
Department
for Business
Innovation & Skills
2014 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 Andrew Miller, Richard Horne and Chris Potter. We'd like to thank all the survey respondents for their contribution to this survey.

In association with:

infosecurity EUROPE

Infosecurity Europe, celebrating 19 years at the heart of the industry in 2014, 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 29 April – 1 May 2014, 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:

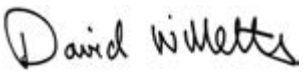
The preservation of the confidentiality, integrity and accessibility of information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can be involved.

Introduction

The UK Government recognises the importance of producing reliable information about cyber security breaches and making it publicly available. I welcome the fact that so many organisations across the UK have shared their experiences in this year's Breaches Survey, a key commitment in the Government's UK Cyber Security Strategy.

This year's survey clearly demonstrates the continuing risks associated with doing business in cyberspace, as well as the encouraging steps some businesses are taking to improve their information security. The sharp increase in the costs associated with security breaches underlines the fact that cyber security is a significant business risk that must be taken seriously. Government is focusing its efforts on working in partnership with industry, academia and international partners. The benefits of a stable and secure cyberspace are a clear driver for a shared responsibility in improving the UK's cyber security.

All our efforts in cyberspace will be supported by the information in this report.



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

Survey approach

This is the latest of the series of Information Security Breaches Surveys, carried out since the early 1990s. PwC carried out the survey, analysed the results and produced the report; Infosecurity Europe assisted with marketing the survey.

To maximise the response rate and reduce the burden on respondents, this year's survey questions were divided into two online questionnaires. We removed some past questions that are no longer so important; where relevant, we've restated past survey comparative figures to remove the responses to questions excluded from the 2014 survey, so that any trends are on a like for like basis. We added a few additional questions to reflect current concerns or key topics within cyberspace.

In total, there were 1,125 respondents. As with any survey of this nature, we would not necessarily expect every respondent to know the answers to every question. For consistency and presentational reasons we have removed the 'Don't Knows' and 'Not Applicable'. Where the proportion of 'Don't Knows' are significant, this has been referred to in the text.

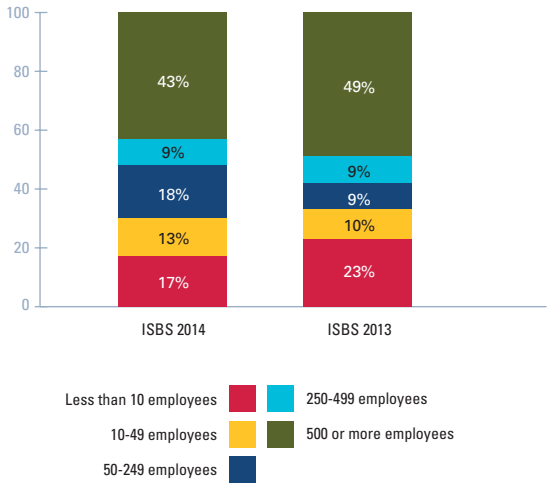
Due to the nature of the survey, the number of responses varies by question. We have included against each figure in the report the number of responses received. This provides a good guide to the margin of error from sampling error to apply when extrapolating the results. As with any self-select survey of this nature, extrapolation to the wider population should be treated with caution; wherever this report refers to "x% of companies", this should be read as short-hand for "x% of companies that responded to this survey".

As in the past, we have presented the results for large organisations (more than 250 employees) and small businesses (less than 50 employees) separately. The results for medium sized businesses (50-249 employees) are similar to the results for the small ones unless stated otherwise and we have explained in the text any differences seen. 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 2013, approximately a third of the respondents were IT professionals, and the remainder were business managers, executives, non-executive directors. This year's highest response rates were once again from organisations headquartered in London or the South-East of England; these made up roughly half of the respondents.

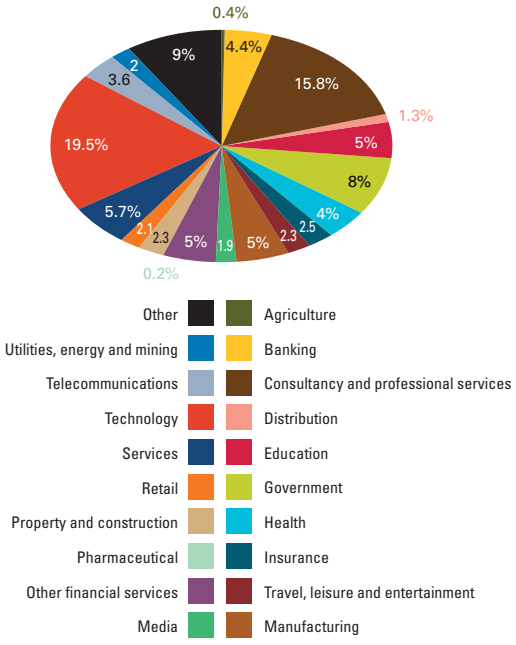
How many staff did each respondent employ in the UK?

Figure 1 *(based on 1,098 responses)*



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

Figure 2 *(based on 1,125 responses)*



Security breaches levels decreased slightly but much more costly

The number of security breaches affecting UK businesses decreased slightly in comparison to last year. However, there has been a significant rise in the cost of individual breaches. The overall cost of security breaches for all type of organisations has increased. 10% of organisations that suffered a breach in the last year were so badly damaged by the attack that they had to change the nature of their business.

Trend since 2013	Organisations participated
% of respondents that had a breach	↓
Average number of breaches in the year	↓
Cost of the worst breach of the year	↑ ↑
Overall cost of security breaches	↑ ↑

Both large and small organisations experienced decreases in security breaches compared to 2013, with almost three fifths of the respondents expecting to see more security incidents in the next year.

81%	of large organisations had a security breach (down from 86%* a year ago)
60%	of small businesses had a security breach (down from 64%* a year ago)
59%	of respondents expect there will be more security incidents in the next year than last

Affected companies experienced approximately a third fewer breaches on average than last year.

16	is the median number of breaches suffered by a large organisation in the last year (down from 21* a year ago)
6	is the median number of breaches suffered by a small organisation in the last year (down from 10* a year ago)

Cost of breaches nearly doubles in the last year

The average cost of the worst breach suffered has gone up significantly particularly for small businesses – it's nearly doubled over the last year.

£600k - £1.15m	is the average cost to a large organisation of its worst security breach of the year (up from £450 - £850k a year ago)
£65k - £115k	is the average cost to a small business of its worst security breach of the year (up from £35 - £65k a year ago)

Organisations of all sizes continue to suffer from external attacks

Attacks by outsiders continue to cause the most security breaches to all organisations. Malicious software is increasingly the means for such attacks. The focus of attacks seems to have shifted back towards large organisations.

55%	of large businesses were attacked by an unauthorised outsider in the last year (down from 66%* a year ago)
73%	of large organisations suffered from infection by viruses or malicious software in the past year (up from 59% a year ago)
38%	of large organisations were hit by denial of service attacks in the last year (similar to 39% a year ago)
24%	of large organisations detected that outsiders had successfully penetrated their network in the last year (up from 20% a year ago)
16%	of large organisations know that outsiders have stolen their intellectual property or confidential data in the last year (up from 14% a year ago)

Fewer small businesses experienced attacks than a year ago.

33%	of small businesses were attacked by an unauthorised outsider in the last year (down from 43%* a year ago)
45%	of small businesses suffered from infection from viruses or malicious software in the last year (similar to 41% a year ago)
16%	of small businesses were hit by denial of service attacks in the last year (down from 23% a year ago)
12%	of small businesses detected that outsiders had successfully penetrated their network in the last year (down from 15% a year ago)
4%	of small businesses know that outsiders have stolen their intellectual property or confidential data in the last year (down from 9% a year ago)

Staff-related breaches have dropped significantly compared to a year ago. However, staff still play a key role in security breaches.

58%	of large organisations suffered staff-related security breaches (down from 73% a year ago)
22%	of small businesses suffered staff-related security breaches (down from 41% a year ago)
31%	of the worst security breaches in the year were caused by inadvertent human error (and a further 20% by deliberate misuse of systems by staff)

* Where relevant, we've restated past survey comparative figures to remove the responses to questions excluded from the 2014 survey, so that any trends are on a like for like basis.

"The Ten Steps" guidance continues to be relied on

Respondents continue to use "the Ten Steps" guidance issued by the UK Government on cyber security threats and protection. This guidance is now recognised as one of the most popular resources for businesses.

26%	of respondents use "the Ten Steps" guidance

Understanding, communication and awareness lead to effective security

The vast majority of organisations continue to prioritise security. The number of worst breaches caused by senior management giving security insufficient priority has reduced highlighting an increased awareness of the importance of security at executive level.

79%	of respondents report that their senior management place a high or very high priority on security (similar to 81% a year ago)
7%	of the worst security breaches were partly caused by senior management giving insufficient priority to security (down from 12% a year ago)

Security budgets reflect this high priority. There has been a marked increase in spending on Information Security in small businesses.

10%	of IT budget is spent on average on security (same as a year ago)
15%	of small businesses spend more than 25% of their overall IT budget on security (versus 10% of large organisations)

Many businesses are becoming more aware of the importance of education on security. More organisations are explaining their security risks to their staff to ensure they take the right actions to protect the information. However, this is by no means universal.

68%	of large organisations provide ongoing security awareness training to their staff (up from 58% last year)
54%	of small businesses provide ongoing security awareness training to their staff (up from 48% last year)
23%	of respondents haven't briefed their board on security risks in the last year (and 13% have never done so)
27%	of large organisations say responsibilities for ensuring data is protected aren't very clear versus 24% who say they are very clear
70%	of companies where security policy was poorly understood had staff-related breaches versus 41% where the policy was well understood

There have been improvements in risk assessment and security skills, but many organisations still struggle to evaluate the effectiveness of their security activities.

20%	of respondents haven't carried out any form of security risk assessment (down from 23% in 2013)
59%	of respondents are confident that they'll have sufficient security skills to manage their risks in the next year (up from 53% in 2013)
33%	of respondents don't evaluate how effective security expenditure is (similar to 31% in 2013)

Businesses need to manage the risks associated with new technology

The use of technology remains a key part of businesses' daily working so it is vital to ensure a flexible approach to security.

12%	of large organisations had a security or data breach in the last year relating to social networking sites (similar to 14% a year ago)
7%	of large organisations had a security or data breach in the last year involving smartphones or tablets (similar to 9% a year ago)
5%	of respondents had a security or data breach in the last year relating to one of their cloud computing services (similar to 4% a year ago)
10%	of the worst security breaches were due to portable media bypassing defences (up from 4% a year ago)

Organisations are seeking new ways to gain assurance over security

As organisations improve their understanding of the security threats they face, they are doing more to manage the associated risks and seeking new ways to gain assurance over security.

