Department
for Business
Innovation & Skills

2013 INFORMATION SECURITY BREACHES SURVEY

Technical Report

Survey conducted by

pwc

In association with

infosecurity
EUROPE

Commissioned by:

Department
for Business
Innovation & Skills

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.gov.uk/bis.

Conducted by:

pwc

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.

The PwC team was led by Chris Potter and Andrew Miller. We'd like to thank all the survey respondents for their contribution to this survey.

In association with:

infosecurity® EUROPE

Infosecurity Europe, celebrating 18 years at the heart of the industry in 2013, is Europe's number one Information Security event. Featuring over 350 exhibitors, the most diverse range of new products and services, an unrivalled education programme and over 12,000 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. Infosecurity Europe runs from the 23rd – 25th April 2013, in Earls Court, London. For further information please visit www.infosec.co.uk.

Reed Exhibitions®

Reed Exhibitions is the world's leading events organizer, with over 500 events in 41 countries. In 2012 Reed brought together seven 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 34 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. www.reedexpo.com.

Information security:

The preservation of the confidentiality, integrity and accessibility of information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can be involved.

Cover image:

The unique markings on each zebra are used as an effective defence mechanism to confuse predators. Large cats can only see in monochrome, so a zeal of zebra running in their natural habitat makes it difficult to identify individual prey.

Introduction

The Department for Business, Innovation and Skills recognises the importance of producing reliable information about cyber security breaches, and making it publicly available. I welcome the fact that so many businesses across the UK economy have shared their experiences for the 2013 Breaches Survey, a key commitment in the Government's UK Cyber Security Strategy. Businesses need to be informed about the severity of the threat - and the impact. This year's survey clearly demonstrates the damage being done to UK companies in cyberspace. Understanding the risks is critical in addressing the challenge of how to manage them. Proactive management of risks represents a competitive advantage; effective cyber security is good for business. The information in this report will support all our efforts in cyberspace.

David Willetts

Survey approach

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.

To maximise the response rate and reduce the burden on respondents, this year's survey questions were broken up into four online questionnaires. Some questions were included in all four questionnaires. In common with the 2010 and 2012 surveys, respondents completed the survey during the February-March period on a self-select basis.

In total, there were 1,402 respondents. 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 and Not Applicables. If the proportion of Don't Knows was significant, we refer to this in the text.

As a result, the number of responses varied significantly by question, so we've included against each figure in the report the number of responses received. This gives a good guide to the margin of error from sampling error to apply when extrapolating the results (at 95% confidence levels, the margin of error on 1,000, 600 and 100 response samples is +/- 3%, +/-4% and +/- 10% respectively).

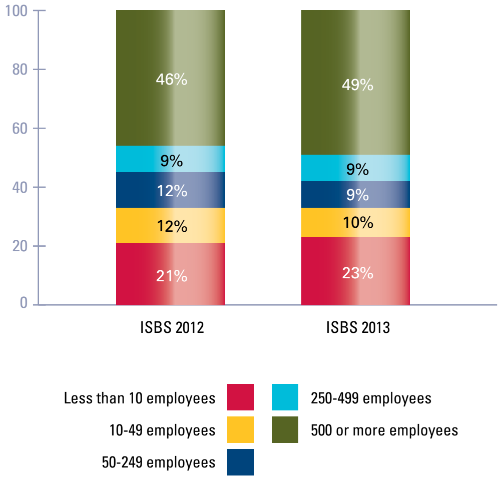
As in the past, we have presented the results for large organisations (more than 250 employees) and small businesses (less than 50 employees) separately, and explained in the text any differences seen for medium-sized ones (50-249 employees). The 2008 and earlier surveys quoted overall statistics based on a weighted average; these were virtually identical to the results for small businesses.

Respondents came from all industry sectors, with a sector breakdown that is consistent with that seen in previous surveys. As in 2012, roughly a third of the respondents were information security professionals, roughly a third were IT staff and the remainder were business managers, executives or non-executive directors. As in the past, the highest response rates were from companies headquartered in London or the South-East of England; these made up just under half of the respondents.

Rt Hon David Willetts MP,
Minister for Universities and Science.

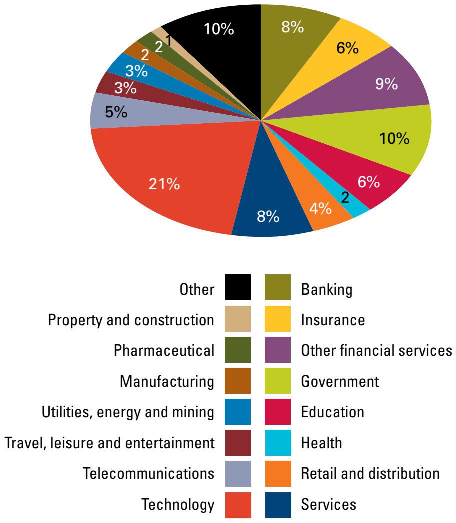
How many staff did each respondent employ in the UK?

Figure 1 *(based on 1,365 responses)*



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

Figure 2 *(based on 1,402 responses)*



Executive Summary

Security breaches reach highest ever levels

The number of security breaches affecting UK business continues to increase.

Trend since 2012	Large organisations (> 250 staff)	Small businesses (< 50 staff)
% of respondents that had a breach	↔	↑
Average number of breaches in the year	↑	↑
Cost of worst breach of the year	↑↑	↑↑
Overall cost of security breaches	↑↑	↑↑↑

The rise is most notable for small businesses; they're now experiencing incident levels previously only seen in larger organisations.

93%	of large organisations had a security breach last year
87%	of small businesses had a security breach in the last year (up from 76% a year ago)

Affected companies experienced roughly 50% more breaches on average than a year ago.

113	is the median number of breaches suffered by a large organisation in the last year (up from 71 a year ago)
17	is the median number of breaches suffered by a small business in the last year (up from 11 a year ago)

The cost of individual breaches continues to vary widely. The average cost of respondents' worst breach of the year has never been higher, with several individual breaches costing more than £1m.

£450k - £850k	is the average cost to a large organisation of its worst security breach of the year
£35k - £65k	is the average cost to a small business of its worst security breach of the year

In total, the cost to UK plc of security breaches is of the order of billions of pounds per annum - it's roughly tripled over the last year.

Both external attacks and the insider threat are significant

Attacks by outsiders (such as criminals, hacktivists and competitors) cause by far the most security breaches in large businesses - the average large business faces a significant attack every few days.

78%	of large organisations were attacked by an unauthorised outsider in the last year (up from 73% a year ago)
39%	of large organisations were hit by denial-of-service attacks in the last year (up from 30% a year ago)
20%	of large organisations detected that outsiders had successfully penetrated their network in the last year (up from 15% a year ago)
14%	of large organisations know that outsiders have stolen their intellectual property or confidential data in the last year (up from 12% a year ago)

Small businesses used not to be a target, but are now also reporting increasing attacks.

63%	of small businesses were attacked by an unauthorised outsider in the last year (up from 41% a year ago)
23%	of small businesses were hit by denial-of-service attacks in the last year (up from 15% a year ago)
15%	of small businesses detected that outsiders had successfully penetrated their network in the last year (up from 7% a year ago)
9%	of small businesses know that outsiders have stolen their intellectual property or confidential data in the last year (up from 4% a year ago)

Staff also play a key role in many breaches. Serious security breaches are often due to multiple failures in technology, processes and people. In addition, staff-related incidents have risen sharply in small businesses.

36%	of the worst security breaches in the year were caused by inadvertent human error (and a further 10% by deliberate misuse of systems by staff)
57%	of small businesses suffered staff-related security breaches in the last year (up from 45% a year ago)
17%	of small businesses know their staff broke data protection regulations in the last year (up from 11% a year ago)

Understanding and communicating the risks is key to effective security

The vast majority of businesses continue to prioritise security.

81%	of respondents report that their senior management place a high or very high priority on security
12%	of the worst security breaches were partly caused by senior management giving insufficient priority to security

This has translated into security budgets increasing, or at least not being cut.

10%	of IT budget is spent on average on security (up from 8% a year ago)
16%	of IT budget is spent on average on security, where security is a very high priority (up from 11% a year ago)
92%	of respondents expect to spend at least the same on security next year (and 47% expect to spend more)

However, many businesses can't translate this expenditure into effective security defences. In large organisations, ineffective leadership and communication about security risks often leaves staff unable to take the right actions.

42%	of large organisations don't provide any ongoing security awareness training to their staff (and 10% don't even brief staff on induction)
26%	of respondents haven't briefed their board on security risks in the last year (and 19% have never done so)
33%	of large organisations say responsibilities for ensuring data is protected aren't clear (and only 22% say they are very clear)
93%	of companies where the security policy was poorly understood had staff-related breaches (versus 47% where the policy was well understood)

Weaknesses in risk assessment and skills shortages also often prevent effective targeting of security expenditure.

23%	of respondents haven't carried out any form of security risk assessment
53%	of respondents are confident that they'll have sufficient security skills to manage their risks in the next year
31%	of respondents don't evaluate how effective their security expenditure is

Many struggle to implement basic security

Overall, the survey results show that companies are struggling to keep up with security threats, and so find it hard to take the right actions. The right tone from the top is vital - where senior management are briefed frequently on the potential security risks, security defences tend to be stronger.

In 2012, the UK Government issued guidance to businesses on how to protect themselves from cyber security threats ("The Ten Steps" - https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility). 30% of large organisations had used this guidance. However, our analysis of the survey results suggests that implementation of these basic practices is patchy, particularly in small businesses:

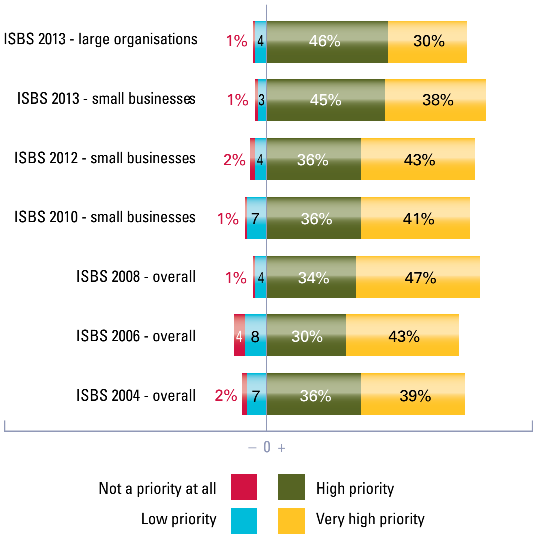
The Ten Steps	Large organisations	Small businesses
Information risk management	Some good, some weak	Some good, some weak
User education and awareness	Some good, some weak	Generally weak
Home and mobile working	Some good, some weak	Generally weak
Incident management	Some good, some weak	Generally weak
Managing user privileges	Some good, some weak	Some good, some weak
Removable media controls	Some good, some weak	Generally weak
Monitoring	Some good, some weak	Generally weak
Secure configuration	Some good, some weak	Some good, some weak
Malware protection	Generally good	Some good, some weak
Network security	Generally weak	Generally weak

Business use of technology is changing fast, so it's important to have a flexible approach to security.

