch devastating distributed denial of service attacks, where hijacked computers are used to bombard the target with messages. Retailers have now overtaken telecoms providers as the most targeted sector for these attacks

A very large technology company had delivered and hosted a website for a customer. Unfortunately, the site was targeted by a denial of service attack, which threw huge amounts of data at the server farm (in excess of 10 gigabytes per second). The contingency plan kicked in and was effective at limiting the disruption to a few hours, but it took a large team and more than £100,000 to fix the problem.

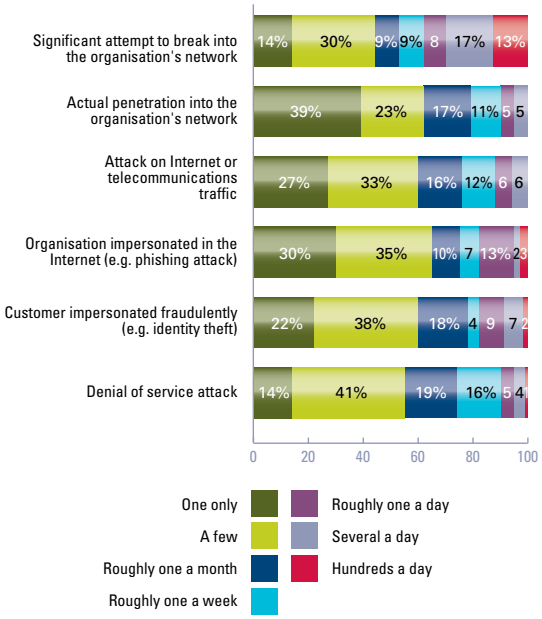
How many respondents were attacked by an unauthorised outsider in the last year?

Figure 32



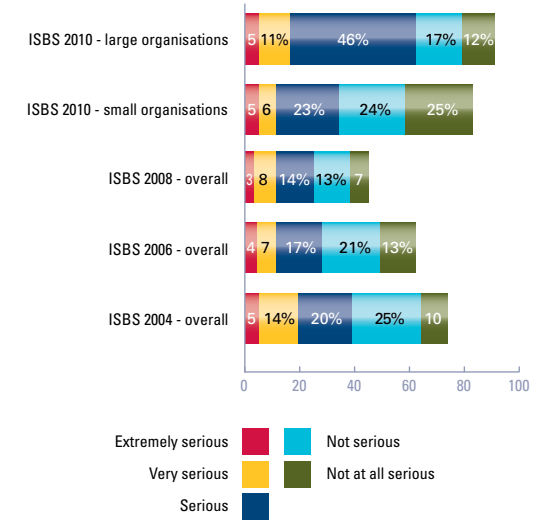
How many incidents did affected organisations have in the last year?

Figure 33



How many respondents had a serious incident?

Figure 34



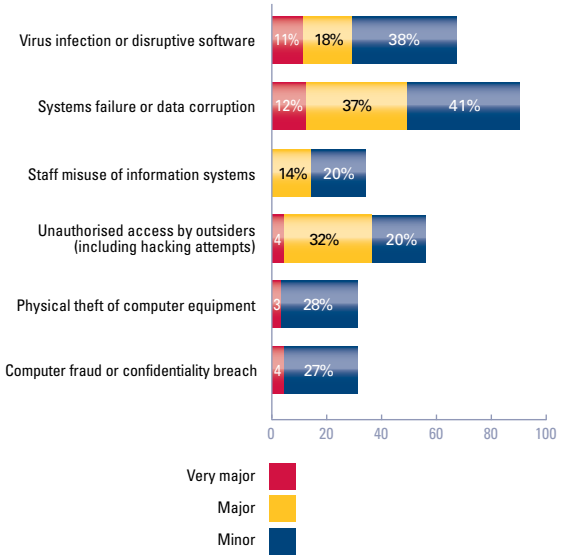
How much disruption to the business did the worst security incident cause?

Figure 35

	None	Less than a day	Between a day and a week	Between a day and a month	More than a month
Very major disruption	33%	4%	4%	0%	1%
Major disruption		9%	8%	1%	1%
Minor disruption		13%	10%	3%	2%
Insignificant disruption		11%	1%	1%	0%

Which incidents were most disruptive to business?

Figure 36



Impact of breaches

The impact of breaches can be measured in several ways. Relying on a single measurement, such as estimated cash cost, can be misleading. For many firms, the impact that an incident has on their reputation may be more important than financial loss. Other indirect costs such as investigation and remediation time also need to be considered. All of these aspects are tracked in this survey.

The good news this year is that, despite the increase in the number of respondents that had a security breach, the number experiencing a very serious breach has remained stable (at 11%). On the other hand, serious breaches have increased; a third of small organisations and three-fifths of large organisations have had at least one serious breach in the last year.