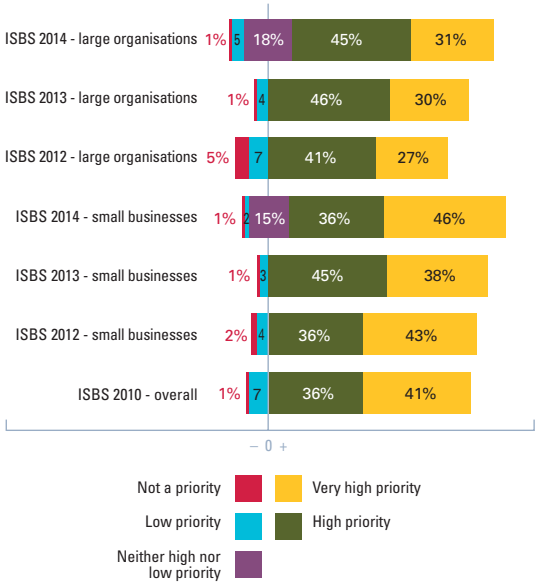
52%	of large organisations have insurance that would cover them in the event of a breach
35%	of small organisations have insurance that would cover them in the event of a breach
69%	of respondents currently invest in or plan to invest in threat intelligence

Key observations of the year

1. While the number of Security Breaches has decreased, the scale and cost has nearly doubled. Nearly 10% of respondents changed the nature of their business as a result of their worst breach.
2. The overall investment in security as part of total IT budget is increasing across all sectors with even the most frugal sector's investment increasing.
3. There has been a marked increase in spending on Information Security in small businesses.
4. Organisations are making risk-based decisions about the introduction of mobile devices in order to facilitate more flexible ways of working.
5. Confidence about the availability of security resources has increased.
6. 70% of organisations keep their worst security incident under wraps. So what's in the news is just the tip of the iceberg.

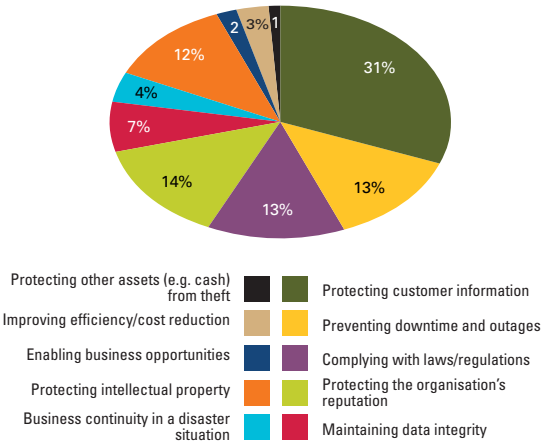
How high a priority is information security to top management or director groups?

Figure 3 *(based on 803 responses)*



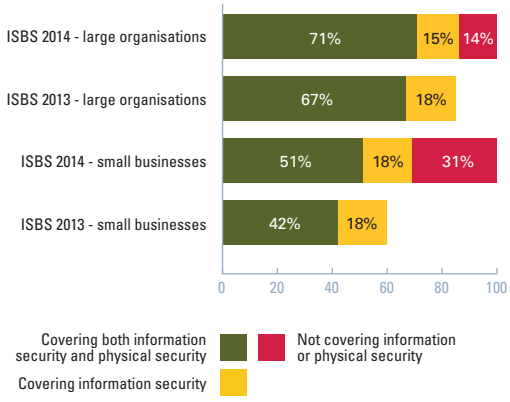
What is the main driver for information security expenditure?

Figure 4 *(based on 572 responses)*



How many respondents carry out security risk assessments?

Figure 5 *(based on 396 responses)*



Attitudes to cyber security

Organisations continue to prioritise cyber security this year. 76% of large organisations and 82% of small businesses believe security is a high or very high priority to their organisations and senior management.

An encouraging 92% of respondents have briefed their senior management on cyber risks. The frequency of briefing varied - 32% brief monthly, 23% brief at least quarterly while 35% rely on annual or less frequent briefings.

Security once again appears to be a higher priority for small businesses than large organisations, continuing the trend seen since 2010. Security priority among large organisations remains consistent with the previous year. Some respondents in large organisations still have concerns about the lack of visible direction from the board and insufficient budget allocated to investment in more effective security measures. The majority of respondents however acknowledged the importance of security priority and the associated beneficial impact to their companies.

The top four drivers for security expenditure remain the same as in 2013. Protecting customer information continues to be the most commonly considered driver by a large margin. Compliance with laws and regulations has become more significant, while protecting reputation remains important among all industries. Although preventing downtime remains one of the top four common drives, its importance has decreased by 7% from 2013. Protecting intellectual property is especially important in the technology, consultancy and professional services sectors.

The number of both large and small businesses that formally assess security risks has increased by 4% and 9% respectively. This is a positive sign more organisations have recognised the need to understand their security status especially given today's rapidly evolving technology and cyber threat environment.

A strong correlation between security priority and risk assessment remains. Consistent with the 2013's findings, almost three quarters of companies where security is a high priority assesses security risks but only half assess where security is rated as low priority. 82% of respondents include cyber risks in their overall risk register. 85% of those that do are companies that consider security as high priority.

Management at a large publisher failed to make security enough of a priority. This led to the electronic theft of their product that was subsequently made freely available to everyone. As well as the loss of the product revenue, the cost of updating the systems and policies was more than £50,000.

Employees of a large property and construction firm deliberately misused its systems, leading to a breach of the Data Protection Act. The company admitted that they did not sufficiently priority security or understand the risks associated with systems, regulations and processes.

Security priority continues to vary across different industries. Technology companies continue to give the highest priority on average with consultancy and professional services firms at the second place. As in the 2013 results, the financial services and government sectors continue to give information security a relatively high priority. A visible improvement can be seen in security priority made among media, distribution, retail, leisure and entertainment companies, whilst travel and pharmaceutical sectors both continue to give lower priority to security than average.

The changing trends

Companies have once again increased the use of remotely hosted services (often referred to as cloud computing) as an affordable and easily accessible alternative to internal IT services. This year's results show that five sixths of respondents are now currently using cloud computing services.

Externally hosted websites and email are the most popular services amongst small businesses; 82% of their websites and about 70% of their email solutions are externally hosted this year. In contrast, only 13% of large organisations use an externally hosted email service. Large organisations are more likely than others to extend this further using externally hosted payment, payroll processing, and data storage solutions. Large organisations have moved towards the external hosting of websites in the past year.

Use of cloud services for data storage is the biggest growth area with a 7% increase from 2013. There's also been a significant shift in who is storing data on the cloud. More small businesses (around two fifths) are using cloud computing solutions for data storage, while the adoption rate among large organisations remained the same as last year at roughly 15%.

Staff from an educational body had their personal data exposed after a third party supplier inappropriately stored it on the Internet. A process to review Cloud services was put in place to minimise the risks of this happening again and staff also received more training on the usage of mobile devices, threats and software.

52% of organisations with externally hosted services believe these are critical to their business with a small drop from 53% in 2013; 10% report that they aren't important, up 4% from 2012. One fifth of organisations of national importance (i.e. financial services, telecommunications and utilities) critically depend on externally hosted services, down three tenths from a year ago. Large organisations are slightly more likely to have critical externally hosted services than small businesses. Increasing numbers of companies are storing confidential data on the Internet. 77% of large organisations and around three quarters of small ones have confidential or highly confidential data on the cloud.

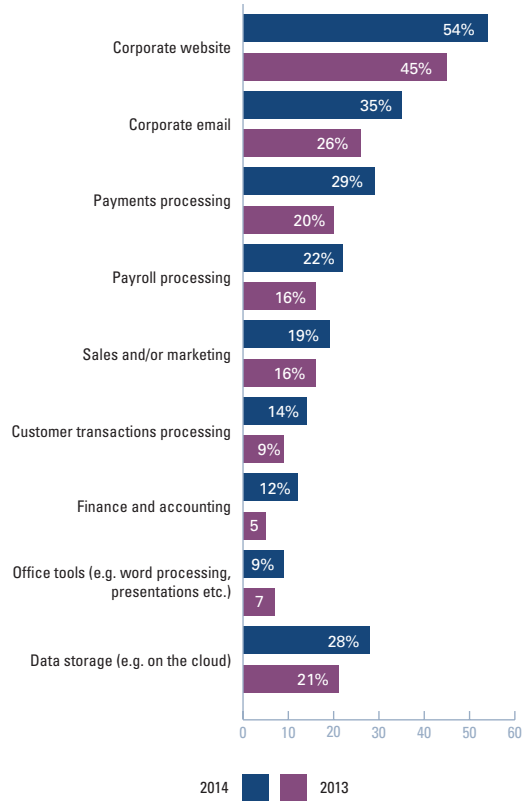
Social networking has become more important to large organisations over the last year. Roughly 60% of large organisations now believe social networks are important to their business versus 47% in 2013. Most are keen to keep this to corporate communications use with half of respondents blocking or monitoring staff activity on those sites. Only 42% of small businesses consider social network important, down slightly by 5% from 2013.

Mobile device use continues to be an un-stoppable trend. While there are business benefits from the use of social networks and mobile devices, companies also need to protect themselves against cyber risks by implementing adequate controls through the use of mobile devices and social networks.

Facing today's fast changing environment, large organisations seem to struggle to clearly define responsibilities for owning critical data and for protecting it. 20% said the responsibilities aren't clear and, none believe the responsibilities were very clear. The potential causes could be the complex organisational structure and operational models within large organisations. Smaller businesses are in a much better position in comparison – 73% are very clear, versus 6% that aren't clear.

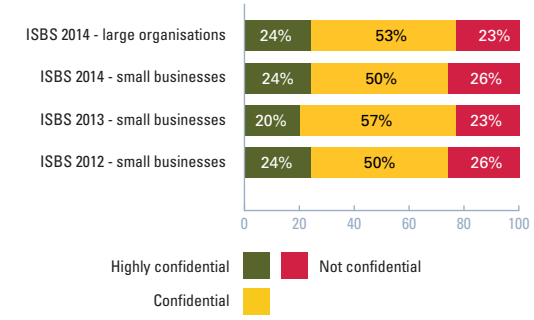
Which business processes have respondents outsourced to external providers over the Internet?

Figure 6 *(based on 465 responses)*



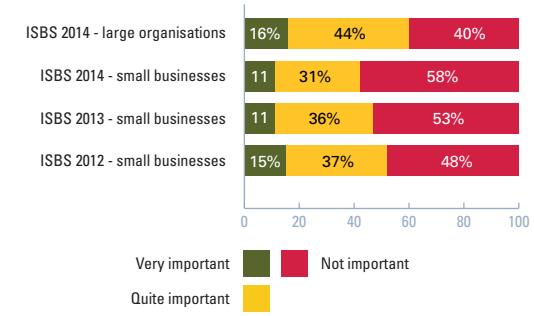
How confidential is the data that respondents store on the Internet?

