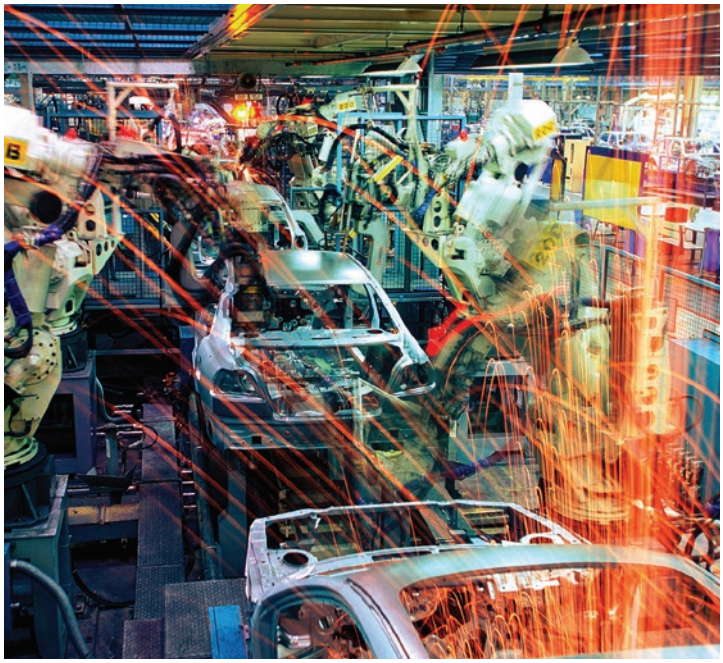
HM Government



2015 INFORMATION SECURITY BREACHES SURVEY

Technical Report

Survey conducted by

pwc

In association with

infosecurity EUROPE

Commissioned by:

HM Government

The UK Cyber Security Strategy published in November 2011, sets out how the UK will support economic prosperity, protect national security and safeguard the public's way of life by building a more trusted and resilient digital environment. The National Cyber Security Programme, backed up by £860 million of Government investment over 5 years to 2016, supports meet the objectives of the strategy www.gov.uk/government/policies/cyber-security.

Conducted by:

pwc

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Our cyber security practice includes more than 150 dedicated specialists in the UK, and more than 1,700 across our international network. Our integrated approach recognises the multi-faceted nature of cyber and information security, and draws on specialists in process improvement, value management, change management, human resources, forensics, risk, and legal. PwC has a world class reputation for its technical expertise and strong cyber security skills in strategy, assessment, design and implementation 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 20 years at the heart of the industry in 2015, 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 2 June – 4 June 2015, at the Olympia, London. For further information please visit www.infosecurityeurope.com.

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.

Ed Vaizey MP
Minister for Culture and the Digital Economy

CONTENTS

EXECUTIVE SUMMARY 6-9

1 INCIDENTS AND BREACHES
- 1.1 Trends in data breach 10
- 1.2 Types of data breach 11
- 1.3 Staff use and misuse of systems 13
- 1.4 Identifying infiltration 16
- 1.5 Reporting 18

2 COSTS AND CONSEQUENCES
- 2.1 Where is the investment in cyber security going? 19
- 2.2 The reputational impact of a breach 20
- 2.3 The most disruptive incidents 21
- 2.4 Cost of dealing with security incidents 21
- 2.5 Responding to security incidents 23

3 ATTITUDES AND TRENDS
- 3.1 What is driving information security expenditure? 24
- 3.2 The changing patterns of security expenditure 25
- 3.3 Where do organisations go for advice and assurance? 26
- 3.4 Is Cyber insurance properly understood? 28

4 ASSURANCE AND EFFECTIVENESS
- 4.1 Mobile devices - risk awareness and policy 29
- 4.2 How effective is security policy? 31

5 APPENDIX 32-48

We live in an inter-connected world that we could not have imagined even two decades ago. While it brings almost limitless opportunities, there are also threats. It is absolutely vital that the applications and connections we use are as secure as possible.

We want the UK to be one of the safest places to do business in cyber space. There are many ways we can achieve this ambition. But we cannot make progress unless we share as much information as possible about the threats we face. So we want to produce reliable information about cyber security breaches and make it publicly available. I welcome the fact that so many organisations across the UK have shared their experiences in this year's Information Security Breaches Survey, which is a key commitment in the Government's National Cyber Security Strategy.

As the number and cost of breaches have risen this year, it is encouraging to see the steps some businesses are taking to improve their cyber security. However, there is clearly a lot more Government and industry can do to continue tackling this issue. Last year, the Government launched the Cyber Essentials scheme. Nearly half of businesses surveyed have either already implemented it or plan to do so. If you use these basic technical controls, you can protect yourself against the most common cyber attacks. All businesses and organisations should adopt the scheme as a vital first step – no ifs or buts.

Of course, many businesses and organisations will need to have in place far more controls and procedures to manage the risks they face, and we will continue to work with them to make this happen.

The Government's ongoing efforts to protect and enhance the UK in cyber space will be informed by the information in this report.