14%	of large organisations had a security or data breach in the last year relating to social networking sites
9%	of large organisations had a security or data breach in the last year involving smartphones or tablets
4%	of respondents had a security or data breach in the last year relating to one of their cloud computing services
4%	of the worst security breaches were due to portable media bypassing defences

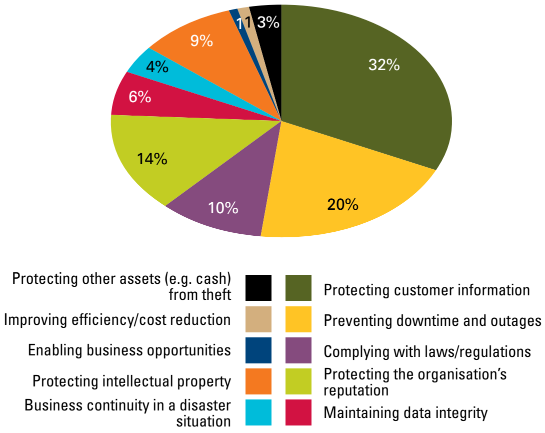
How high a priority is information security to senior management?

Figure 3 *(based on 1,204 responses)*



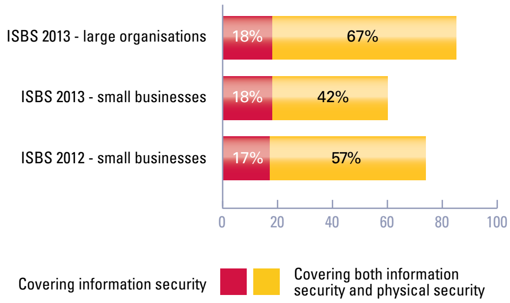
What is the main driver for information security expenditure?

Figure 4 *(based on 160 responses)*



How many respondents carry out security risk assessment?

Figure 5 *(based on 146 responses)*



Attitudes to information security

As in the past, companies continue to prioritise information security. 76% of large organisations and 83% of small businesses believe security is a high or very high priority to their senior management. This is consistent with previous years' results.

There's still a significant industry variation. The financial services, government and technology sectors give information security a relatively high priority. Technology companies give the highest priority on average, while travel, leisure and entertainment companies are least likely to prioritise security. The pharmaceutical and retail sectors both give lower priority to security than average.

In 2010, we saw small businesses overtake large ones in the priority given to security. This trend has continued in 2013, though the difference remains small. There's been a small rise in security priority among large organisations. However, some respondents in large organisations expressed concerns about the lack of priority they see and the impact this has. This is often connected with lack of visible action at board level.

Following reports in the media of similar attacks, a large technology company discovered that hackers had accessed their website through a known vulnerability. The attack specifically targeted the organisation and was facilitated by the lack of priority placed on security. The company suffered significant adverse media coverage after taking a month to restore business as usual.

The top four drivers for security expenditure are the same as in 2012. The most common driver by a large margin continues to be protecting customer information. There's been a small shift towards preventing downtime and protecting reputation. Compliance with laws and regulations remains particularly important in the financial services and government sectors.

The number of small businesses that formally assess security risks has dropped by 15%. This is worrying at a time when both cyber threats and business use of technology are rapidly evolving. As in the past, most large organisations consider both physical and information security risks. Utilities, travel and distribution companies are most likely to conduct risk assessment. The weakest sectors are leisure, health and property; less than half of them assess their security risks. There's still a strong correlation between security priority and risk assessment; three quarters of companies where security is a high priority assess security risks but only half where security is a low priority.

A couple of new questions asked whether respondents include cyber risks in their overall risk register, and whether their risk assessment included insider risks. The results are encouraging; in both cases, 85% of respondents responded positively. There was little difference between large and small businesses in this respect. In contrast, organisations seem to struggle more with dealing with the risks posed by third parties involved in their supply chain.

Management at a small London insurer didn't focus enough on security at their service provider – this led to a substantial data security breach. Information (such as announcements and business development reports) which they believed could only be accessed internally was actually being indexed by web crawlers and being made available in search rankings. It took nearly a month to detect the problem, and then systems had to be taken offline for a week to fix it.

81% of respondents have briefed their board or senior management on cyber risks. The frequency of briefing varied considerably, however. 43% brief at least monthly, while 15% rely on annual or less frequent briefings. The company size doesn't appear to be a major determinant of the frequency of briefings – this seems much more connected with the priority given to security and the proactivity of those responsible for security.

Changing environment

Companies are increasingly adopting remotely hosted services (often referred to as cloud computing) as an affordable and easily accessible alternative to internal IT systems. Roughly four fifths of respondents are using at least one cloud computing service, up from 73% in 2012.

Website and email remain the most commonly used services, particularly for small businesses, where 55% of websites are external and just under two-fifths use a hosted email solution. In contrast, only 14% of large organisations use an externally hosted email service. Large organisations are more likely to use externally hosted payroll processing solutions.

The biggest rise in cloud computing usage has been data storage on the cloud. Interestingly, there's been a significant shift in who is storing data on the cloud. More large organisations are using online data storage, while the adoption rate among small businesses (who previously pioneered this) has dropped by 9%. One in six large organisations is also using cloud computing solutions other than those listed.

53% of organisations with externally hosted services believe these are critical to their business, up slightly from 47% in 2012; in contrast, only 6% report that they aren't important, the same as in 2012. Three-tenths of organisations of national importance (i.e. financial services, telecommunications and utilities) critically depend on externally hosted services, down somewhat on a year ago. Leisure companies and retailers are most likely to have business critical externally hosted services; roughly two-thirds do so. Small businesses are slightly more likely to have critical externally hosted services than large organisations.

Increasing numbers of companies are storing confidential data on the Internet. 83% of large organisations and around three quarters of small ones have confidential or highly confidential data on the cloud. Manufacturing, and financial services companies are most likely to have confidential data on the Internet.

Use of social networking sites hasn't changed greatly since last year. Roughly half of respondents believe social networks are important to their business, a statistic that applies to both small and large businesses.

We continue to see increased penetration of smartphones and tablets into UK businesses. 87% of large organisations (and 65% of small businesses) now allow mobile devices to connect to their systems remotely, both up on 2012 levels.

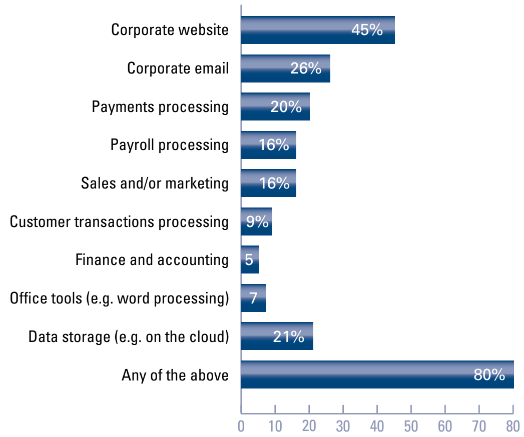
While there are business benefits from the use of social networks and mobile devices, companies also need to be aware of the data loss and security risks associated with them.

An associate of a large consultancy bought tablet computers and used them with a client without checking with the IT department. To make this work, he used Dropbox to store client confidential data, without getting security clearance from either the consultancy or the client.

In this changing environment, responsibilities for owning critical data and for protecting it often become unclear, particularly in large organisations – 33% said the responsibilities were not clear, versus only 22% where responsibilities were very clear. Smaller businesses tend to be less confused – 48% were very clear, versus 15% that were not clear.

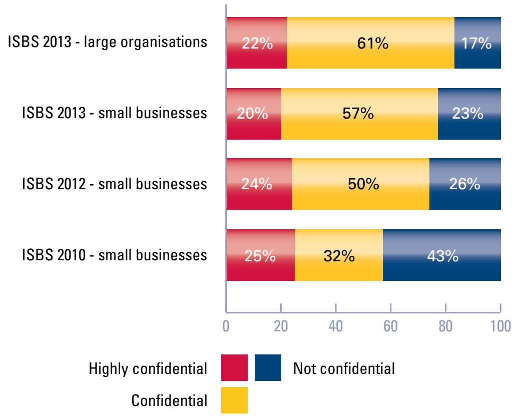
Which business processes have respondents outsourced to external providers over the Internet?

Figure 6 *(based on 172 responses)*



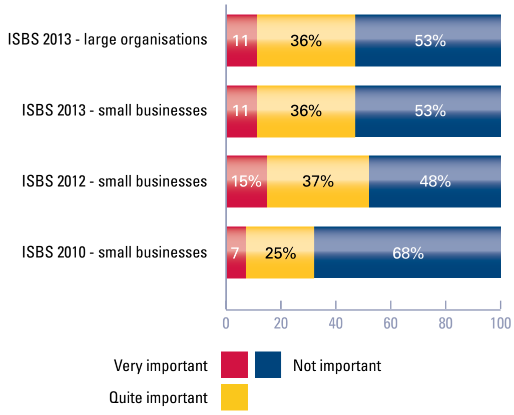
How confidential is the data that respondents store on the Internet?

Figure 7 *(based on 98 responses)*



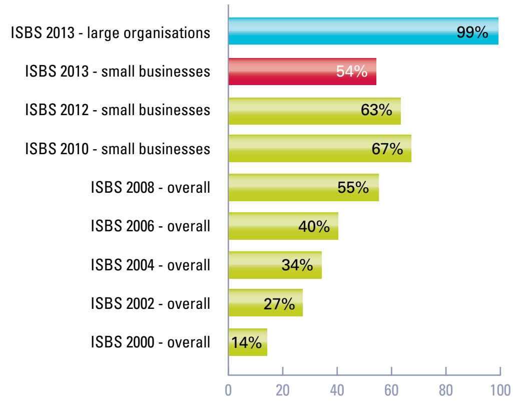
How important is the use of social networking sites to the organisation?

Figure 8 *(based on 137 responses)*



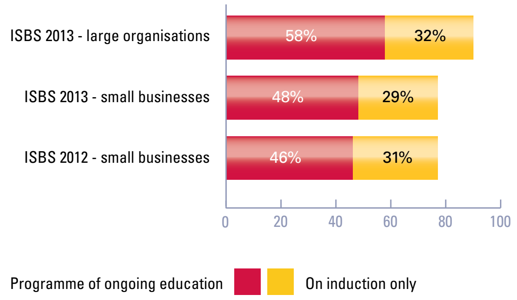
How many respondents have a formally documented information security policy?