Figure 7 *(based on 289 responses)*



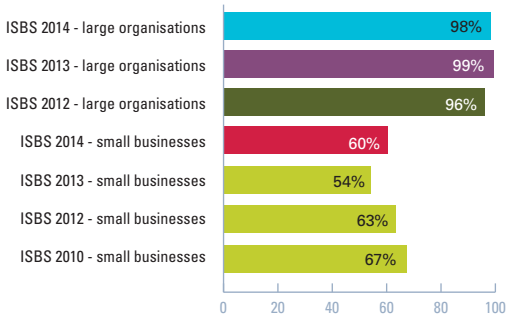
How important is the use of social networking sites to the organisation?

Figure 8 *(based on 337 responses)*



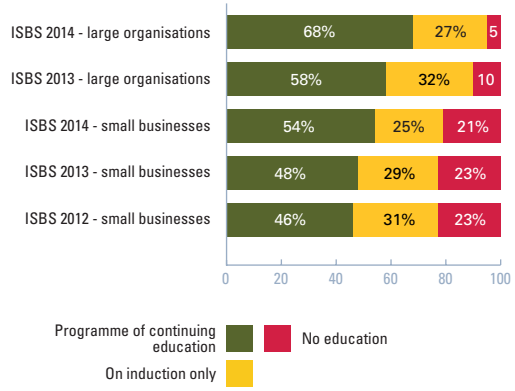
How many respondents have a formally documented information security policy?

Figure 9 *(based on 404 responses)*



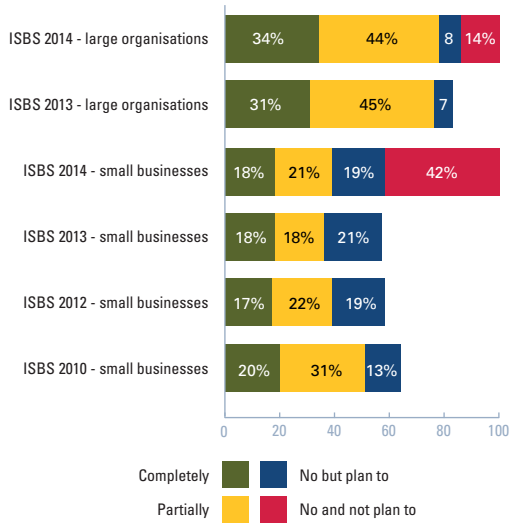
How do respondents ensure staff are aware of security threats?

Figure 10 *(based on 413 responses)*



How many respondents implemented ISO 27001?

Figure 11 *(based on 366 responses)*



Culture and behaviours

As we saw in 2013, almost every large organisation now has a documented security policy. More encouragingly, adoption levels in small businesses have increased from 54% in 2013 to 60% this year, reversing the decline seen since 2010. This indicates an acknowledgement of the importance of written security policies in the wider community.

Although there are more written policies in place to guide employees' behaviours towards security, we haven't yet seen this translate into better understanding of these policies. Only a quarter of respondents with a security policy believe their staff have a very good understanding of it versus a fifth that believe the level of understanding is poor.

There has been an encouraging rise in the proportion of businesses that have a programme of continuing security education for their staff, which is now at the highest level ever. 68% of large organisations and 54% small businesses provide ongoing security training to their staff, up by 10% and 6% respectively. Organisations increasingly recognise that staff are a great asset but also a huge potential threat. Organisations also often provide more training to staff as one of the most commonly seen remediation actions after a serious breach or incident. This year's results show that large organisations suffer more from staff-related breaches whereas small businesses were affected more by outsider attacks.

A small financial services firm lost a half-day of work after one of their staff downloaded a file containing malware from his personal webmail. This encrypted several files shared between staff. It took a week to fully resolve the incident. As a result, the company made changes to their email usage policy and reconfigured the structure of their system to prevent this happening again.

"The Ten Steps" guidance issued by the government to businesses on how to protect themselves from cyber security threats continues to be relied on with 26% of respondents using it this year. This guidance is increasingly recognised as one of the most popular resources for businesses especially for large organisations - 70% of respondents that use the guidance to evaluate their security threats are large organisations. In contrast, the implementation of ISO27001 is still not on everyone's radar and remains an elusive goal. Business adoption of ISO 27001 by large organisations has increased only slightly - around a third have fully implemented it versus 14% who haven't and don't plan to. Small businesses seem less open to the idea - only 18% have implemented ISO27001 versus 42% that haven't and don't plan to.

Discussions with senior management and views of internal security experts remain the most popular other sources for evaluating cyber threats. Interestingly, both small and medium sized businesses rely mostly on news and media stories, whereas large organisations rely on external security consultants and alerts from government/intelligence services.

Inappropriate staff behaviours at a large technology firm led to the theft and unauthorised disclosure of information. The incident resulted in the near total compromise of personal information and also the controls in place for protecting such information. After the breach, the company overhauled its policies and security procedures.

When things do go wrong, 92% of large organisations have a formal incident response process in place, and furthermore 56% of them also have a specified response team in place. Small businesses are still less well prepared with 51% having incident response plans in place. This is consistent with what we saw in 2013.

Investing in security

It is increasingly difficult for organisations to protect their key information assets and infrastructure in the face of constantly changing technology. Information security is wider than just IT. However, given the close relationship to IT, security spending often forms part of the overall IT budget. Therefore this survey has historically used the percentage of IT budget spent as a guide to the level of investment in security.

Large organisations now spend on average 11% of their IT budget on security; small businesses spend even more of their IT budget on security than large ones with an average of almost 15% of their IT budget. This is the highest level ever recorded in this survey. 15% of small businesses spend more than 25% of their overall IT budget on security, versus 10% of large organisations. These figures highlight the increasing recognition by businesses of all sizes of the importance of protection and defence against cyber security threats.

86% of the large organisations and 94% of small businesses are expecting to spend at least the same on security next year. 51% of large organisations are expecting their security expenditure to increase.

We continue to see that organisations that suffered a breach during the year spent on average less of their IT budget on security than those that didn't. Corrective actions after the breach still form the biggest part of their spending. This suggests that organisations who have invested more in security defences have fewer breaches. Given the rising cost of those breaches, under-investment in security seems a false economy.

An unexpected server network failure caused a 48 hour outage for a healthcare facility in the South-West of England. This failure was caused by the lack of resources available to rebuild or replace the network with a more robust system. It took the company a week to restore business operations back to normal after the incident. Following the incident, they changed their contingency plan, updated their existing system configurations and deployed a new system as a result of the incident.

The gap between the highest and lowest spenders has narrowed. Roughly one in seven organisations now spends less than 1% of IT budget on security; this is down from one in six in 2013. The picture continues to vary by region. Two fifths of London based companies are expecting to spend more on information security next year. In contrast, only one in seven of the companies in Wales and one in six of the companies in Yorkshire and the Humber are expecting so.

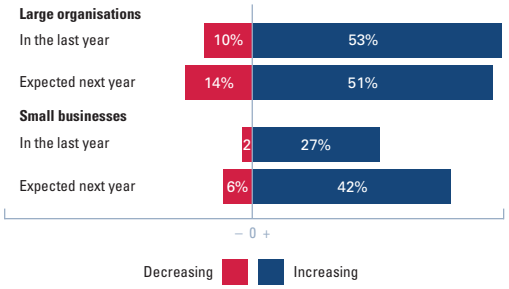
A Welsh consultancy and professional services firm suffered a major service outage while recovering from a ransomware attack and a number of phishing attempts. This was caused by a failure to devote resources to maintain updated security software.

Services and telecommunication providers spend the most on security followed by other big spending sectors including technology, health and government bodies. All sectors are now convergent on a narrower band with 6-14% of IT budget spent on security. Even the most frugal sector, retail and distribution, spends 6% of their IT budget on security - a big increase from 3.8% a year ago.

Respondents are more confident of being able to source sufficient security skills to enable them to manage their security risks. 17% of respondents are very confident that they will be able to source sufficient security skills to enable them to manage their security risks, up by 4%from 2013. 17% of respondents aren't confident, down 3% from 2013. Large organisations still seem to have a skills shortage - 12% are very confident versus 21% that aren't confident.

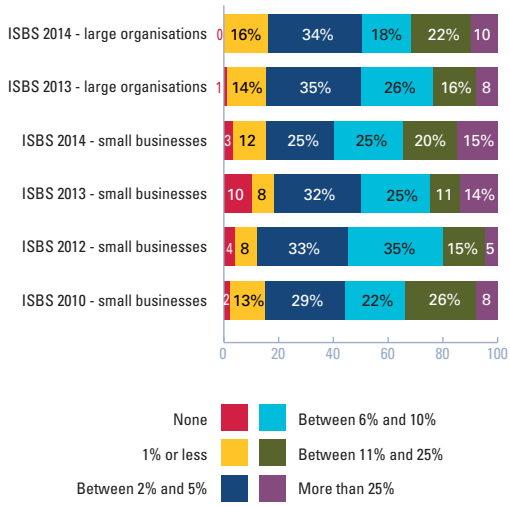
How is information security expenditure changing?

Figure 12 *(based on 682 responses)*



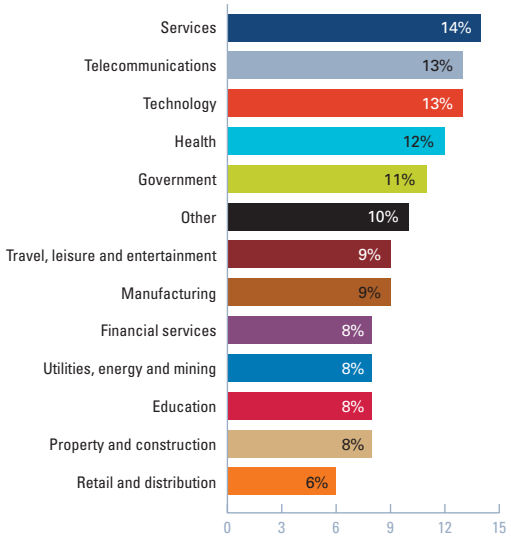
What percentage of IT budget was spent on information security, if any?

Figure 13 *(based on 589 responses)*



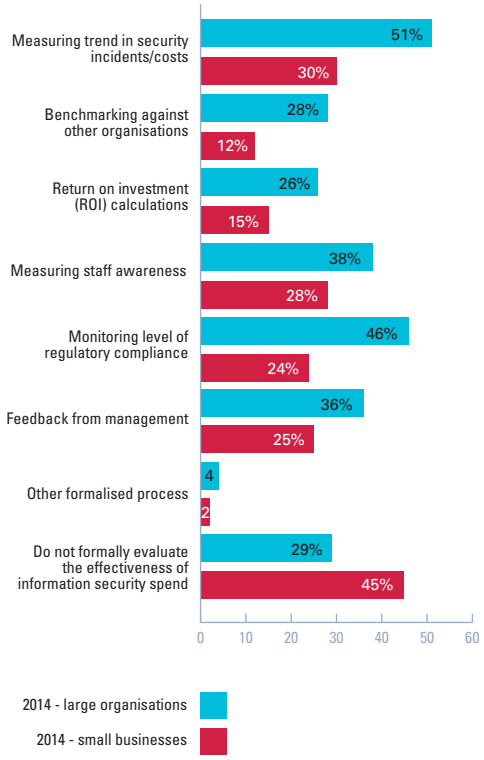
Which sectors spend most on security?