Business disruption

Business disruption continues to be the biggest single impact of security breaches. Roughly two-thirds of the worst incidents reported caused disruption, up somewhat on previous surveys.

In the last year, viruses and malicious software have been the biggest cause of service interruption. This is a reversion to the pattern last seen in ISBS 2004. Viruses caused most damage in the government and financial services sectors.

A local authority in the South-West had major business disruption for more than a month after its systems were infected by the Conficker worm. This led to some customer complaints. A contributing factor was the lack of a contingency plan.

In ISBS 2006 and 2008, the biggest cause of disruption was systems failure and data corruption. It is now the second most important source of service interruptions, behind virus infection. System failures were particularly important in the telecoms, retail and financial services sectors.

A power outage at a medium-sized telecoms provider disrupted its operations. Unfortunately, the UPS and the backup generator both failed.

Sometimes improving security can be a risk in itself. Changes made to systems can cause them to malfunction.

Changes made to implement PCI at a large retailer inadvertently caused the point of sale systems to fail, disrupting the business for several days.

Attacks by outsiders, especially denial of service attacks, and staff misuse of systems were the main other types of incident that caused business disruption.

A very large public sector body suffered from loss of productivity when staff were found to be spending excessive time shopping on the Internet. The adverse media coverage led to significant expenditure on controls to prevent further such misuse.

By using similar techniques to previous surveys, an estimate of the cost of disruption from companies' worst incidents has been calculated. This shows an increase in service disruption experienced by small organisations, to 2-4 days at an average cost of £15,000-£30,000. Large organisations also suffered more disruption than in 2008, with average interruption of 2-5 days and an average cost of £200,000-£380,000.

Incident response costs

Regardless of how much damage an incident causes, organisations still incur the indirect cost of staff time responding to it. For some incidents (such as staff misuse), this time is primarily investigation of what went wrong and may include building up evidence to support disciplinary or legal proceedings. 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.

The time spent to remediate incidents has increased since 2008. A third of large organisations had at least one breach in the year that took more than ten man-days to deal with, up from 14% two years ago. However, three-fifths of small organisations were able to deal with all of their security breaches within a man-day each.

On average, small organisations spent £4,000-£7,000 responding to their worst incident of the year; large organisations spent £25,000-£40,000. The largest costs were as a result of virus outbreaks, data protection infringements and physical thefts of computer equipment.

A large Scottish utility provider had very major business disruption for more than a month after a virus outbreak. There was a contingency plan for dealing with viruses, but it proved ineffective; fixing the problem cost more that £1m and took more than 100 man-days of effort.

A large insurer lost a backup tape which contained customer data. The subsequent investigation involved more than 100 man-days of effort, but enabled the company to make a public statement about the breach. This minimised the adverse media coverage.

Direct financial loss

A security breach may also cause direct financial loss. As well as loss of assets, direct costs may include fines imposed by regulators or compensation payments to customers. Direct costs remain relatively rare, but are on the increase. On average, small organisations incurred £3,000-£5,000 of direct loss from their worst incident of the year; large organisations spent £25,000-£40,000. Computer frauds are by far the biggest cause of large losses, but physical theft of computer equipment and confidentiality breaches also tend to lead to direct losses.

A breach of internal control at a large Scottish financial services provider resulted in a large fraud being perpetrated over a long period of time. The losses were in excess of £500,000 and the investigation cost more than £100,000.

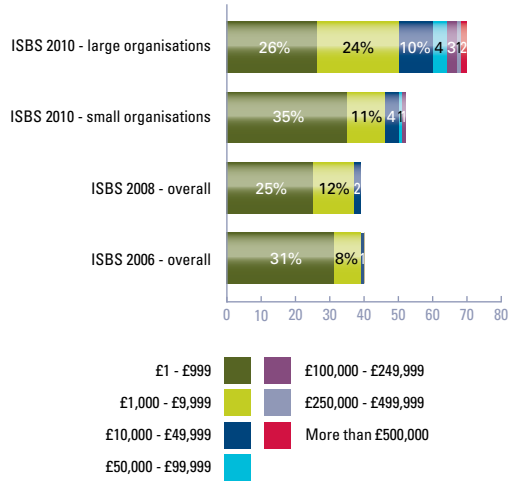
Indirect financial loss

Losses can also be indirect, for example through the loss of intellectual property or revenue leakage. Less than one in five respondents had any indirect loss from their worst incident, but those losses were often substantial. On average, small organisations incurred £5,000-£10,000 of indirect loss from their worst incident of the year; large organisations lost £15,000-£20,000. The largest indirect financial loss (of more than £500,000) was reported by a large retailer following a legal infringement. Normally, it was computer frauds and confidentiality breaches that caused the damage.