Figure 9 *(based on 152 responses)*



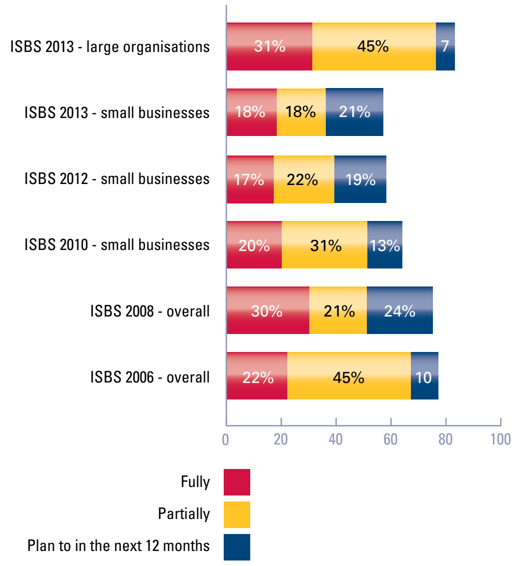
How do respondents ensure staff are aware of security threats?

Figure 10 *(based on 159 responses)*



How many respondents that are aware of ISO 27001 have implemented it?

Figure 11 *(based on 132 responses)*



Security culture

Encouragingly, almost every large organisation now has a written security policy. In contrast, adoption levels in small businesses have fallen back a bit since the 2010 peak. Many small businesses instead rely on word of mouth.

Having a security policy is just the start; to prevent breaches, senior management need to lead by example and ensure staff understand the policy and change their behaviour. Less than a quarter of respondents with a security policy believe their staff have a very good understanding of it; 34% say the level of understanding is poor.

There's a clear payback from investing in staff training. 93% of companies where the security policy was poorly understood had staff-related breaches versus 47% where the policy was well understood.

Worryingly, levels of training haven't improved much – 42% of large organisations don't provide staff with any ongoing security awareness training, and 10% don't even brief staff on induction. Many instead seem to wait until they have a serious breach before training staff.

An employee at a small telecoms provider inadvertently infected a laptop with malicious software, leading to the total loss of its data. There was a clear process for reporting and dealing with such situations, so the incident was resolved within a day. Afterwards, staff received extra training on security risks.

In 2012, the UK Government issued guidance to businesses on how to protect themselves from cyber security threats ("the Ten Steps"). 30% of large organisations had used this guidance. The most popular other sources for evaluating cyber threats were discussions with senior management and views of internal security experts. Small businesses place more influence on news media stories, medium-sized businesses on security vendors and large organisations on guidance from industry bodies.

A government warning enabled a small educational body in the North-West to detect that its systems had been used to send out junk email ("spam"). The incident was then dealt with quickly and staff briefed to avoid any recurrence.

Reporting in the media of similar incidents helped a large manufacturer to detect that staff had deliberately misused confidential data. It took several man-weeks to investigate the breach, but the main impact was reputational damage from adverse media coverage.

Business adoption of ISO 27001 remains at similar levels to a year ago - around a quarter of respondents have fully implemented it, but a similar number haven't and don't plan to.

94% of large organisations have a formal incident response process in place, and more than half of them also have a response team in place. Small businesses are less well prepared – 51% have contingency plans, but this up on last year's 40%.

It took a large pharmaceutical company nearly a month to discover that an attacker had accessed its internal network. The technical configuration was poorly designed and hadn't been kept up to date. There were no contingency plans in place, so resolving the issue took over 100 man-days and cost over £100,000. Afterwards, the company deployed new security systems and changed its policies and procedures.

Investing in security

Understanding the exact spending on security has always been challenging because each organisation manages its expenditure differently. Information security spending often forms part of the overall IT spending given its close relationship to IT. So, this survey has historically used the percentage of IT budget spent as a guide to the level of investment in security.

Respondents now spend 10% of their IT budget on security on average; this is up from 8% in 2012 and is the highest level ever recorded in this survey. Small and medium-sized companies spend slightly more of their IT budget on security than large organisations, on average 12% of IT budget.

As in the past, the priority that senior management place on security strongly correlates with the amount spent on it. When security is a very high priority, average spend is 16% of IT budget. This falls to only 4% when security is a low priority.

92% of the respondents are expecting to spend at least the same on security next year and 47% expect to spend more. Large organisations are expecting the biggest increase in expenditure on security defences next year.

Organisations that suffered a breach during the year spent on average less of their IT budget on security than those that didn't. Most of them spent money on corrective actions after the breach, which means their pre-breach spending was even lower. This suggests they had under-spent on preventative controls before the breach, and that businesses that invest in preventative controls are less likely to have breaches. Failure to invest in preventative controls can be a false economy.

A mid-sized energy company suffered disk corruption in their storage area network. Unfortunately, it hadn't been designed with sufficient redundancy in place. As a result, it took nearly a month to restore service to 'business as usual', after several man-weeks of effort and tens of thousands of pounds spent.

The gap between the best and worst spenders continues to widen. Roughly one in six organisations now spends less than 1% of IT budget on security; this is up from one in eight in 2012.

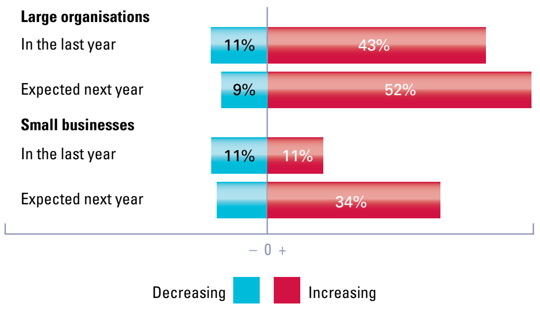
The picture varies by region. Almost half of London based companies are expecting to spend more on information security next year. This compares with only one in four in the Midlands.

Telecoms providers and government bodies spend the most on security, 12.6% of IT budget on average. Other big spending sectors include services, health and technology sectors, all at around 11% of IT budget on average. The financial services sector spent a little less than in the past, but expect the biggest expenditure increase next year. Retailers and property companies have historically been relatively low spenders on security defences.

There's some evidence that skills shortages may be inhibiting what companies spend on security. Only 13% of respondents are very confident that they will be able to source sufficient security skills to enable them to manage their security risks. This compares with 20% who aren't confident. The skills shortage appears most acute in large organisations, where 9% are very confident versus 25% that aren't confident.

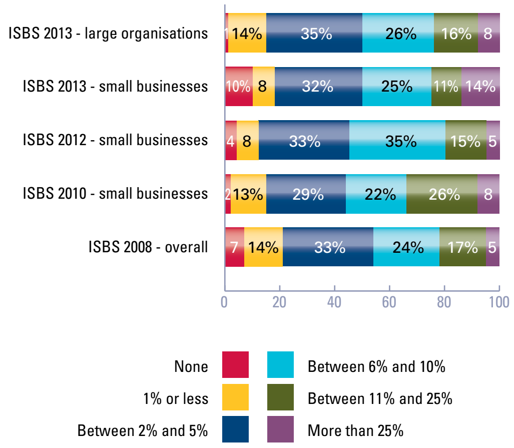
How is information security expenditure changing?

Figure 12 *(based on 145 responses)*



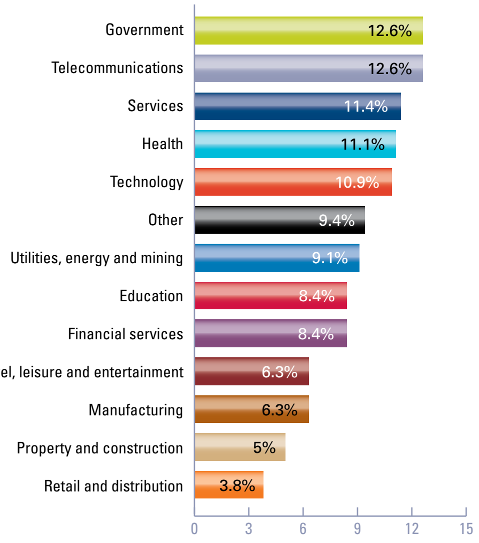
What percentage of IT budget was spent on information security, if any?

Figure 13 *(based on 845 responses)*



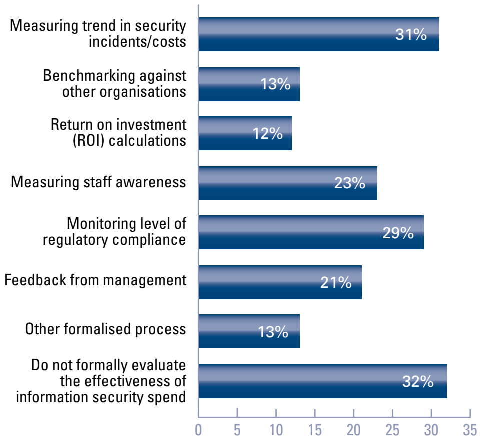
Which sectors spend on average the highest % of their IT budgets on security?

Figure 14 *(based on 845 responses)*



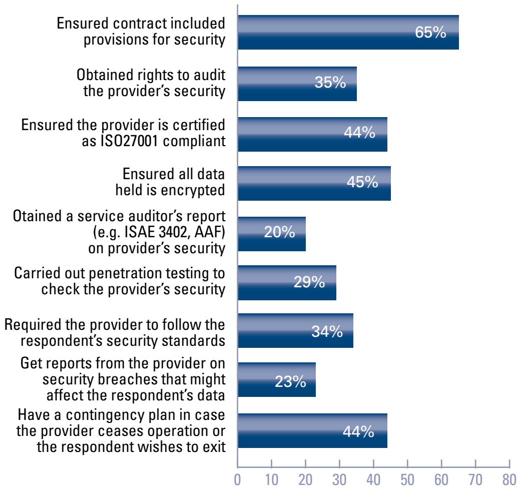
How do respondents measure the effectiveness of their security expenditure?

Figure 15 *(based on 164 responses)*



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

Figure 16 *(based on 172 responses)*



Evaluating spend effectiveness

Cost control is high up the agenda of most businesses today. We might, therefore, expect businesses to evaluate the effectiveness of their security expenditure. Yet, a third of respondents don't try to do this. Practices here haven't improved over the last year.

Among those that try to measure the effectiveness of security, trend analysis of the number or cost of security incidents remains the most common measure employed; this is consistent with last year's results. Given the increasing legal and regulatory focus on cyber security, monitoring the level of regulatory compliance is rising in popularity.

Over the last decade, organisations haven't made much progress in treating security as an investment rather than an overhead. Only 12% of organisations try to calculate return on investment on their security expenditure; this is worse than we saw in 2012, and substantially down on the 39% figure for 2004.