Figure 14 *(based on 449 responses)*



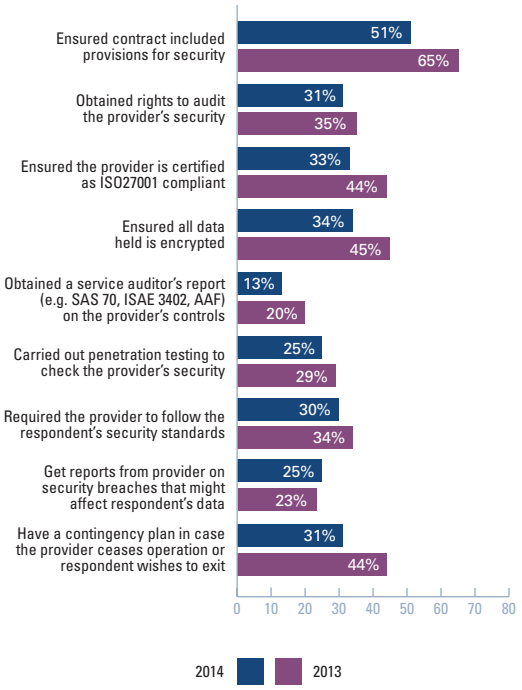
How do respondents measure the effectiveness of their security expenditure?

Figure 15 *(based on 367 responses)*



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

Figure 16 *(based on 467 responses)*



Evaluating spend effectiveness

Given that cost control remains a high priority for most organisations, one might expect that organisations would seek to evaluate the effectiveness of their security spend. However, there hasn't been any real shift over the last year; 45% of small businesses don't do anything to evaluate the effectiveness of what they spend on security – given they are spending at record levels this is a concern. It seems that evaluation of security spend is an area that sees little focus and clarity.

Among those that try to measure the effectiveness of security, trend analysis of the number or cost of security incidents remains the most commonly used measure; this is consistent with the trend seen since 2012. Unsurprisingly, given the increasing legal and regulatory focus on cyber security, monitoring the level of regulatory compliance has risen significantly in popularity.

There's been a small increase in the use of return on investment to evaluate security expenditure; a quarter of large organisations now do this. The results are dependent on the roles of the respondents and whether they have a comprehensive insight of how security expenditure is evaluated within their organisations.

The assurance challenge

Five out six respondents now use outsourced services yet there has not been a similar increase in the number of organisations that seek assurance about the security of externally hosted services. Cyber security assurance remains a challenging area which lacks investment and focus.

A mid-sized manufacturing company based in the South West uses externally hosted solutions including payroll processing and storing highly confidential data, but hasn't checked their external provider's security. They admit that they aren't at all confident that they would be able to detect the latest generation of attacks especially to their externally hosted services.

Large organisations continue to show much more diligence at gaining assurance over third parties' security status. They are almost five times as likely as small businesses to obtain audit rights, more than three times as likely to obtain a service audit report (such as ISAE 3402 or AAF 01/06) on provider's controls, three times as likely to require the provider to follow their own security standards and twice as likely to carry out penetration testing.

A large technology company based in London uses an externally hosted solution for many of its applications including data storage and HR. The data processed by these applications is considered highly confidential and the external services are as critical to the business. Although several precautions were taken to ensure the diligence of the external provider, the company had a data breach related to a cloud service in the past year. They now plan to invest in threat intelligence in the next 12 months to gain more assurance over the security status of the company and its confidential data.

In some areas, there is little difference between large and small businesses. Just under half of each ensure all data held by third party is encrypted and around two fifths of each have contingency plans in place in case the provider ceases business. In contrast with last year's results, large organisations are now slightly more likely to seek ISO27001 compliance from their providers.

69% of large organisations have platforms to monitor incident levels and 52% of them have insurance to cover them in the event of a breach. This could indicate an emerging culture for cyber security insurance.

Social networks and mobile computing

Social networking has become more important in the past year for large organisations. However, organisations of all sizes struggle to understand the best way to control the risks associated with social networking sites.

Instead of simply blocking access to social network websites, large organisations tend to restrict use to corporate communications only; over half of respondents restrict or monitor staff activity on social networking sites. The proportion of respondents using different techniques is very similar to last year. As in the past, large organisations tend to have better controls than small ones.

16% of large organisations detected a security breach involving social networking sites in the last year. The situation appears better for small businesses - only 5% detected a security breach related to social networking sites. This could be influenced by the results mentioned earlier that fewer small businesses consider social network important this year and that they often have less detection capability than large organisations.

A small London-based IT company didn't restrict the use of social network sites. Unfortunately, they had multiple breaches relating to misuse of social networking sites by staff last year and these incidents weren't detected in a timely manner due to the lack of focus on social network usage.

Removable media devices have rapidly become a key area of exposure. Over 10% of the worst security breaches of the year being caused at least partly by portable media bypassing security defences – this is more than double the level we saw in 2013. More and more organisations are focusing on developing security policy and controls around the use of mobile phones and tablets but these measures do not always consider the usage of removable devices such as USB sticks, removable hard drives, CD or DVDs.

Mobile devices are now an unstoppable trend with almost all organisations making risk based decisions on how to facilitate their introduction into the organisation. Just over half of large organisations and three quarters of small organisations have adopted a Bring Your Own Device (BYOD) culture. Most organisations are using a range of techniques to protect themselves from mobile threats, using both policies and technical defences. This is a positive sign - businesses have become increasingly aware of the importance of protecting themselves against cyber risks through mobile devices.

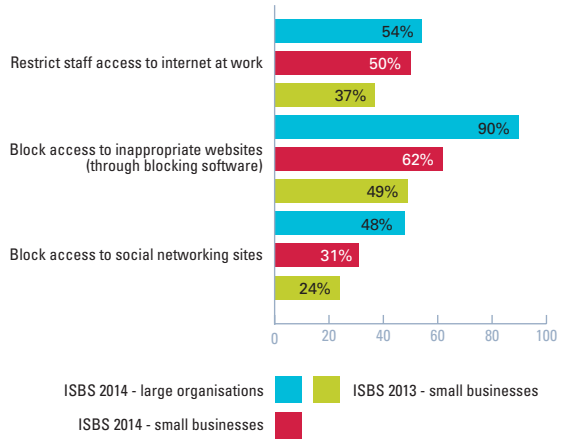
A large government body had a security breach related to inappropriate use of mobile devices last year. As a result of this incident, they have now issued a policy on mobile computing and only allow access via corporate devices.

A small company in the education sector suffered from a serious security breach related to a cloud service and the use of smart phones/ tablets. The data access and sharing facility weren't properly secured leading to loss of some confidential customer data. Following the breach, the company defined and implemented a mobile device policy and is now planning to invest more in threat intelligence.

The risks associated with mobile devices increase as the use of mobile devices increases. 9% of large organisations had a data or security breach involving smartphones or tablets, the same level as a year ago, although it is not clear whether all breaches are being detected currently. Only 38% respondents encrypt the data held on mobile phones and only 42% of respondents train their staff on the threats associated with mobile devices. An alarming 16% of respondents don't take any steps to address the risks associated with mobile devices. This is concerning given the increasing prevalence of the use of mobile devices in daily business operations among all organisations.

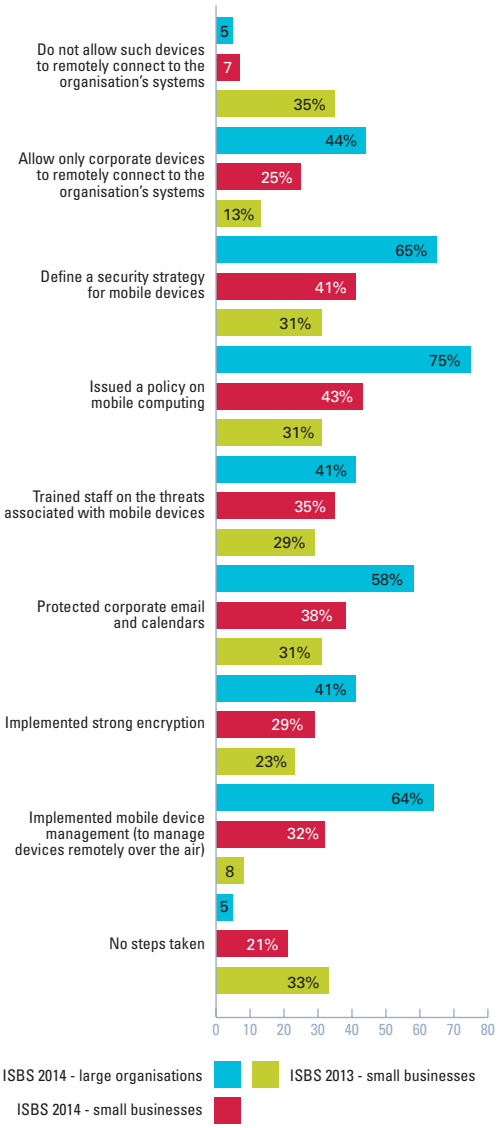
How do respondents prevent staff misuse of the web and social networking sites?

Figure 17 *(based on 693 responses)*



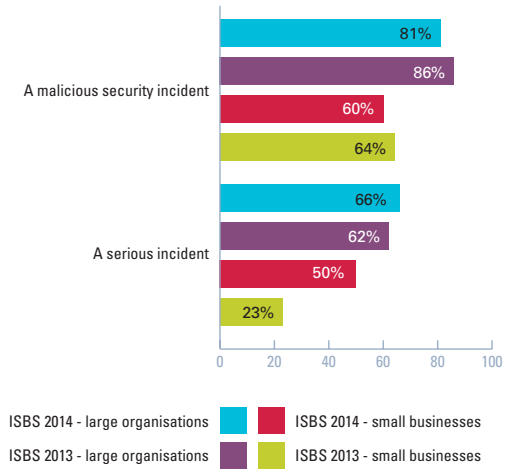
What steps have respondents taken to mitigate the risks associated with staff using smartphones or tablets?

Figure 18 *(based on 352 responses)*



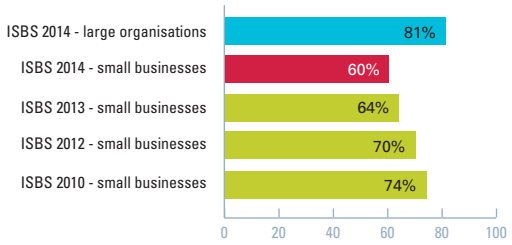
In the last year, how many respondents had...