A security leak at a large music company led to the deliberate pre-release leaking of a superstar artist's latest album. As well as losing the company revenue of more than £100,000, there was also the embarrassment of the media coverage to contend with.

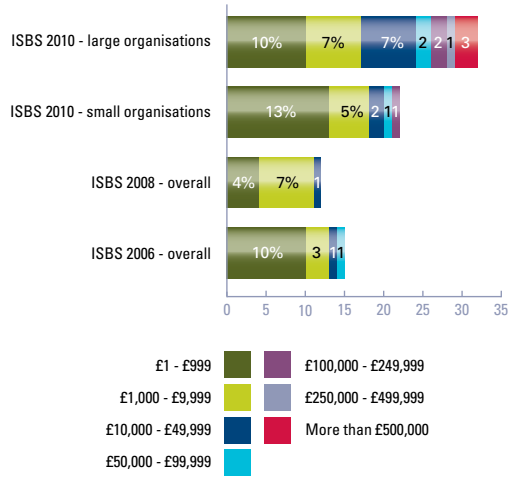
How much cash expenditure was required to recover from the worst security incident of the year?

Figure 37



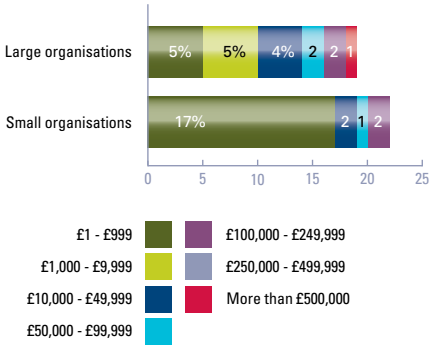
Was there any direct financial loss associated with the worst security incident of the year?

Figure 38



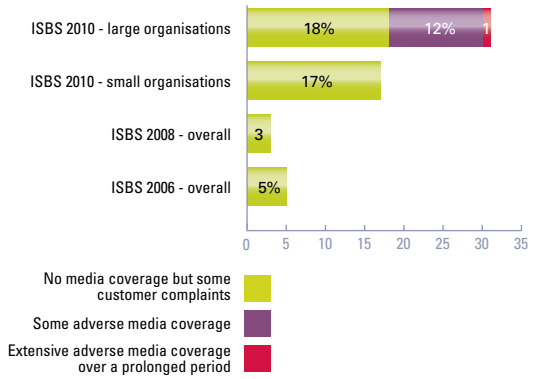
Was there any indirect financial loss associated with the worst security incident of the year?

Figure 39



To what extent did the worst incident damage the reputation of the organisation?

Figure 40



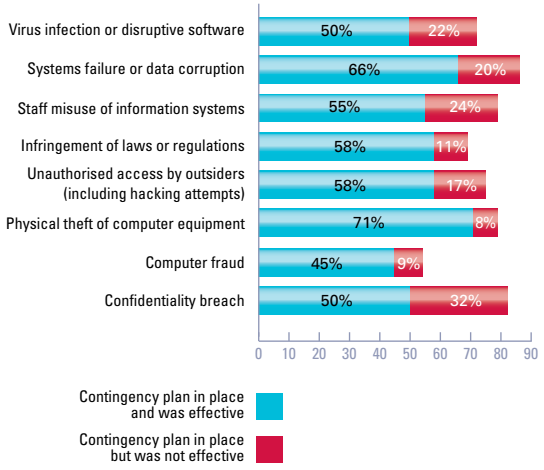
What was the overall cost of an organisation's worst incident in the last year?

Figure 41

	ISBS 2010 small organisations	ISBS 2010 large organisations
Business disruption	£15,000 - £30,000 *over 2-4 days*	£200,000 - £380,000 *over 2-5 days*
Time spent responding to incident	£600 - £1,500 *2-5 man-days*	£6,000 - £12,000 *15-30 man-days*
Direct cash spent responding to incident	£4,000 - £7,000	£25,000 - £40,000
Direct financial loss (e.g. loss of assets, fines etc.)	£3,000 - £5,000	£25,000 - £40,000
Indirect financial loss (e.g. theft of intellectual property)	£5,000 - £10,000	£15,000 - £20,000
Damage to reputation	£100 - £1,000	£15,000 - £200,000
Total cost of worst incident on average	£27,500 - £55,000	£280,000 - £690,000
2008 comparative	*£10,000 - £20,000*	*£90,000 - £170,000*

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

Figure 42



Damage to reputation

The vast majority of respondents have been able to keep the impact of security breaches within their organisation. However, an increasing number of breaches have led to customer complaints or stories in the media. Confidentiality breaches are most likely to become known outside the organisation, with one in five attracting media coverage. Attacks by outsiders and computer frauds also tend to result in publicity. Retailers and public sector organisations were affected most, with financial services close behind.