Demand for assurance

More than three quarters of respondents now use outsourced services. Worryingly, 4% of respondents have detected a security or data breach that affected a cloud-based service they use. Given that only 23% get reports of breaches from their provider, this suggests the actual breach levels may be much higher. Sadly, breach information is often only requested after a major breach has occurred.

A government body in the South-West suffered a major data breach when poor practices at a third party led to the accidental release of private data. Despite internal controls discovering this within a few hours, it took several man-weeks of effort to investigate and fix the incident, and tens of thousands of pounds of business was lost as a result. Afterwards, the body took disciplinary action against the people responsible, as well as increasing their monitoring of third parties' security.

Large organisations are generally more diligent at ensuring third parties have adequate security. For example, they are three times as likely as small businesses to obtain audit rights and twice as likely to carry out penetration testing. It's important that penetration testing is done carefully, though.

A large technology company suffered when one of their customers decided to carry out an unauthorised destructive penetration test on their systems. This took down systems and led to customer complaints. Fortunately, the breach was identified and resolved immediately.

In certain areas, there's little difference between large and small businesses. Roughly half of each have contingency plans in place in case the provider ceases business, and a similar proportion check that data is encrypted. Small companies are slightly more likely to seek ISO27001 compliance from their provider.

85% of large organisations and 61% of small businesses have been asked by their customers to comply with security standards. For small businesses, this is largely either government standards (24% affected) or payment card standards (18%). 45% of large organisations have been asked for ISO27001 compliance, 36% for government standards and 30% for payment card standards. 12% of large organisations, particularly in the technology and financial services sectors, have been asked to provide an independent service auditor's report (e.g. ISAE 3402) over their security, and this number is rising.

Social networks and mobile computing

Use of the Internet is increasingly important to businesses, either as a way of operating cloud services or to access social networks. Simply blocking all staff Internet access no longer works for most businesses; instead, organisations tend to restrict which staff have access and block inappropriate sites. The proportion of respondents using different techniques is very similar to that seen a year ago. As in the past, large organisations tend to have better controls than small ones.

Worryingly, 14% of large organisations have detected a security breach involving social networking sites in the last year. There's a strong correlation between those with monitoring controls in place and those detecting breaches; companies that don't monitor postings to social networking sites are three times less likely to have detected a breach as those that do. This suggests that most breaches aren't being detected.

Staff at a large insurer in the South-West misused Facebook (as well as internal email systems). Fortunately, routine security monitoring picked this up within a few days and it was quickly dealt with.

Removable media devices continue to be an area of exposure. 4% of the worst security breaches of the year were caused at least partly by portable media bypassing security defences.

A large London insurer suffered a significant data breach when a contractor downloaded sensitive project files onto a removable storage device prior to his termination. Routine security monitoring detected the breach almost immediately and there was an effective contingency plan in place to deal with it. Despite this, it still cost more than £10,000 to respond to the incident. Following the breach, the company implemented additional policies and procedures, including changing how they vet potential employees.

Smartphones and tablets present another area of security exposure. Roughly half of large and small businesses now allow staff to connect their own phones or tablets to corporate systems (often referred to as Bring Your Own Device).

Inevitably, this has resulted in security breaches. 9% of large organisations had a data or security breach in the last year involving smartphones or tablets. Controls appear to be lagging behind usage – a third of small businesses still haven't thought about mobile security. Only a third of respondents encrypt the data held on mobile phones.

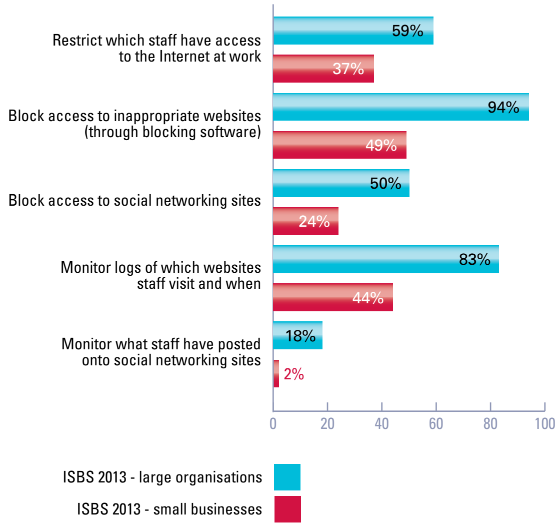
Often a user will access both personal and business email through the same mobile device – this can lead to blurring of boundaries.

An employee at a large government body sent sensitive emails from their work email account to their personal account. This was only discovered by accident. Due to the sensitive nature of the information involved, it's hard to put a value on the lost data. After the breach, the body took legal action against the employee, improved vetting processes and invested in additional staff training.

Given the rapid changes to the way that businesses are using technology, it's important that businesses have a flexible approach to security. Security risks need to be frequently reviewed and senior management engaged. Today's processes won't necessarily protect against tomorrow's threats.

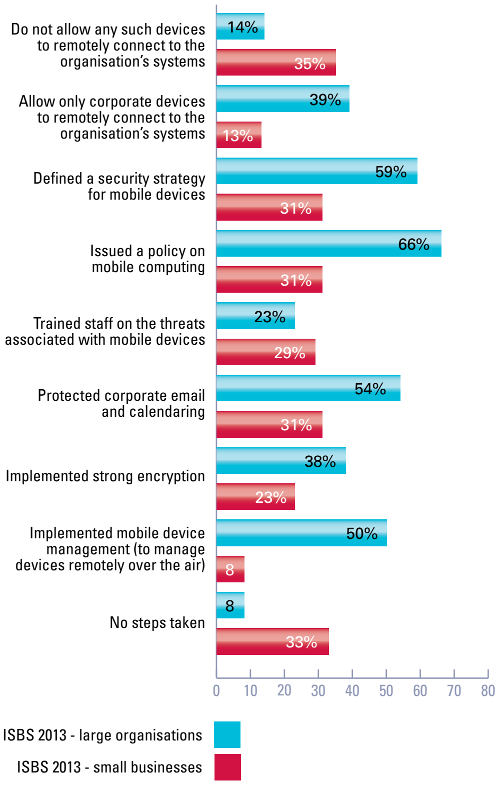
How do respondents prevent staff misuse of the web and social networking sites?

Figure 17 *(based on 163 responses)*



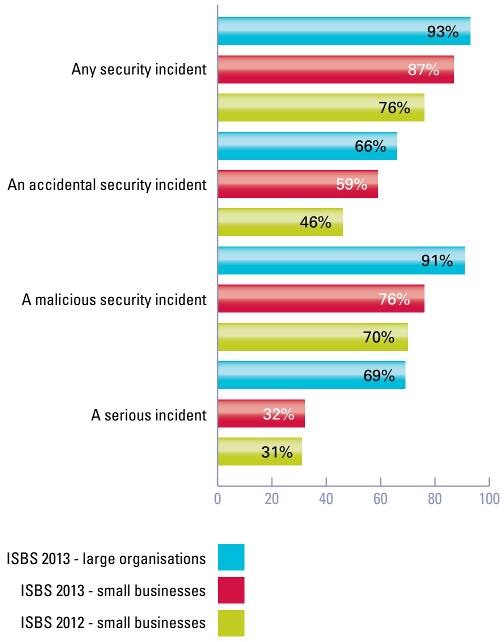
What steps have respondents taken to mitigate the risks associated with staff using smartphones or tablets?

Figure 18 *(based on 167 responses)*



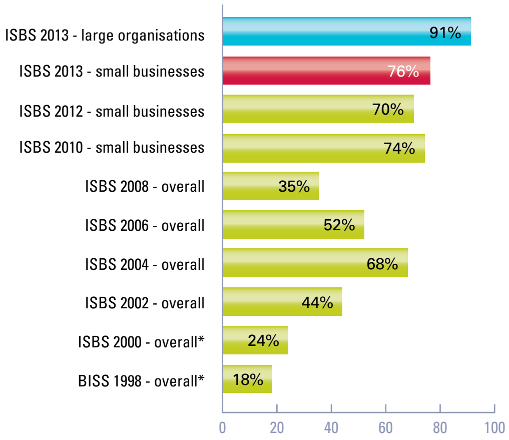
In the last year, how many respondents had...

Figure 19 *(based on 717 responses)*



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

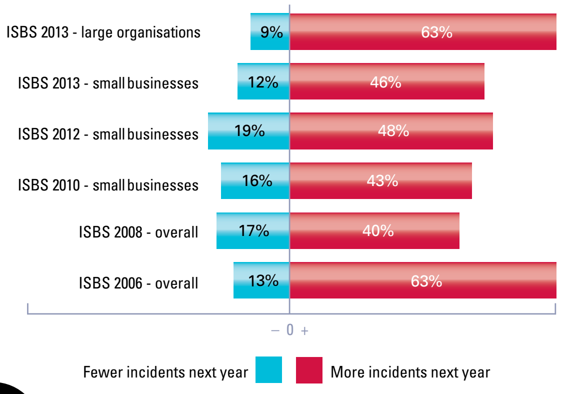
Figure 20 *(based on 708 responses)*



* 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 *(based on 145 responses)*



Incidence of security breaches

The number of respondents reporting that they have had security incidents is at an all-time high. Large organisations continue to be affected badly - nine tenths had malicious breaches, and two thirds of them had a serious incident. The biggest rise, however, was for small businesses - 87% of them reported a breach, a level previous only seen for large businesses.

As in the past, large organisations report more breaches than small ones. The size and complexity of the organisation is a factor. Also, the more staff there are, the greater the chance of staff-related incidents. However, the maturity of controls is another reason - large organisations are more likely to detect sophisticated breaches than small businesses.

No sector or region was immune from malicious security breaches. At least seven-tenths of respondents in every sector reported malicious breaches, as did at least three-quarters of respondents from every region.

A disgruntled employee at a large utility company stole some sensitive information which he had access to as part of his job and began selling this. The breach was discovered by accident, over a month after it started. The value of the lost data was several hundred thousand pounds, but the impact on the business of the investigation and aftermath was even greater. The lack of a contingency plan contributed to this cost. After the breach, the company deployed new systems, changed its procedures and introduced a formalised post-incident review process.

The number of accidental incidents among small businesses has increased compared to 2012.

The pattern of how organisations detected their most significant breach of the year is similar to last year. Routine internal security monitoring detected 42% of the worst breaches, while 30% were obvious from their business impact (e.g. systems outage, assets lost). 9% of organisations' worst security incidents were discovered by accident, up from 6% in 2012.

This year, we asked a new question about how quickly organisations detected their worst breach of the year. Most detected the breach in less than a day. However, 5% took several weeks to detect and a further 6% took more than a month. These breaches tended to be in large organisations, and typically involved loss of confidential data, outsider attacks or data protection breaches.