Figure 19 *(based on 530 responses)*



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

Figure 20 *(based on 449 responses)*



What do respondents expect in the future regarding number of incidents?

Figure 21 *(based on 323 responses)*

Incidence of security breaches

There's been a small reduction in the proportion of companies having security breaches, down from the record high level seen a year ago. However, organisations of all sizes continue to be badly affected. 81% of large businesses had malicious breaches, and two thirds of them had a serious incident. 60% of small businesses also suffered from malicious breaches and half of them had a serious incident.

Consistent with the past, large organisations reported more breaches than small ones. The size and complexity of the organisation and the number of staff both increase the likelihood of breaches occurring. Large organisations more likely to detect sophisticated breaches than the small ones as they often have effective technical measures in place for monitoring and detecting suspicious activities. Small businesses are less likely to have staff related breaches as they have fewer people to manage than large organisations.

All sectors and regions suffered from malicious security breaches. At least 70% of respondents in every sector reported malicious breaches, as did at least 80% of respondents from every region.

The pattern of how organisations detected their most significant breach of the year remains similar to last year. Routine internal security monitoring is still the most commonly used method; this detected 29% of the worst breaches. 21% were noticed due to their business impact (e.g. systems outage, assets lost etc.). 10% of organisations' worst security incidents were discovered by accident. It's concerning that this figure has risen from only 6% in 2013. Although 29% of organisations detected the breach in less than a day, many breaches took longer to detect - 6% (up by 1% from 2013) of respondents took a few weeks and 14% (up by 5% from 2013) took more than a month to detect their worst breach of the year.

A Trojan attack allowed remote access to the accounts of a mid-sized media firm. It bypassed several layers of security before it was detected and caused business disruption and loss of data. The recovery took around 10 days. The firm consequently introduced additional staff training, changed its contingency plans and updated the existing system configurations to prevent reoccurrence of this type of incident in the future.

Future Outlook

While most of the respondents from small businesses do not expect to see fewer incidents next year, only 40% of them (down from 46% last year) expect to see an increase. This suggests an increasing confidence in their ability to defend themselves. Large organisations also share the more optimistic view. 51% of large organisations expect the number of breaches to increase next year, down from 63% in 2013. The number of large organisations expecting fewer incidents also followed the trend with 14% this year (5% up from 2013). This correlates to higher spending on security across all types and sizes of businesses.

About two fifths 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. This number is higher than last year and correlates to the increased confidence in sourcing sufficient security skills to manage security risks. About one fifth of respondents are not confident, and this is particularly the case in large organisations and the financial services sectors. The consultancy and professional services, health and utilities, energy and mining sectors also flagged concerns about their inability to detect the latest attacks this year.

With this view of the future, it is vital to have the skills necessary to prevent, detect and manage breaches. More than three fifths of the respondents are very or quite confident that they have the skills they require. In contrast, one in six aren't confident. This is particularly an issue for large organisations who should consider how to address their skills shortage.

Types of security incident

The number of outsider attacks suffered by large and small organisations both decreased substantially this year by over 10%. 55% of large organisations reported being attacked (down from 66% a year ago) versus 33% of small businesses (down from 43% a year ago). Large organisations still suffer from a serious outsider attack every few days and slightly more attacks on average comparing to a year ago; small businesses on average have a serious attack once every few weeks, though the average number of attacks suffered stayed the same as a year ago.

A government body's website was under persistent attack after a previously unknown exploit was discovered by the attacker. It took the organisation a few months to resolve the issue completely. Consequently, this incident also had a significant impact on the limited resources of the organisation.

It is reassuring to see a big decrease in staff-related incidents at small businesses, both in terms of number of companies affected and the average number of breaches suffered in each category. The results correlate with the increasing amount of effort that organisations are investing in security training and awareness this year. 58% of large organisations suffered staff-related breaches versus 22% for small businesses.

Computer fraud and theft levels dropped slightly from those noted in last year's survey and on average, affected businesses suffered fewer instances of this type of breach.

There has been a noticeable increase in the number of respondents that have been infected by viruses or malicious software. 45% of small business respondents experienced infection, a 4% rise, with a worrying 73% of larger companies reporting infection – constituting a 14% increase in the past 12 months. The average number of infection incidents reported by those affected in small businesses remained at the same level, but the average number in large organisations has risen from a year ago. It is strongly advisable to use automated detection technology, rather than relying solely on traditional anti-virus software, which is not always effective.

A small technology company in the UK suffered from a banner message malware infection on their website. They deployed an encryption solution and improved other technical security measures on the website as a result of this incident.

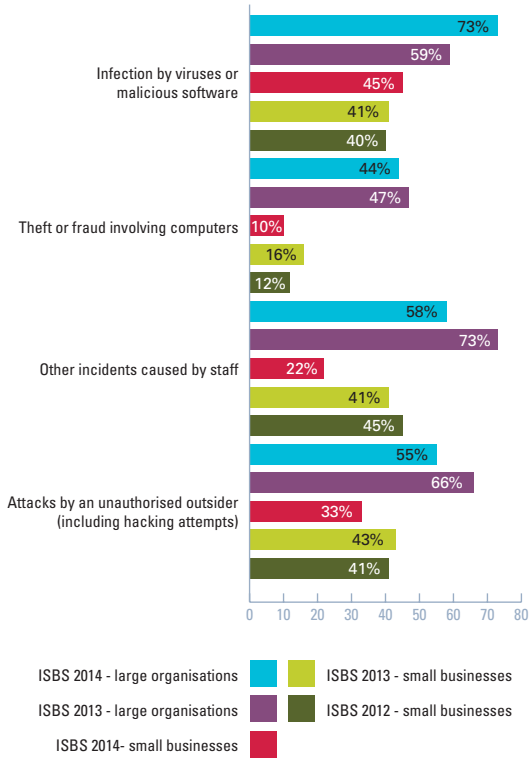
A large London based technology firm were attacked by a large array of botnet programs. It required a large amount of work and changes to their systems to recover from the incident, resulting in significant costs to the business.

With the exception of the increase in the number of respondents that have been infected by viruses or malicious software, a reduction is seen in other incidents this year. The average number of breaches suffered in the year has reduced by roughly 24% for large organisations and 40% for 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. The way of calculating the medians this year has been altered as a number of questions relating to hacking attempts and system failure or data corruption were not included in this year's survey. We also adjusted last year's figures to ensure like comparatives have been used.

A small telecommunications company encountered a four-day service and system disruption when a PHP zero day vulnerability in their web server exploited. This incident resulted in a number of man hours to recover and changes to their backup and contingency procedures.

What type of breaches did respondents suffer?

Figure 22 *(based on 829 responses)*



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

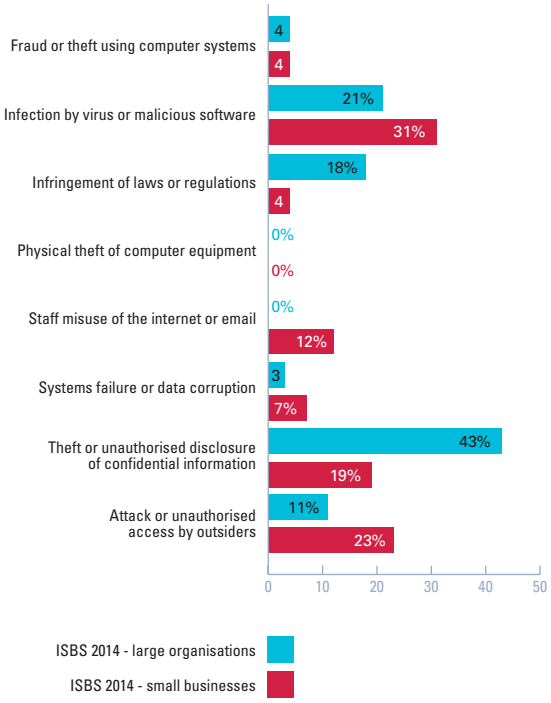
Figure 23 *(based on 449 responses)*

	Large organisations	Small businesses
Infection by viruses or other malicious software	5 (3)	3 (3)
Theft or fraud involving computers	3 (5)	1 (2)
Other incidents caused by staff	6 (10)	3 (6)
Attacks by an unauthorised outsider (excluding hacking attempts)	11 (10)	5 (5)
Any security incidents	16 (21)	6 (10)

Equivalent comparative statistics from ISBS 2013 are shown in brackets

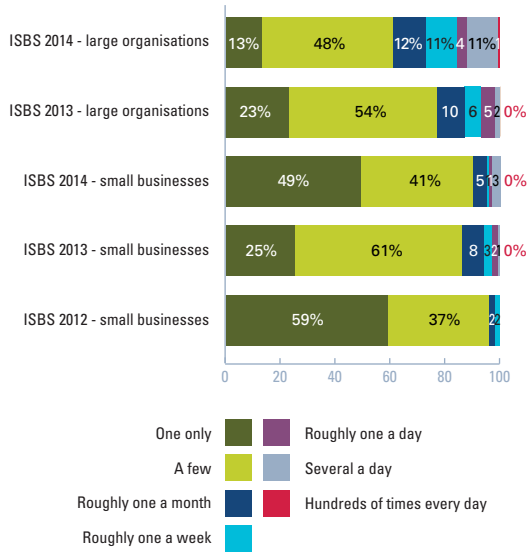
What was the worst security incident faced by respondents?

Figure 24 *(based on 54 responses)*



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

Figure 25 *(based on 228 responses)*



Infection by viruses and malicious software

There's been a significant increase in the virus infection rate this year. Infection by virus and malicious software remains one of the most commonly seen security incidents faced by respondents and it's continuingly proven to be particularly harmful to small businesses with 31% of the worst breaches experienced by small businesses last year being virus infection related.

A small technology firm, focused on online security, had their systems infected by a virus via emails masquerading as false certificates. This virus wasn't detected by a number of commercial anti-virus applications and caused minor business disruption and damaged the reputation of the firm.

As mentioned previously, mobile computing is one the fastest evolving areas in business. Virus and malicious software infection on mobile devices has reached new heights in terms of both quality and quantity as a result of its popularity. An industry trend continuing from last year is the rapid movement of virus infection mechanisms from PC to mobile devices.

The increasing popularity of the use of online banking is a key motivation for mobile malware. If a smartphone is infected, the devices are often checked by cybercriminals to see whether a bank card is associated with it. Industry experts have predicted that new types of attacks targeting mobile devices will evolve, including the possibility of the first real mobile device ransomware attack. Other forecasts indicate the possibility of enterprise infrastructure being attacked through the wide usage of "Bring Your Own Device" coupled with weak mobile security technologies and policies.