A Midlands-based technology company lost a USB stick containing a customer's test data. Unfortunately, this resulted in extensive adverse media coverage over a prolonged period. The extensive review of procedures that followed consumed many man-months of effort and more than £100,000 in cash costs.

A hacking attack on a server at a medium-sized financial services provider in the North-West caused some disruption to services for several weeks. More importantly, it resulted in several adverse media stories.

Total cost of incidents

The average total cost of a small respondent's worst incident is between £27,500 and £55,000, up significantly on 2008. A similar trend is seen amongst large respondents, with the average total cost of the worst incident now up to between £280,000 and £690,000.

Extrapolation of cost data across the whole of the UK should always be treated with caution, particularly given the change in the nature of the respondents compared with previous ISBS. However, the survey results suggest that, after the drop in the previous few years, the total cost of security incidents to UK plc has increased back up to levels last seen in the mid-noughties. An indicative estimate of the overall cost is in the order of several billion pounds a year.

Contingency planning

Four-fifths of respondents that suffered a breach had a contingency plan in place, up from three-fifths two years ago. However, roughly a quarter of these proved ineffective at addressing the incident. In the past, large companies have been better at contingency planning than small ones; this gap appears now to have closed. The incidents with the highest total cost were those without an effective contingency plan.

The Conficker worm exposed weaknesses in a large financial services provider's contingency plans. It caused very major business disruption for several hours, and it took roughly a hundred man-days of effort to get the systems back up and infections eliminated.

A hospital was exposed after a doctor left a laptop with research information and patient details on a train. There was some adverse media coverage, but the hospital's contingency plan proved effective at minimising the damage.

A technology company's website was defaced. There was an effective contingency plan, which meant that the site was restored within 2 hours.

Staff at a large public sector body inadvertently emailed a classified attachment over the Internet. Fortunately, the organisation had invested in software that scans for potential breaches of this kind; the attachment was quarantined before reaching the Internet.

Independent reviewers

ASIS International is the largest organisation for security professionals, with more than 35,000 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.

BCS, The Chartered Institute for IT, promotes wider social and economic progress through the advancement of information technology science and practice. We serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally. For more information, see www.bcs.org.

Eskenzi PR are a creative and strategic PR Consultancy that specialises in the hi-tech sector. Our objective is to be the best niche PR consultancy in IT/Comms with an unrivalled reputation with journalists and clients. For more information, see www.eskenzipr.com.

The **European Information Society Group (EURIM)** brings together politicians, officials and industry to help improve the quality of policy formation, consultation, scrutiny, implementation and monitoring in support of the creation of a globally competitive, socially inclusive and democratically accountable information society. For more information, see www.eurim.org.uk.

GetSafeOnline.org is a joint initiative between HM Government, the Serious Organised Crime Agency (SOCA) and leading businesses, which aims to help individuals and small businesses protect themselves against internet security risks. For more information, see www.getsafeonline.org.

ICAEW (www.icaew.com) is a world leader of the accountancy and finance profession. We provide our members with knowledge and guidance based on the highest ethical and technical standards. We shape opinion, understanding and delivery to ensure the highest standards in business and in the public interest. ICAEW's IT Faculty helps chartered accountants make the best possible use of IT.

The mission of the **Institute of Information Security Professionals (IISP)** is to be the authoritative body of information security professionals. We are achieving this by advancing the professionalism of information security practitioners through personal development, exchange of information, professional assessment and qualification, liaison with government, and providing other services required and driven by the industry. For more information, see www.instisp.org.

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.

With more than 86,000 constituents in more than 160 countries, **ISACA®** (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance of IT, and IT-related risk and compliance.

The **Information Security Forum (ISF)** is the world's leading independent authority on information security; its members include 50% of Fortune 100 companies. For more information, see www.securityforum.org.

With active participation from individuals and chapters all over the world, **the Information System Security Association (ISSA)** is the largest international, not-for-profit association for information security professionals. It provides educational forums, information resources, and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. For more information, see www.issa.org.

The **International Information Systems Security Certification Consortium**, Inc. is the internationally recognised Gold Standard for certifying information security professionals. Founded in 1989, (ISC)² has certified over 68,000 information security professionals in over 130 countries. For more information, see www.isc2.org.

The **National Computing Centre** is the single largest UK corporate membership body in the IT sector. NCC champions the effective deployment of IT to maximise the competitiveness of its members' business, and serves the corporate, vendor and government communities. For more information, see www.ncc.co.uk.

Royal Holloway is a multi-faculty College of the University of London. Its Information Security Group is recognised worldwide and in 1998 was awarded a Queen's Anniversary Prize. For more information, see www.isg.rhul.ac.uk.

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 responsibility for, raising awareness about security within their organisations.

The **UK ISO/UK 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 http://www.iso27001usergroup.co.uk