More than half the respondents expect the number of breaches to increase in the next year; this is five times as many as expect fewer incidents. No sector was optimistic; financial services and the public sector were particularly concerned about the future.

About a third of respondents are very or quite confident that they will be able to detect the latest generation of attacks that are designed to evade standard protection tools; technology companies are among the most confident. However, about a third aren't confident, and this is particularly the case in large organisations, the public sector and financial services.

With this view of the future, it's crucial to have the adequate skills to prevent, detect and manage breaches. Roughly half of respondents are very or quite confident that they'll be able to access the skills they need. In contrast, one in five aren't confident. This is particularly the case for large organisations, who are twice as likely to worry about skills shortages as small businesses. A strategic approach to risk assessment is key to identifying the skill requirements.

Type of security incident

System failures and data corruptions affected more respondents than a year ago. Two-thirds of large organisations and three-fifths of small businesses experienced such problems. All industry sectors were affected by these incidents. Telecommunications, education, retail, leisure and manufacturing were most likely to have systems failures. Agriculture, property and health had the fewest problems with their systems.

Failure to keep configuration up to date led to a network drive failing at a small media company in London. The business was seriously disrupted for several days, during which time staff lost access to their data. No steps were taken afterwards to prevent similar incidents in the future.

The number of respondents infected by malicious software remains similar to the levels reported in 2012. Two-fifths of small businesses and three-fifths of larger companies were infected. The amount invested in anti-virus solutions appears to be at least stemming the tide. The average number of virus infections in large businesses is relatively low, but worryingly the average number of infections in small businesses has risen. It's important that companies don't become complacent.

Management at a healthcare provider in the South-East failed to put a high enough priority on security patching. As a result, the *Conficker* worm infected their systems, causing very serious disruption for several days and resulting complaints from their patients. It took several man-months of effort to eliminate the infection.

Computer fraud and theft levels remain very similar to those seen in the last two surveys. More small businesses were affected than in the past, but on average each affected business suffered fewer breaches.

There's been a big increase in other staff-related incidents at small businesses, both in terms of number of companies affected and the average number of breaches each suffered. These are now at record levels. For large organisations, the picture is mixed – 84% is the highest figure ever recorded, but the average number of breaches each affected business suffered has dropped.

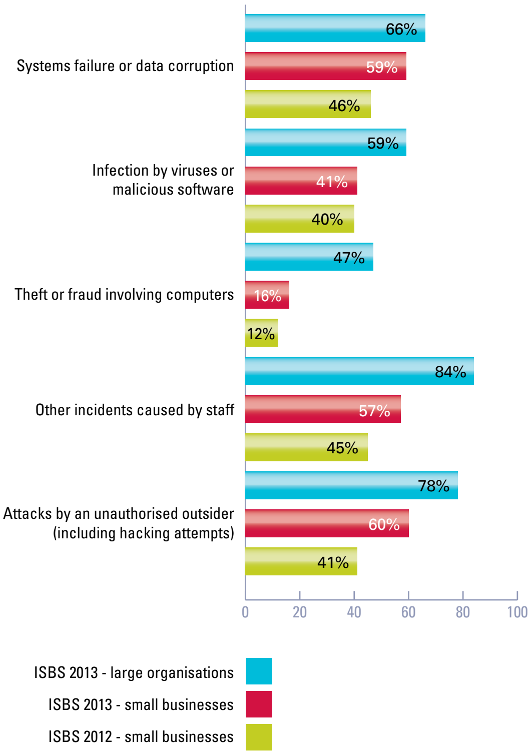
Outsider attacks also increased substantially, especially against small businesses; 63% report being attacked, up from 41% a year ago. Large organisations still bear the brunt of attacks, with the average company having a serious attack every few days. But, small businesses are rapidly becoming a target too, on average suffering a serious attack once every six weeks.

The public website of a financial services provider was attacked using SQL injection. Poor design of the site's technical configuration made it vulnerable to the attack. This resulted in the attackers then sending a large number of "phishing" emails to staff. This caused a lot of disruption for about a day. After the attack, the company changed its website configuration and also trained staff on security risks.

The average number of breaches suffered in the year has gone up by roughly 50% for both large and small businesses. As in the past, we quote the median figure since this is more typical of what the average business suffers than the mean, which is distorted by a small tail of respondents with very large numbers of breaches. For reference, the mean is roughly 2,500 breaches per annum for small businesses and roughly 6,500 for large businesses. Hacking attacks are the biggest single contributor – excluding these, the mean is roughly 700 breaches per annum for small businesses (dominated by staff-related incidents) and 3,500 breaches per annum for large organisations (mostly staff-related and outsider attacks).

What type of breaches did respondents suffer?

Figure 22 *(based on 686 responses)*



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

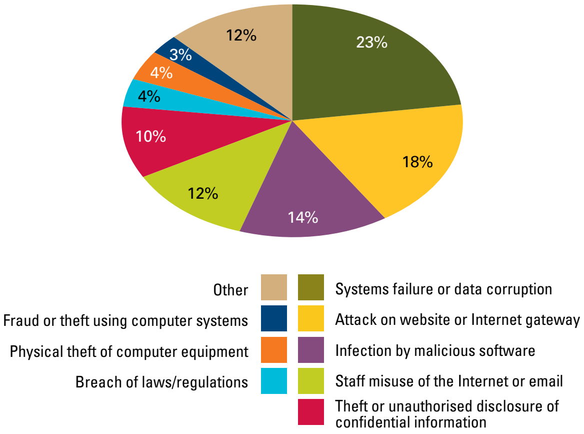
Figure 23 *(based on 686 responses)*

	Large organisations	Small businesses
Systems failure or data corruption	3 (3)	2 (2)
Infection by viruses or other malicious software	3 (3)	3 (1)
Theft or fraud involving computers	5 (5)	2 (3)
Other incidents caused by staff	18 (24)	11 (8)
Attacks by an unauthorised outsider (including hacking attempts)	106 (54)	10 (8)
Any security incident	113 (71)	17 (11)

Equivalent comparative statistics from ISBS 2012 are shown in brackets

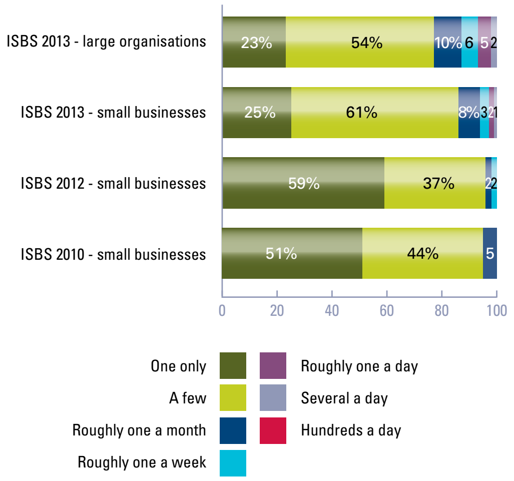
What was the worst security incident faced by respondents?

Figure 24 *(based on 147 responses)*



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

Figure 25 *(based on 656 responses)*



Infection by viruses and malicious software

The virus infection rate appears to have stabilised, yet many businesses are still being caught out. Often, staff are tricked into infecting themselves.

A volunteer at a small Yorkshire charity clicked on a link in an email and inadvertently infected the computer with a blackmail virus. This was easily removed with anti-virus software.

Worryingly, the survey results highlight that many organisations have left themselves vulnerable by not applying patches. There were a surprising number of major incidents involving the *Conficker* worm, despite a patch being available for this since 2008. The impact of these infections varied considerably.

An employee at a large bank plugged an unauthorised USB device into an unpatched computer, and so inadvertently introduced the *Conficker* worm into the network. This caused very serious business disruption for several days. Cleaning up the infection involved many man-months of effort and cost several hundred thousand pounds. In the wake of the breach, the bank disciplined the employee responsible and trained its staff on security risks. The technical systems configuration was also enhanced, with real-time monitoring introduced.

An unpatched system at a large agricultural business in the South-East became infected by the *Conficker* worm. Routine security monitoring picked it up immediately and an effective contingency plan kicked in. As a result, the business disruption was minor and dealt with within a day.

Failure to patch systems at a large bank led to an infection by the *Poison Ivy* backdoor. There was an effective contingency plan in place, but it still took several man-months of effort to eliminate the infection from systems. After the breach, procedures (in particular for rolling out operating system patches) were improved.

More and more sophisticated viruses are written every day to target specific system weaknesses. The race between the attacker and the anti-virus solution providers has never stopped. For example, *SpyEye* and *ZeuS* formed a new variant attacking mobile phone banking information. *Shamoon*, designed to target computers running Microsoft Windows in the energy sector, was discovered in August 2012. The *Flame* or *sKyWIper* virus, first seen in May 2012, was claimed to be the most sophisticated and complex malware ever found. Virus writers continue to move their historic focus away from Windows computers onto other platforms such Apple and Android operating systems for mobile devices. Some respondents had suffered from these newer attacks.

A government warning enabled a military body to detect that several of their officers had been subject to targeted attacks using the *Miniduke* program. Investigation showed that the in-place controls had been sufficient to block the attack.

Virus infections continue to be among the more costly breaches to deal with. Despite making up only 2% of the number of security breaches, virus infections contributed 14% of the worst breaches of the year. Virus infections were particularly significant in small businesses, where they contribute a sixth of the total breaches (up significantly on last year) and a third of the worst ones.

Multiple systems at a large outsource services provider became infected by a virus which spread by manipulating networking packets and then began reporting to command and control servers based in Eastern Europe and China. Fortunately, routine internal security monitoring identified this within a few hours. However, it caused serious disruption for a few weeks, as well as taking several man-weeks of effort to eliminate from the network. The value of any data lost is unknown. Following the breach, the company deployed new systems as well as changing the configuration of their existing systems.

Systems failure and data corruption

Around two-thirds of large organisations and three-fifths of small ones suffered from systems failure or data corruption during the year. The number of small businesses having problems increased, perhaps due to the increased complexity of their systems. The main causes of incidents were hardware failures, problems with backups and poorly tested changes to systems.

A software bug at a large educational body in the Midlands led to hundreds of students' personal data being mistakenly handed out to other students. Several days of complaints and follow-up ensued.

A systems change at a large bank based in central London went wrong, leading to a failure in the main payment system. This made it impossible to check payment information properly, which resulted in some erroneous payments being made.

While most incidents involved technology faults, human error also contributes. There's a clear correlation between these incidents and staff security awareness. 80% of organisations whose security policy is poorly understood had system-related problems, compared to 50% of those whose policy is well understood.