In the past 12 months, the majority of detected attempts to exploit vulnerabilities on PCs and servers targeted 'Oracle Java' followed by the 'Windows components' category, including vulnerable Windows OS files that don't apply to Internet Explorer and Microsoft Office. Once again, the importance of applying appropriate patches to hardware and software levels in addition to the operating systems in a timely manner is highlighted. Continuing the worrying trend we saw in 2013, many organisations still don't take patching seriously leaving themselves vulnerable to attack.

A medium sized distribution company based in the South East suffered a serious virus infection. The incident was only identified due to its serious negative effect on business operations. It took a day for the business to restore its normal operations and the company spent £10k resolving the incident. Following the incident, the company implemented additional staff training, invested in a more effective contingency plan and also made changes to their existing system configurations.

A small office supply and distribution company had a serious virus infection that disabled their firewall, restricted their access to key data and randomly modified their files and directories. It took them almost a day to restore business operation and a further 10 days to fully recover the incident.

There have been a few interesting developments in the last year in the area of the web-based malware: most malicious URL detections were for websites containing exploits or redirecting to exploits. A number of concerns were raised in the survey this year over the robustness and reliability of the current mainstream anti-virus software with several organisations experiencing virus and malware breach despite having anti-virus software installed.

An IT specialist discovered that their systems had been infected with malware after noticing strange ICMP packets originating from the network. It took almost a week to remove the malware from the system completely. They have raised concern over current mainstream anti-virus software's inadequate ability to identify or remove certain types of malware.

Deliberate sabotage by staff of systems or data

Deliberate sabotage by staff of systems or data remains relatively rare, consistent with last year's results. 5% of respondents were affected in comparison to 6% in 2013. However, the 4% increase in the total number of such breaches identified raised an alarming point, indicating that deliberate sabotage by staff, when occurring, is moving towards becoming a repeated offence. 7% of the affected respondents suffered several times a day in the past year.

A deliberate fraud and bypassing security controls on corporate systems due to a known system security weakness resulted in the misuse of customer information by staff at a large telecommunications firm. This breach took months to rectify and additional staff training was provided directly as a result. In addition, the deployment of new systems was implemented and disciplinary action was taken.

The worst security breach question from this year's survey provided us a clear picture that while technology faults exist in majority of the incidents, human error, either deliberate or accidental, is also a big contributing factor.

Computer theft and fraud

Computer theft and fraud suffered by respondents was reported as the worst security breach, with results aligned to prior years' results. There was a big jump in the proportion of the worst breaches attributed to theft or unauthorised disclosure of confidential information, especially in large organisations.

Small businesses seemed have suffered less in this category: the number of small businesses that reported theft of confidential data or intellectual property by staff or outsiders both dropped to least half of the numbers seen in 2013. In contrast, large organisations suffered about the same level of staff related data loss but a slightly higher level of respondents reported theft of confidential data or intellectual property by outsiders.

An employee of a social care facility based in the South East of England repeatedly gained unauthorised access to confidential information about individuals he knew in order to facilitate fraudulent activities. As a result, the police were informed and disciplinary steps were taken against the employee. Stricter staff training and vetting process were also implemented as a result.

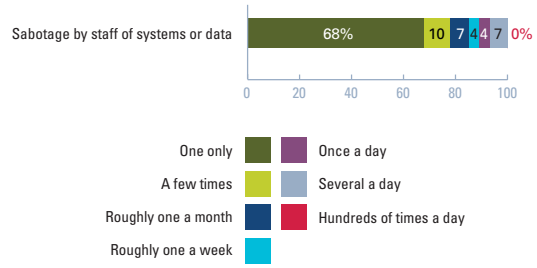
Confidential information was stolen by an employee of a small technology business from the Midlands. This employee was leaving to join a competitor firm and the information was passed on to the direct competitor. This incident wasn't detected for over a month giving the business a huge disadvantage in the market. They made changes to their policies and procedures and enhanced their system monitoring as a result of this incident.

A number of respondents continue to suffer from physical theft of computer equipment although this is no longer flagged as the most common cause of worst breaches. For large organisations, there was a small decrease of 5% in the physical theft of computer equipment by staff but an increase of 7% of physical theft by outsiders. Adequate encryption of the computer equipment could significantly reduce the impact of these thefts and it is now more and more commonly implemented by organisations.

An employee of a mid-sized technology firm reported the theft of multiple company laptops that contained confidential information. Fortunately the risk of data loss was significantly mitigated as the company encrypted all of their equipment and the impact on the business was minimal.

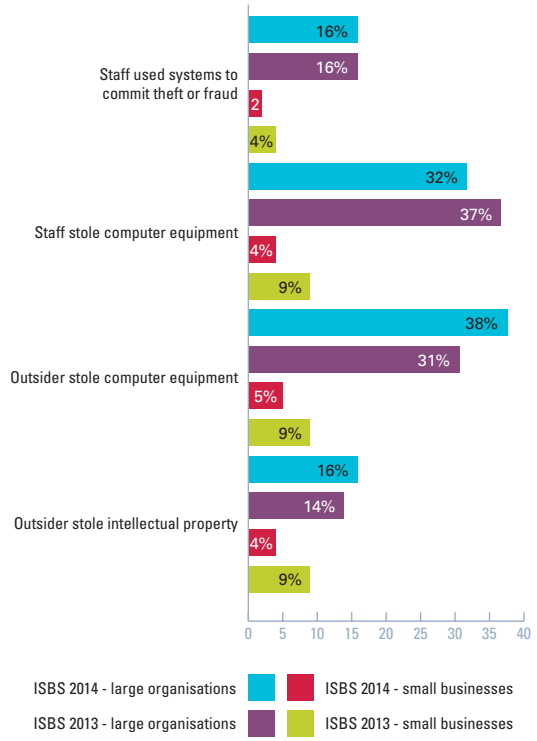
How many systems failures or data corruptions deliberately caused by staff did the affected organisation suffer in the last year?

Figure 26 *(based on 28 responses)*



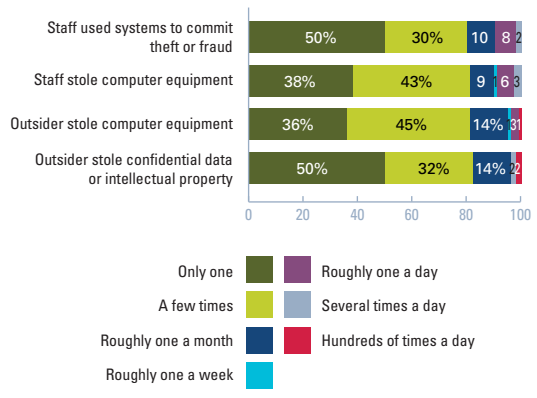
What type of theft or fraud did respondents suffer?

Figure 27 *(based on 449 responses)*



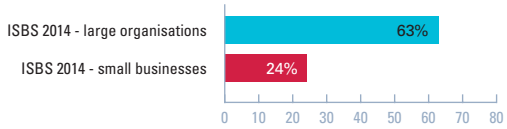
How many thefts or frauds did the affected organisations have last year?

Figure 28 *(based on 283 responses)*



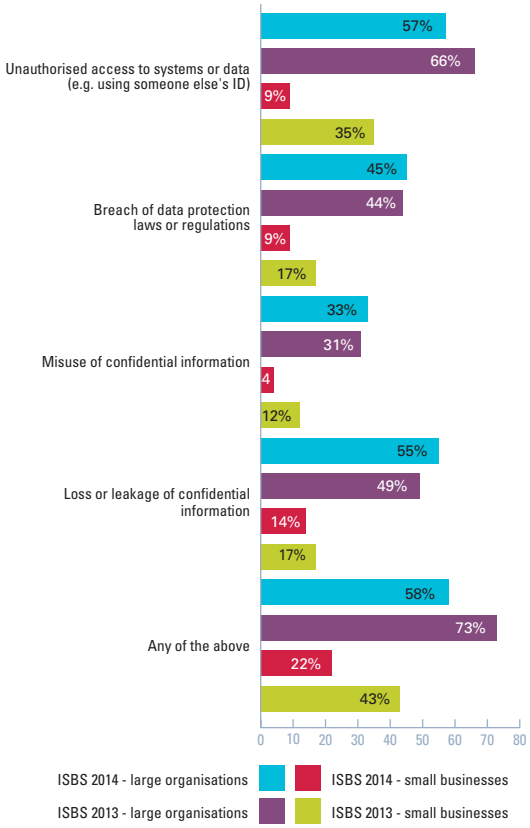
How many respondents have staff related incidents?

Figure 29 *(based on 449 responses)*



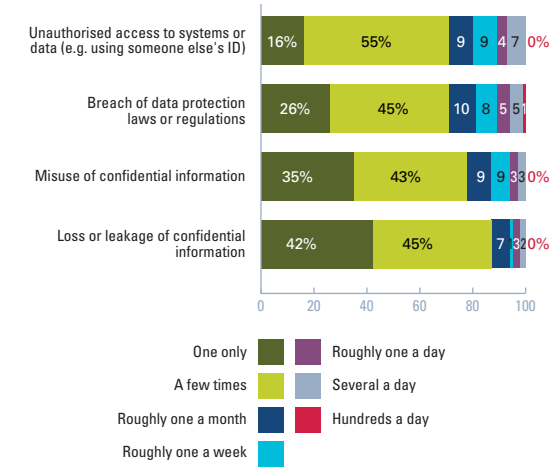
What type of staff related incidents did respondents suffer?

Figure 30 *(based on 379 responses)*



How frequent did the affected organisation have staff related incidents in the last year?

Figure 31 *(based on 531 responses)*



Other incidents caused by staff

For the first time in four years, there was a drop in the number of respondents that had staff-related incidents and this drop is significant. This year, 58% of large organisations suffered staff-related breaches (down from 73% a year ago); 22% of small businesses suffered staff-related security breaches (down from 41% a year ago). There's a strong correlation between the extent to which companies deploy ongoing information security training and awareness programmes and the likelihood of staff-related breaches. As more companies have deployed ongoing security training this year, the number of staff-related breaches has decreased as expected.

Most staff-related incidents involved unauthorised access to systems or data (e.g. using someone else's ID) for large organisations. This affected nearly three fifths of large organisations who have had staff-related incidents. This type of breach does not affect small businesses as much – only 9% of them reported this type of breach in the past year. 55% of all respondents said that they suffered this type of breach a few times in the past year but worryingly, 7% of them reported several breaches a day.

For small businesses, there is a slight decrease of 3% compared to a year ago and most of the breaches involved loss or leakage of confidential information by staff. This type of breach is the second most reported breach type for large organisations – the number reported actually rose by 6% from a year ago to 55%. The bad news continues for large organisations with a 2 % rise in the number of reported breaches due to staff misuse of confidential data. In summary, staff accidentally lost confidential information at more than half of large organisations, and actively misused it at a third of them. These results indicate that staff still play a key role in security breaches particularly for large organisations.

A member of the staff at an education institution in London did not follow the standard data handling procedure and this led to confidential information being leaked online. This incident was brought to light after a third party spotted the data and contacted them. The incident caused serious reputational damage and resulted in organisational restructuring, retraining and disciplinary action.

An employee from a large UK consultancy firm accidentally sent an email containing sensitive personal information to the wrong client. They were only made aware of this error after the unintended recipient responded to the email in complaint. This caused reputational embarrassment to the business and led to a full investigation of the incident.

Data protection breaches stayed at a similar level in the past year for large organisations, with an occurrence at almost half of them. Roughly one in ten small businesses were also affected. This type of incident is often associated with relatively large regulatory fines, high costs in terms of investigation and resolution and substantial impacts to brand reputation.

An employee of a large services company in Wales caused unauthorised disclosure of information and breach of the Data Protection Act. This breach resulted in a week of work and over £50,000 of recovery cost. Additional staff training was provided and amendments were made to security processes and procedures afterwards.

There's quite a lot of variation by sector in the extent of staff-related breaches with financial services and government sectors the most affected. It's likely that some of this disparity is due to variations in the monitoring and detection of breaches. The regional variation has also changed from a year ago. Scottish business reported a visible improvement from almost all businesses being affected in 2013 to roughly one in five this year. In contrast, around one in three respondents from London or Wales were affected.

Unauthorised access by outsiders

Cyber attacks have continued to grow in frequency and intensity over the last year and the focus seems to have shifted back towards large organisations. The proportion of large organisations that were successfully hacked continues to rise - up to nearly a quarter of respondents this year. One in four large organisations reported penetration of their networks, up by 4% from a year ago.

More worryingly, most of the affected companies were penetrated not just once but once every few weeks during the year - nearly a tenth of those affected are being successfully penetrated every day. Small businesses experienced fewer outsider attacks with 12 % of them being penetrated (down from 15% last year). Different industries experience different levels of network penetration attacks. Telecommunication companies were the most affected; nearly a quarter of them reported penetration. Roughly one in six utility companies and banks were also affected.

A mid-sized financial services company based in Wales had files randomly zipped and password protected in a hacking attempt. The business was seriously disrupted for the few days. Following this breach, the company made changes to their backup and contingency plans and increased their monitoring of third party security.

Denial-of-service attacks remain at a similar level for large organisations and decreased slightly for small businesses. Nearly two-fifths of large organisations and one in six of small businesses were affected. Telecommunications, utilities, energy and educational sectors were particularly affected by these attacks. Retail companies also reported a high volume of this type of attack in the past year. The attacks typically disable unprotected websites, but often also affect email, telephony and cause system disruption or outage.

Attackers trying to impersonate companies over the internet typically seen as phishing attacks, followed the trend as Denial-of-service attacks, remaining at similar levels for large organisations and decreasing slightly for small businesses. Half of the utilities, energy and financial services organisations were affected. Telecommunication and government sectors were also among those badly impacted. The volume of such attacks is very concerning - 9% of the affected organisations have to deal with "phishing" attacks several times a day and 5% of them receive hundreds of attacks a day.

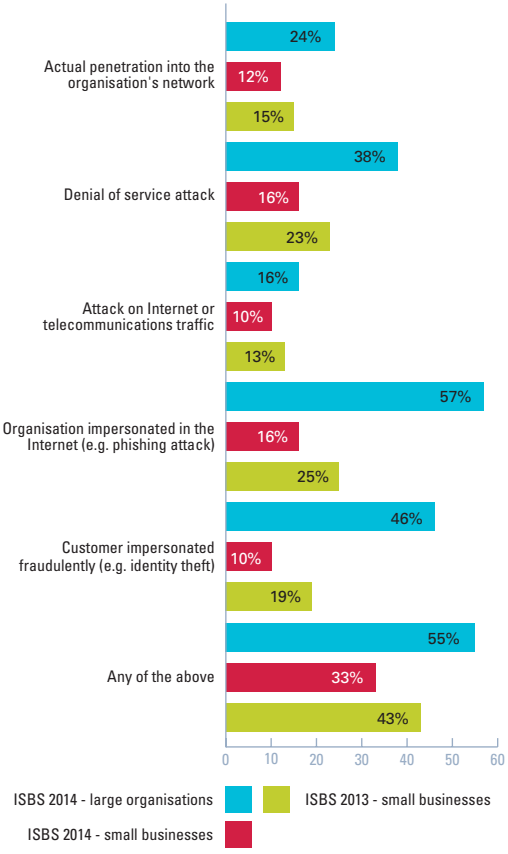
Customer impersonation and identity fraud have decreased from a year ago for among all sizes of organisations. The organisations suffering from this type of attack are mainly from the financial services and government sectors. Almost half of the financial services companies and roughly one in four government bodies were affected.

The systems of a main government body in London experienced a Denial-of-service attack. Following the incident, the software patch required to specifically guard against this type of attack was applied to the existing systems and staff were given training on its use.

A small consultancy firm lost over £10,000 in business after their website was hacked despite the attack being detected and dealt with quickly. Changes to their backup process and the existing system configurations were made after the attack. The firm is also considering increasing their threat intelligence to actively monitoring their systems.

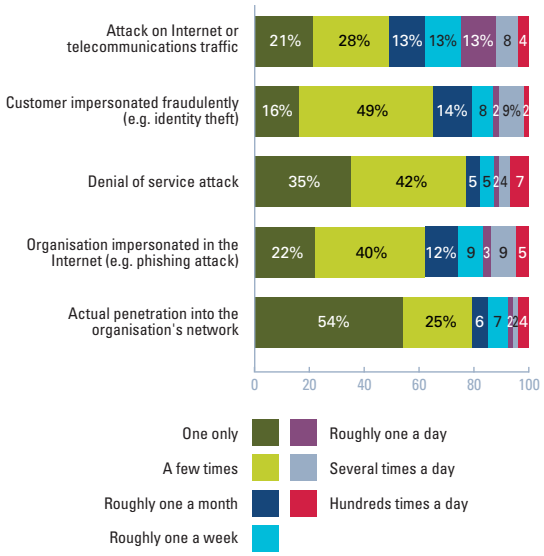
How many respondents were attacked by an unauthorised outsider in the last year?

Figure 32 *(based on 449 responses)*



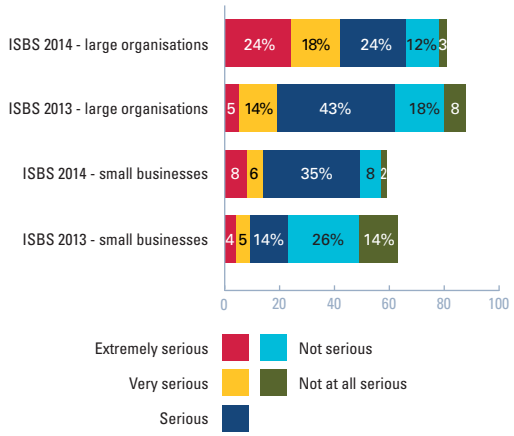
How many incidents did affected organisations have in the last year?

Figure 33 *(based on 558 responses)*



How many respondents had a serious incident?

Figure 34 *(based on 81 responses)*



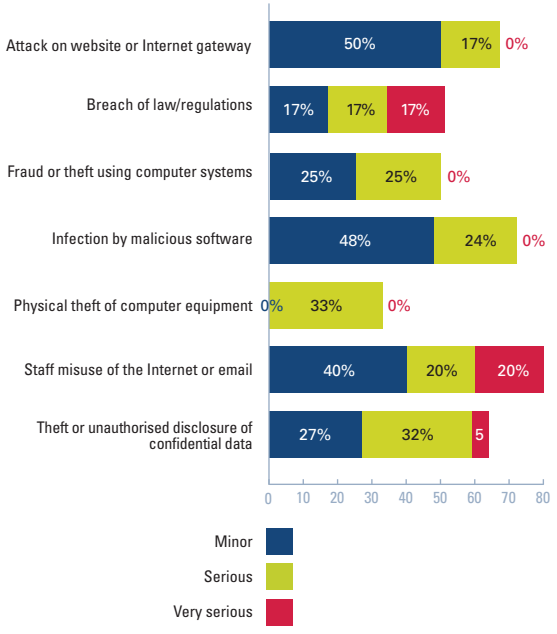
How much disruption to the business did the worst security incident cause?

Figure 35 *(based on 147 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	31%	3%	1%	0%	0%
Serious disruption		10%	5%	4%	7%
Minor disruption		5%	12%	3%	5%
Insignificant disruption		3%	5%	1%	3%

Which incidents were most disruptive to business?

Figure 36 *(based on 73 responses)*



Impact of breaches

Security breaches have direct and indirect consequences for businesses. System downtime, incident recovery cost and direct financial loss can often be easily calculated. Indirect costs such as reputational damage, legal implications and loss in revenue are harder to estimate. This survey focuses on measuring the cost of an organisation's worst security breach in the year.

Through measuring the respondents' subjective assessment of the breach's seriousness, the level of incidents has escalated this year. All sizes of organisations have experienced serious or very serious incidents. The impacts are rising and have a direct correlation to the cost of impact which has nearly doubled since 2013. 42% of large organisations have had extremely or very serious incidents reported; almost half of the small businesses have experienced serious, very serious or extremely serious incidents. Consistent with last year, respondents from financial services were most likely to have suffered a serious security breach.

A large charity organisation suffered a focused attack on their website. As there were no contingency plans in place, it took them over a week to repair the operational damage caused. They received several complaints from the customers and incurred several thousands of pounds in direct costs. As a result, the charity changed the way it fundraises from using an internally hosted website to using an external charity fundraising provider to prevent similar issues in the future.

Business disruption

The average length that respondents' worst breaches disrupted operations has once again increased, to 7-10 days for small businesses and 5-8 days for large companies. It was only 3-5 days for small businesses and 3-6 for large ones a year ago, and 1-2 days on average for both in 2012. Breaches involving staff misuse of the Internet or emails are now most disruptive to businesses this year. Breach of law/regulations and theft or unauthorised disclosure of confidential data were highly likely to cause serious business disruption. Attacks on websites and virus infection are slightly less disruptive to businesses in comparison.

The number of breaches that disrupted the business has increased from last year. A possible explanation could be that organisations are becoming more aware of what business disruption actually entails. 31% of worst breaches did not cause business disruption this year compared to 37% a year ago. Regardless of how serious the business disruption was, there has been a big jump in the proportion of businesses that had security breaches that impacted the business for more than a month.

Using the same basis as previous surveys, the cost of business disruption from the worst breach of the year continues to rise. The average business disruption cost of the worst breach range from £40,000 to £70,000 for small businesses (up from £30,000 to £50,000) and £350,000 to £650,000 for large organisations (up from £300,000-£600,000).