An error by a developer at a large educational body in East Anglia took down systems for several days, causing serious disruption.

Lack of staff awareness, poorly designed configuration and process failures combined to allow an employee at a medium sized technology company to delete important data from a critical system. It took nearly a month to restore the system, after more than a man-week of effort. Afterwards, the company changed its procedures, the configuration of its live systems and its backup and contingency plans.

Deliberate sabotage by staff remains relatively rare. 6% of respondents were affected, the same as in 2010 and 2012. Such breaches were almost always isolated incidents.

Computer theft and fraud

Computer theft and fraud remain at relatively high levels compared with past years' results. The results for large organisations are at similar levels to 2012, but small businesses are more likely to suffer than in the past. Twice as many small businesses reported theft by outsiders of confidential data or intellectual property as did so in 2012.

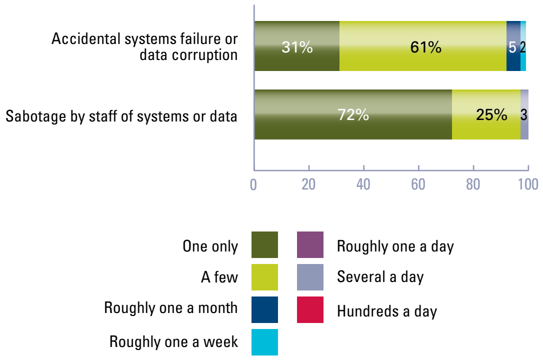
A leaver from a large financial services company based in London downloaded confidential data onto a portable media device, before taking it to his new employer (a competitor). The breach led to customer complaints, which spurred the firm onto legal action against the former employee.

Physical theft of computers remains the most common cause of breaches. The perpetrators are fairly evenly split between outsiders and staff. Much of the time, failure to encrypt data means the impact of the thefts is much greater than the replacement cost of the equipment.

Thieves stole a classified laptop belonging to a large technology company from a parked vehicle. It was an indiscriminate attack and the value of the laptop was only a few hundred pounds. However, the data on it was worth much more, and the investigation that followed consumed several man-weeks of effort and cost tens of thousands of pounds.

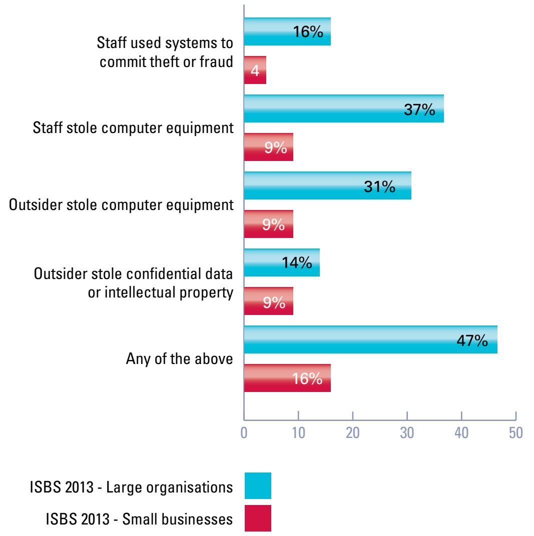
How many systems failures or data corruptions did the affected organisations suffer in the last year?

Figure 26 *(based on 662 responses)*



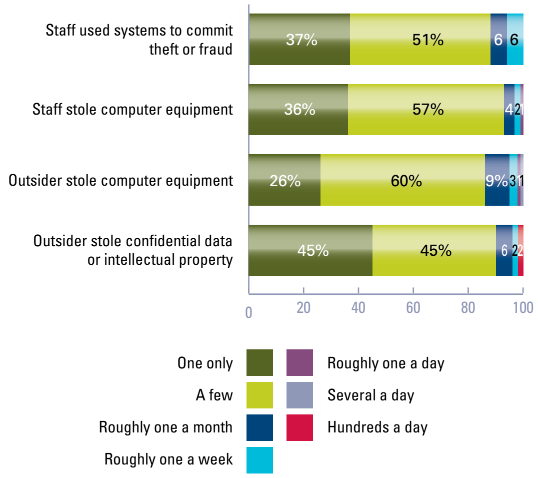
What type of theft and fraud did respondents suffer?

Figure 27 *(based on 551 responses)*



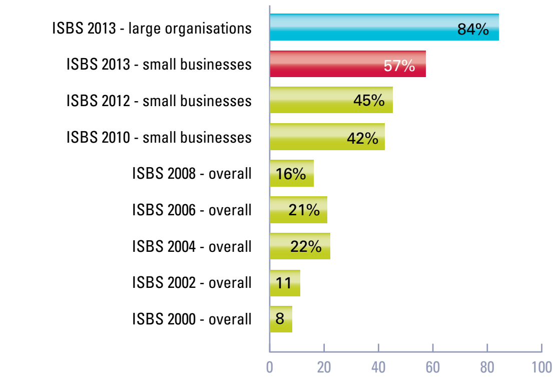
How many thefts or frauds did affected organisations have last year?

Figure 28 *(based on 551 responses)*



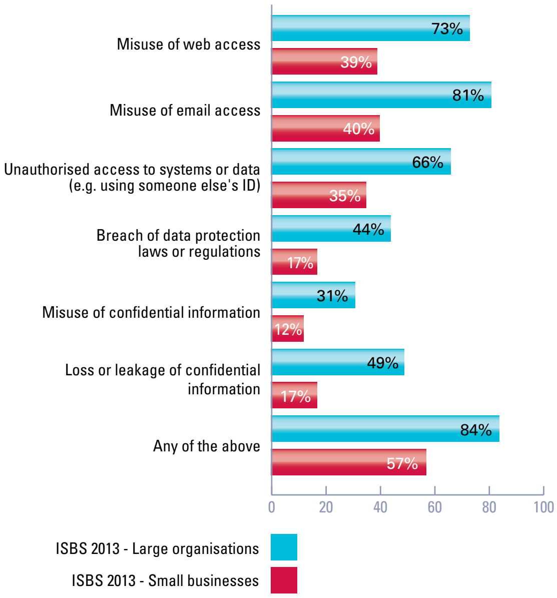
How many respondents had staff-related incidents?

Figure 29 *(based on 632 responses)*



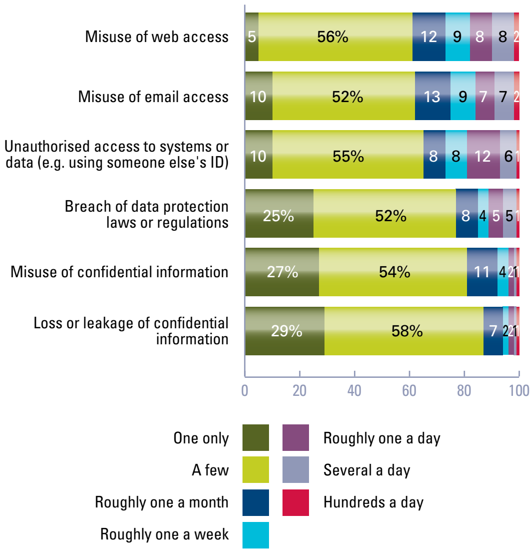
What type of staff-related incidents did respondents suffer?

Figure 30 *(based on 528 responses)*



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

Figure 31 *(based on 528 responses)*



Other incidents caused by staff

Staff-related breaches include both misuse of systems and inadvertent leakage of confidential data. Most businesses of all sizes now have to deal with this kind of breach, with the average small business having one such breach a month. More respondents were affected than ever before recorded in this survey.

Most staff-related incidents involved staff misuse of the Internet or email. This happened in more than three-quarters of large organisations and around two-fifths of small businesses. The average affected company had about one breach a month, though some reported many more.

A member of staff at a small security consultancy firm accidently replied to all recipients of an email with an inappropriate response. This small mistake resulted in several thousand pounds of lost business, and consumed several days of management time dealing with the complaints from customers. The employee was disciplined and additional staff training was implemented.

The number of small businesses reporting unauthorised access to others' user accounts has doubled in the last year. This is now the third most reported staff-related incident. Affected businesses typically had only a few such breaches a year.

There's a strong correlation between the extent to which staff understand the security policy and the likelihood of staff-related breaches. Companies with a poorly understood policy were twice as likely to have a staff-related breach as those with a very well understood policy. Monitoring and policing alone aren't sufficient. Companies also need to deploy ongoing information security training and awareness programmes.

An employee of a mid-sized government department used their security training to harvest data from public websites without prior consent. Despite being detected within a few hours, the action caused significant reputational damage and consumed several man-weeks of management time.

Data protection breaches occurred in almost half of all large organisations and one in six small businesses. Although few respondents reported large regulatory fines, the costs of investigation, recovery and reputation repairing were often substantial.

Levels of loss or misuse of confidential information by staff are similar to those seen in 2012. Staff accidentally lost confidential information at almost half of large organisations, and actively misused it at a third of them. Staff at one in six small businesses leaked confidential data.

Staff at a medium-sized financial services provider in the Midlands sent confidential data by insecure email. Fortunately, internal security monitoring picked this up, and the data doesn't appear to have been intercepted or misused.

There's quite a lot of variation by sector in the extent of staff-related breaches. Only a quarter of property companies reported such breaches. At the other end of the spectrum 94% of banks and utilities were affected. It's likely that some of this disparity is due to variation in the monitoring and detection of breaches. There's also a significant regional variation – almost every Scottish business reported staff-related breaches, but only about half those from the East of England were affected.

Unauthorised access by outsiders

Cyber attacks have continued to grow in frequency and intensity over the last year. Three quarters of large organisations have detected significant attempts to break into their networks. Three-fifths of small businesses have been attacked. These are the highest levels ever recorded in this survey. The volume of attacks has also increased, with the average large business attacked every few days.

One in five of large organisations and one in six small businesses had been successfully penetrated, again historical highs. Even more worryingly, most of the affected companies were penetrated not just occur once but several times during the year. Educational bodies were the most affected; over half of them had been penetrated. A quarter of banks, utilities and telecoms providers had also been broken into in this way.

A group of hacktivists targeted a large manufacturer in the South-East with an 'advanced persistent threat' (APT) attack. Weak security at a third party enabled the attackers to get in. It took over a month before the routine internal security monitoring picked up the breach, but then an effective incident response plan was invoked. It took several man-weeks of effort to investigate and fix the problem, and the investigation cost tens of thousands of pounds. Following the breach, the company increased its monitoring of third parties to avoid similar incidents in the future.

Denial-of-service attacks have also become more common; they affected two-fifths of large organisations and a quarter of small businesses. Banks and educational bodies were particular targets of these attacks, while health, energy and services companies reported fewer attacks. The attacks typically disabled unprotected websites, but often also affected email, telephony and caused system disruption or outage.

A large technology company suffered a sustained distributed denial-of-service (DDoS) attack specifically targeted against the systems they support. It took several days to return their service to business as usual. Despite the company suffering no direct financial losses, it had to pay tens of thousands of pounds in compensation following customer complaints. Following the incident, the company changed its contingency plans.

A government department suffered a DDoS attack on their externally facing internet gateway. It took over a week to resume normal service, costing over £50,000 and resulting in significant adverse media coverage. As a result, the department changed the configuration of systems and its contingency plans.

The DNS infrastructure for a small technology company in the South-West was targeted, so that the attackers could then use it as part of a DDoS attack against another organisation.

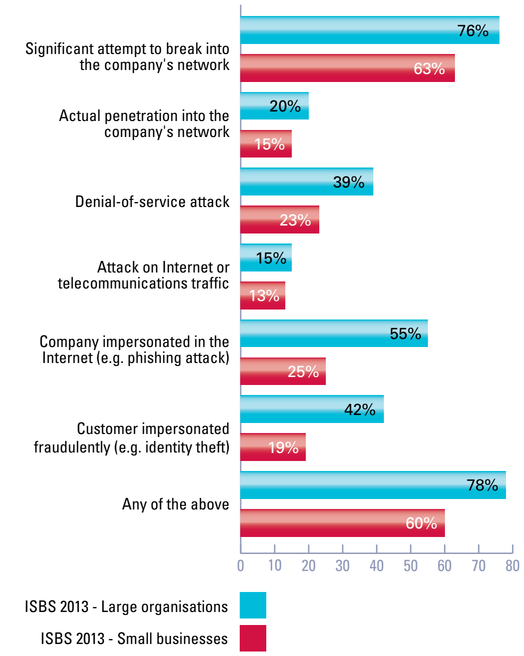
"Phishing" attacks, where attackers on the Internet try to impersonate companies, have increased significantly. Four-fifths of banks and three-fifths of educational bodies were affected. Other sectors were also affected, and the biggest rise was for small businesses. Several affected organisations have to deal with "phishing" attacks several times a day.

Customer impersonation and identity fraud have also risen significantly. More than three-quarters of banks and travel companies were affected. While no sector was immune, only about a quarter of utilities, technology, telecoms, services, pharmaceutical, health, insurance and government bodies had detected this.

Criminals targeted staff at a very large financial services provider, sending them emails that were apparently from people they knew but which contained links to malicious software. While this 'spear phishing' attack didn't result in significant financial or reputational loss, it highlighted that staff weren't aware of the security risks. As a result, additional staff training was put in place to avoid future incidents.

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

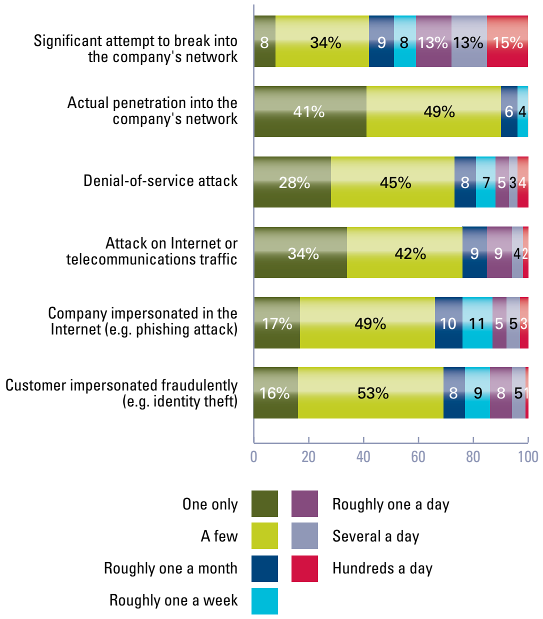
Figure 32 *(based on 544 responses)*



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

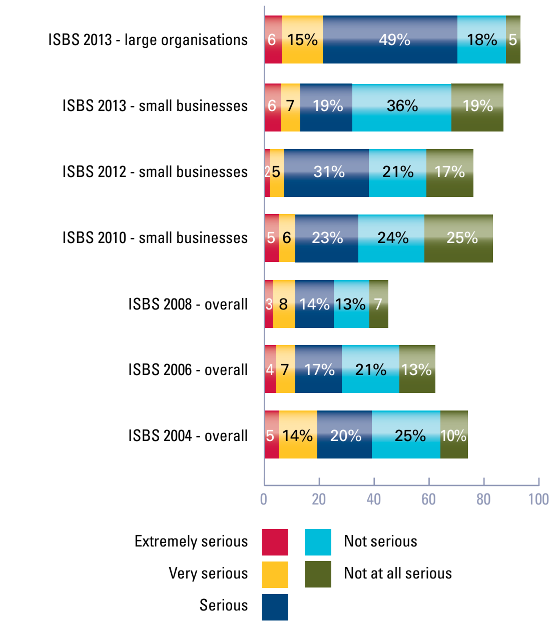
How many incidents did affected organisations have in the last year?

Figure 33 *(based on 544 responses)*



How many respondents had a serious incident?

Figure 34 *(based on 119 responses)*



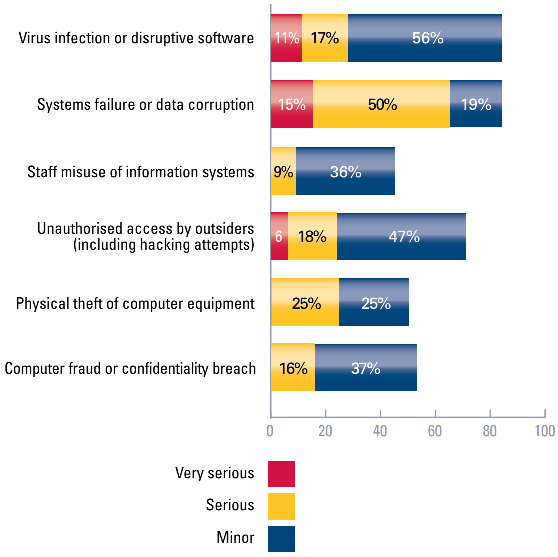
How much disruption to the business did the worst security incident cause?

Figure 35 *(based on 104 responses)*

	None	Less than a day	Between a day and a week	Between a week and a month	More than a month
Very serious disruption	37%	2%	4%	2%	1%
Serious disruption		5%	10%	4%	1%
Minor disruption		10%	10%	5%	1%
Insignificant disruption		5%	2%	1%	0%

Which incidents were most disruptive to business?

Figure 36 *(based on 96 responses)*



Impact of breaches

Security breaches lead to many different types of impact. Direct costs, such as system downtime and cash spent dealing with the breach, are easy to estimate. Indirect costs are harder to determine, especially reputational damage. 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 respondents' subjective assessment of the breach's seriousness. Overall the seriousness of large organisations' worst breach of the year has increased substantially versus 2012. For small businesses, although there are more extremely serious and very serious incidents reported, the average seriousness of worst breaches reported has fallen somewhat.

The vast majority of worst breaches involving theft or unauthorised disclosure of confidential data were serious. In contrast, roughly half of the worst breaches involving staff misuse of the Internet, virus infection or outsider attack weren't serious. Respondents from financial services and government bodies were most likely to have suffered a serious security breach. Those from educational bodies and travel companies were the least concerned about the breaches they'd had.

Business disruption

The length that respondents' worst breaches disrupted operations has increased significantly, to 3-5 days for small businesses and 3-6 days for large ones. It was only 1-2 days on average for both in 2012. Systems failure or data corruption was most likely to cause serious business disruption.

A mid-sized financial services company based in London suffered several hours of systems outage after a well-intended but unstructured change to systems. Unsurprisingly, this led to changes to their change management procedures.

Virus infection and attacks by outsiders are also reasonably likely to cause serious disruption.

A hard disk at a government body in the Channel Islands failed. Unfortunately, the replacement disk installed by a third party had a virus on it. This resulted in serious business disruption over several days, and several man-weeks of effort to clean up the infected systems.

The number of breaches that disrupted the business for more than week has tripled compared with a year ago. And, the proportion with no or insignificant disruption has dropped from 56% to 45%.

A web forum run by a media company based in Greater London was attacked, and had to be taken down for several weeks, causing serious business disruption. This caused significant reputational damage, with many complaints from customers.

Using the same basis as previous surveys, the cost of business disruption from the worst breach of the year appears to have roughly tripled since 2012. The worst breach cost £30,000 to £50,000 for small businesses (up from £7,000 to £14,000) and £300,000 to £600,000 for large organisations (up from £60,000-£120,000). These are similar to the levels seen in 2010.

Incident response costs

The cost of responding to and recovering from an incident can easily outweigh its direct cost. Staff-related incidents may involve lengthy investigation to identify the root cause and build up evidence for subsequent action. System failures and virus infections can take a long time to correct.

A large insurer suffered significant data loss as a result of poor backup processes. It took nearly a month, several man-months of effort and several hundred thousand pounds to recover from the incident. Unsurprisingly, new backup procedures and systems were later introduced.

The average time spent to fix breaches was longer than last year. Among small businesses, the average time spent on responding to incident is 6-12 man-days, up from 2-5 man-days in 2012. The average cost of this time was £2,000-£5,000, plus a further £500-£1,500 in cash costs (down from £1,500-£3,000 in 2012). In large organisations, the effort required was much higher with an average 25-45 man-days, up from 15-30 man-days in 2012. Large organisations incurred £6,000-£13,000 in time costs, and £35,000-£60,000 in cash costs (up from £25,000-£40,000 in 2012) on average.

A temporary employee at a bank abused their access privileges to steal customer information. Fortunately this was picked up by the company's control activities within a week. Dealing with the investigation and customer complaints involved several man-months of effort and cost tens of thousands of pounds.

Financial loss

About a quarter of the worst security breaches of the year led to lost business. The average cost was £300-£600 for small businesses and £10,000-£15,000 for large organisations. In some cases, the amount of business lost was significant.

A large insurance company lost millions of pounds of business and received multiple complaints from customers after their web-site went down. A failure in their monitoring systems meant that business impact triggered the alert rather than the alerting system itself. Unfortunately, their contingency plan was ineffective, so it took several days to restore normal service.

A large insurer lost several hundred thousand pounds of business after an employee copied confidential material to an external mailbox for their own financial gain.