Legal Implication

A new question was asked regarding legal implication of a breach. 43% of respondents were able to identify the legal implication and took action but 7% of them were unaware of the associated regulations therefore no action was taken. Large organisations are doing slightly better at identifying legal implications and act on them: 52% of them were able to do so versus 46% of small businesses.

Incident response costs

The cost of incident response, recovery and remediation can easily outweigh the direct financial cost of the incident. Staff-related incidents may involve lengthy investigation to identify the root cause and to build up evidence for subsequent action. System failures, virus infections and intrusion on the network may involve process change and deployment of new systems therefore can be time consuming and expensive to fully rectify.

A large transportation company in Wales encountered a malware infection on their systems. This infection was not detected for a number of months and resulted in a massive number of man-hours and more than £250,000 spent to address the issue.

Continuing last year's increasing trend, the average time spent to fix breaches has doubled this year. Among small businesses, the average time spent on responding to incidents is 12-24 man-days, up from 6-12 man-days in 2013. The average cost of this time also rose significantly to £3,000-£9,000 compare to £2,000-£5,000 a year ago; in addition, there is a further £9,000-£17,000 in average direct cash spent on responding to incidents (up from only £500-£1,500 in 2013). In large organisations, the effort required was also much higher with an average 45-85 man-days, up from 25-45 man-days in 2013. Large organisations incurred £12,000-£34,000 in time costs compare to £6,000- £13,000 in 2013, and £80,000-£135,000 in cash costs (up from £35,000-£60,000 in 2013) on average.

A mid-sized marketing firm were informed by the National Crime Agency of their loss of customer data after receiving a number of customer complaints. Not only did this incident cause embarrassment for the company, they also spent around £250,000 responding to the incident.

Financial loss

About three tenths of the worst security breaches of the year led to lost business – rising from one in four a year ago. For small businesses, the average cost was £3,500-£7,000. This is an enormous increase and is more than ten times of the average of £300-£600 in 2013. For large organisations, £80,000-£135,000 was the average cost of lost business, roughly eight times of the £10,000-£15,000 average cost in 2013.

A local government body received a warning from law enforcement officials for a malicious attack on their systems. The attack originated from within the organisation and ended in the loss of over £500,000.

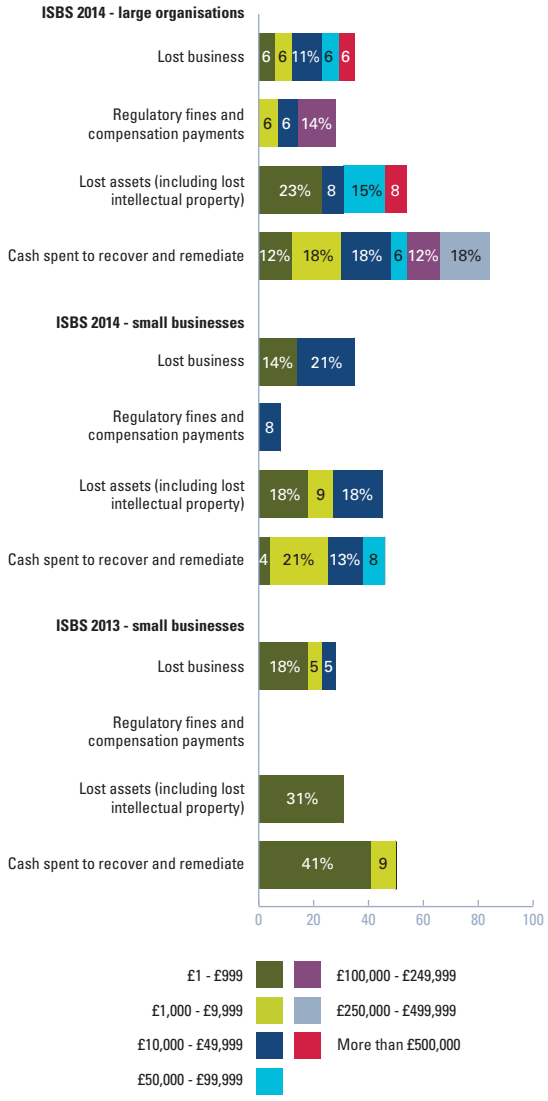
About half of the worst security breaches of the year resulted in financial loss as a result of lost assets including both physical assets and intellectual property – this figure also increased from a year ago. Consequently, there has been a significant rise in the cost of lost assets: small companies reported losses averaging £5,000-£10,000 (up from £150-£350 in 2013) and large organisations reported average losses at £70,000-£100,000 (up from £30,000-£40,000 in 2013).

One in five respondents reported losses due to compensation payments and regulatory fines. This is much more than we saw a year ago. Small businesses reported the average losses of £2,000-£4,000 compared to nothing last year; large organisations averaged £24,000-£40,000, an huge increase from £750-£1,500 a year ago.

A large legal firm in the West-Midlands suffered a £20,000 theft by a staff member who took advantage of poorly designed security processes. In addition to the monetary loss, it also took a large number of hours to detect and rectify the issue.

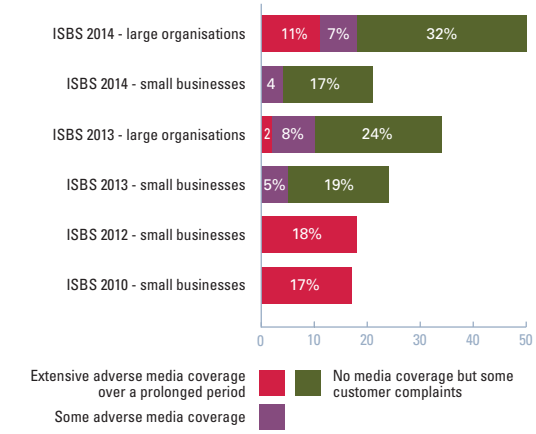
How much cash was lost or spent dealing with the worst security incident of the year?

Figure 37 *(based on 123 responses)*



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

Figure 38 *(based on 52 responses)*



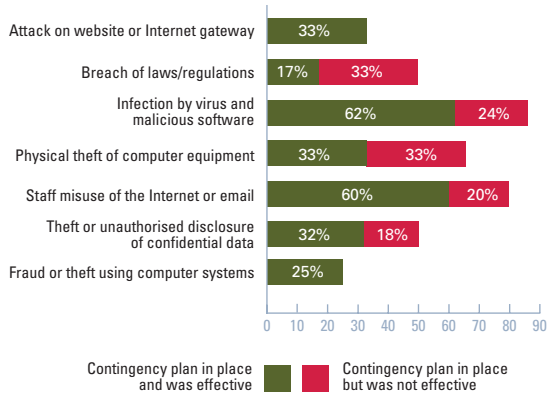
What was the overall cost of an organisation's worst incident in the last year?

Figure 39 *(based on 449 responses)*

	ISBS 2014 small businesses	ISBS 2014 large organisations
Business disruption	£40,000 - £60,000 *over 7-10 days*	£350,000 - £650,000 *over 5-8 days*
Time spent responding to incident	£3,000 - £9,000 *12-24 man-days*	£12,000 - £34,000 *45-85 man-days*
Lost business	£3,500 - £7,000	£17,000 - £24,000
Direct cash spent responding to incident	£9,000 - £17,000	£80,000 - £135,000
Regulatory fines and compensation payments	£2,000 - £4,000	£24,000 - £40,000
Lost assets (including lost intellectual property)	£5,000 - £10,000	£70,000 - £100,000
Damage to reputation	£1,600 - £8,000	£50,000 - £180,000
Total cost of worst incident on average	£65,000 - £115,000	£600,000 - £1,150,000
2013 comparative	*£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*

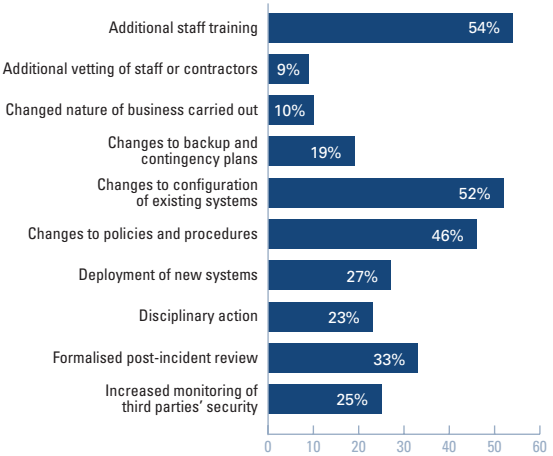
What type of security incidents do organisations plan for; and how effective are these contingency plans?

Figure 40 *(based on 73 responses)*



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

Figure 41 *(based on 79 responses)*



Damage to reputation

Damage to an organisation's reputation is challenging to quantify. Using the same approach as in previous years, our best estimate of reputational damage is £1,600-£8,000 for small businesses (similar to last year) and £50,000-£180,000 for large organisations (up from £25,000-£115,000). Reputational damage seemed to affect large organisations much more than the small ones. Although almost 70% of companies were able to keep knowledge of their worst incident internal, there was a large rise in adverse media coverage of security breaches.

A technology manufacturer operating in Wales had their reputation brought into question after the media exposed an issue of sensitive information being sent to third parties without the appropriate checks or authorisation. It resulted in a large fine paid to the authorities.

Total cost of incidents

The large rise in adverse media coverage of security breaches led to a huge rise in the average cost of organisations' worst breach of the year. Using the same basis as previous surveys, the cost of the worst breach of the year has nearly doubled last year's figures to £65,000-£115,000 for small businesses and £600,000-£1,150,000 for large organisations. As always, extrapolation of cost data across the whole of the UK should 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 doubled from 2013 and is in the order of billions of pounds per annum.

Contingency planning

66% of respondents had contingency plans in place to deal with the worst incident of the year. This figure has dropped again compared to last year as has been the case for the past two consecutive years. Large organisations continue to be more likely to have a contingency plan in place, but once again more likely for it to fail in practice.

Staff at a scientific institute were unknowingly involved in the propagation of malware across their systems through the use of infected USB devices. It took over 50 days to recover after their contingency plan was found to be ineffective. This led to changes made to their systems and implementation of more effective contingency plans.

43% of contingency plans proved to be effective. Contingency plans for virus infection and staff misuse of the internet or email proved the most effective. However, almost half of contingency plans dealing with systems failure and data corruption did not work as effectively as expected. Most organisations still struggle to get effective contingency plans in place for loss of confidential information and dealing with information security breaches.

Only 3% of respondents did not take action after their worst breach of the year. Additional staff training remains the most common step taken following breaches, which highlights the importance of staff behaviours towards effective protection. Similar to 2013, organisations are still focused on updating their technologies, improving the processes and providing training to staff after the most serious of breaches. This highlights a significant dependency on technical controls. 10% of respondents chose to change the nature of their business after their worst security breach of the year to better manage the business risk. There is also an increase in the proportion of organisations that increased their monitoring of third party security after their worst breach of the year.

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/14/767