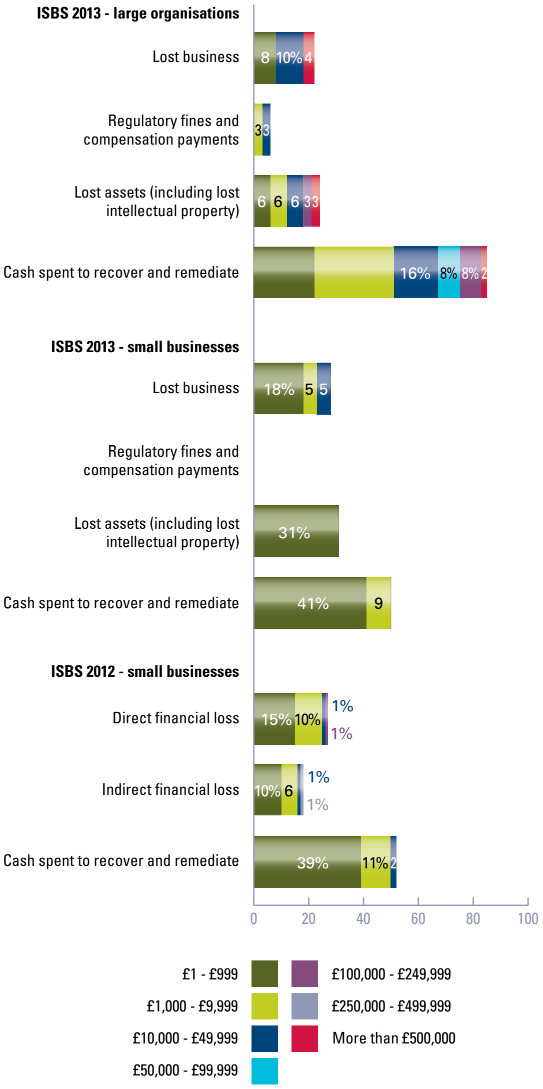
About a third of the worst security breaches of the year resulted in financial loss as a result of lost assets. These included both physical assets and intellectual property. Small companies reported relatively small losses, averaging £150-£350. The picture was much more variable for large organisations, with an average cost of £30,000-£40,000.

Failure to follow defined processes led to inadvertent loss of confidential data at a large financial services provider. Routine security monitoring detected the breach within a few hours, and an effective contingency plan kicked in. However, more than half a million pounds of assets were lost as a result of the breach. Follow-up actions included disciplinary measures, post-incident review and changes to system configuration.

Very few respondents reported losses due to compensation payments and regulatory fines. No small businesses reported any such losses, and it averaged only £750-£1,500 for large organisations.

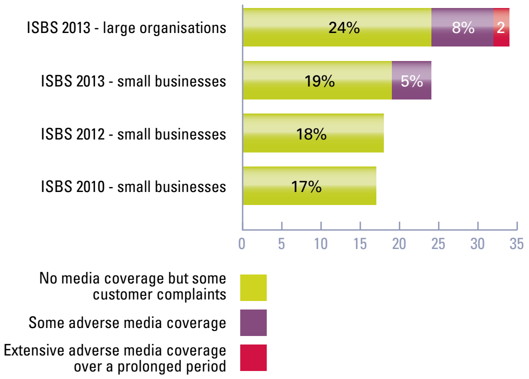
How much cash was lost or spent dealing with the worst security incident of the year?

Figure 37 *(based on 84 responses)*



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

Figure 38 *(based on 94 responses)*



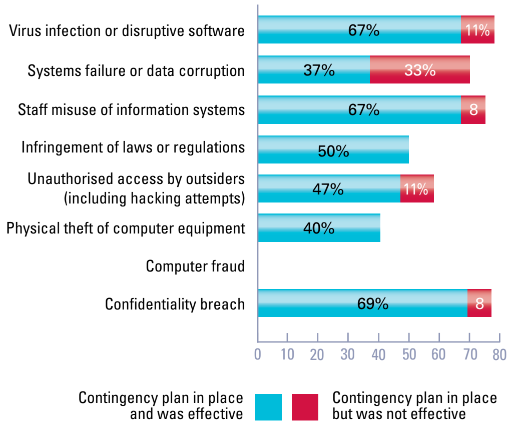
What was the overall cost of an organisation's worst incident in the last year?

Figure 39 *(based on 104 responses)*

	ISBS 2013 small businesses	ISBS 2013 large organisations
Business disruption	£30,000 - £50,000 *over 3-5 days*	£300,000 - £600,000 *over 3-6 days*
Time spent responding to incident	£2,000 - £5,000 *6-12 man-days*	£6,000 - £13,000 *25-45 man-days*
Lost business	£300 - £600	£10,000 - £15,000
Direct cash spent responding to incident	£500 - £1,500	£35,000 - £60,000
Regulatory fines and compensation payments	£0	£750 - £1,500
Lost assets (including lost intellectual property)	£150 - £300	£30,000 - £40,000
Damage to reputation	£1,500 - £8,000	£25,000 - £115,000
Total cost of worst incident on average	£35,000 - £65,000	£450,000 - £850,000
2012 comparative	*£15,000 - £30,000*	*£110,000 - £250,000*
2010 comparative	*£27,500 - £55,000*	*£280,000 - £690,000*

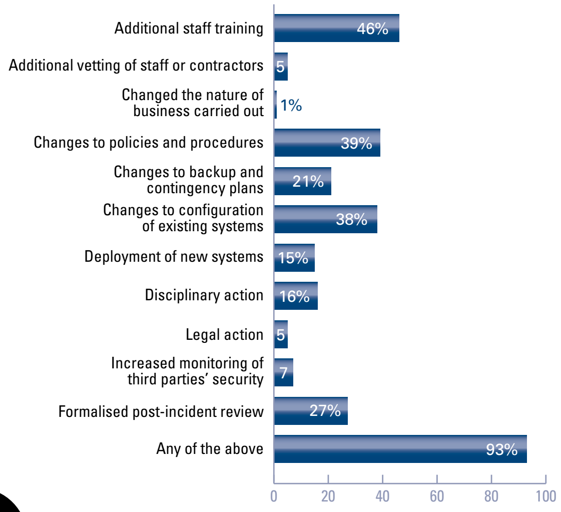
What type of security incidents do organisations plan for, and how effective are those contingency plans?

Figure 40 *(based on 99 responses)*



What steps did respondents take after their worst security breach of the year?

Figure 41 *(based on 122 responses)*



Damage to reputation

Damage to an organisation's reputation is very hard to quantify. However, using the same approach as in previous years, our best estimate of reputational damage is £1,500-£8,000 for small businesses and £25,000-£115,000 for large organisations. The proportion of companies that were able to keep knowledge of their worst incident in-house has dropped. System failures, data loss and confidentiality breaches attracted the most media coverage.

Despite a large technology company having policies in place, staff discussed confidential information where it could be overheard. This damaged the reputation of the company. After the breach, staff received additional training.

Total cost of incidents

Using the same basis as previous surveys, the cost of the worst breach of the year appears to have significantly increased, to £35,000 - £65,000 for small businesses and £450,000-£750,000 for large organisations.

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 and the response levels for some of the questions. However, based on the number of breaches and the cost of the worst breaches, we estimate that the total cost of breaches has roughly tripled from the 2012 levels, and now exceeds the previous 2010 peak. Our best estimate of the total cost to UK plc is in the order of billion pounds per annum.

Contingency planning

Overall, 68% of respondents had contingency plans in place to deal with their worst incident of the year, slightly down on last year. Large organisations are more likely to have had a contingency plan in place, but also more likely for it to have failed in practice.

A large technology company suffered a catastrophic power outage which disrupted the business for several days. The cause was insufficient testing of generator switch-over processes. It took several man-weeks of effort and tens of thousands of pounds to fix the problem. After the event, the company invested in better contingency planning.

Most contingency plans proved to be effective. However, almost half of contingency plans dealing with systems failure and data corruption did not work effectively as expected.

Following Superstorm Sandy, a mid-sized technology company primarily based in London was forced to fail over from their primary servers in the USA to their backup server in the UK. Although the failover procedure was successful, a later power outage on their secondary site led to their client-facing systems being inaccessible. It took around several man-weeks of effort over a 24 hour period to restore service.

There's a good correlation between the effectiveness of contingency plans and the seriousness of the breach. When contingency plans worked, just over half of the incidents were serious; when the plans failed, three quarters were serious.

Almost every respondent took action after their worst breach of the year. Additional staff training remains the most common step taken following breaches. This highlights how important staff behaviour is towards preventing serious security breaches. Organisations tend to change configuration and update policies and procedures after systems failures, hacking attacks and virus infections. Slightly more originations changed their backup and contingency plans compared to 2012.

After the most serious breaches, organisations tend to update their technologies, improve their processes and also train their people. The worst security breaches are triggered by multiple weaknesses in people, processes and technology within an organisation.

Independent reviewer information

We'd like to thank all the independent reviewers who ensured the survey was targeted at the most important security issues and the results were fairly interpreted.

The ABPI represents innovative research-based biopharmaceutical companies, large, medium and small, leading an exciting new era of biosciences in the UK. Our industry, a major contributor to the economy of the UK, brings life-saving and life-enhancing medicines to patients. Our members supply 90 per cent of all medicines used by the NHS, and are researching and developing over two-thirds of the current medicines pipeline, ensuring that the UK remains at the forefront of helping patients prevent and overcome diseases. The ABPI is recognised by government as the industry body negotiating on behalf of the branded pharmaceutical industry, for statutory consultation requirements including the pricing scheme for medicines in the UK. You can visit us at www.abpi.org.uk.

ICAEW's IT Faculty provides products and services to help its members make the best possible use of IT. It also 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. For more information about the IT Faculty please visit www.icaew.com/itfac.

The Institution of Engineering and Technology (IET) is a world leading professional organisation sharing and advancing knowledge to promote science, engineering and technology across the world. A professional home for life for engineers and technicians, and a trusted source of essential engineering intelligence. The IET has more than 150,000 members worldwide in 127 countries. You can visit us at www.theiet.org.

ISACA, is an international, non-profit, global association, that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA has more than 100,000 members worldwide and has been in existence since 1969. The London Chapter, was established in 1981, other UK Chapters now include Northern England, Central England, Winchester 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.

(ISC)² is the largest not-for-profit membership body of certified information security professionals worldwide, with over 89,000 members worldwide, including 14,000 in the EMEA. 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.

Founded in 1989, the **Information Security Forum (ISF)** is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members. ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own. Further information about ISF research and membership is available from www.securityforum.org.

ORIC is the leading operational risk consortium for the (re)insurance and asset management sector globally. Founded in 2005, to advance operational risk management and measurement, ORIC facilitates the anonymised and confidential exchange of operational risk data between member firms, providing a diverse, high quality pool of qualitative and quantitative information on relevant operational risk exposures. As well as providing operational risk data, ORIC provides industry benchmarks, undertakes leading edge research, sets trusted standards for operational risk and provides a forum for members to exchange ideas and best practice. ORIC has over 30 members with accelerating growth. www.abioric.com

This publication is available from www.gov.uk/bis

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/13/P184