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 continued to be divided into two online questionnaires and 'sticky sessions' were introduced to help increase the quality of the raw data by reducing incomplete responses and potential duplication. We removed some past questions that were no longer so important and added a few additional questions to reflect current concerns or key topics within cyberspace.

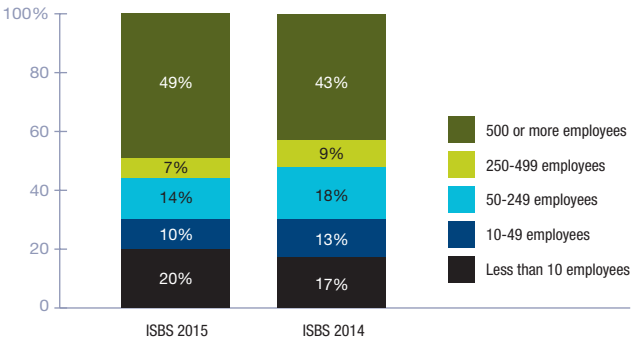
In total, there were 664 respondents. As with any survey of this nature, we would not necessarily expect every respondent to know the answers to every question. For consistency and presentational reasons we have removed the 'Don't Knows' and 'Not Applicable'. Please note that the analysis methodology is consistent with prior surveys enabling the identification and analysis of trends.

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 to the relevant question(s). 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.

The calculation of the percentages within the report is based only on those organisations who knew the answer to the relevant question(s) and also responded to that question. Therefore, wherever this report refers to "x% of organisations", this should be interpreted as "x% of organisations who knew the answer to the question and responded to it".

How many staff did each respondent employ in the UK?

(Based on 661 responses)



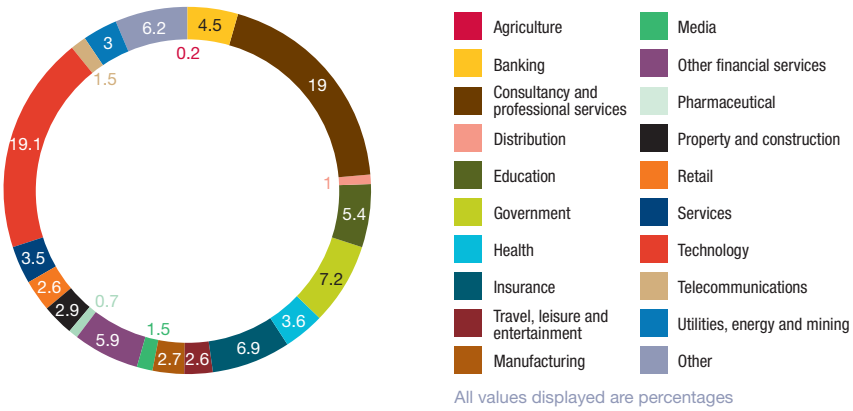
For example, where a figure shows "50% of small organisations spent up to £999 cash to recover from their worst security incident of the year" this should be interpreted as "50% of small organisations who disclosed their worst security incident and knew how much cash they had spent to recover from their worst security incident spent up to £999".

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 2014, 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.

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

(Based on 664 responses)



All values displayed are percentages

EXECUTIVE SUMMARY

Security breaches levels rise again

There has been an increase in the number of both large and small organisations experiencing breaches, reversing the slight decrease found in last year's report. 90% of large organisations reported that they had suffered a security breach, up from 81% in 2014.

90% of large organisations

74% of small businesses

had a security breach.

▲ Up from 81% a year ago.
▲ Up from 60% a year ago.

Small organisations recorded a similar picture, with nearly three-quarters reporting a security breach; this is an increase on the 2014 and 2013 figures.

59% of respondents expect there will be more security incidents in the next year than last.

The majority of UK businesses surveyed, regardless of size, expect that breaches will continue to increase in the next year. The survey found 59% of respondents expected to see more security incidents. Businesses need to ensure their defences keep pace with the threat.

14 for large organisations

4 for small businesses

is the median number of breaches suffered in the last year.

▼ Down from 16 a year ago.
▼ Down from 6 a year ago.

The median number of breaches suffered in 2015 by large and small organisations has not moved significantly from 2014.

Cost of breaches continue to soar

The average cost of the worst single breach suffered by organisations surveyed has gone up sharply for all sizes of business. For companies employing over 500 people, the 'starting point' for breach costs – which includes elements such as business disruption, lost sales, recovery of assets, and fines & compensation - now commences at £1.46 million, up from £600,000 the previous year. The higher-end of the average range also more than doubles and is recorded as now costing £3.14 million (from £1.15 in 2014).

£1.46m - £3.14m is the average cost to a large organisation

£75k - £311k is the average cost to a small business

of its worst security breach of the year.

▲ Up from £600k - £1.15m a year ago.
▲ Up from £65k - £115k a year ago.

Small businesses do not fare much better – their lower end for security breach costs increase to £75,200 (from £65,000 in 2014) and the higher end has more than doubled this year to £310,800.

Organisations continue to suffer from external attacks

Whilst all sizes of organisations continue to experience external attack, there appears to have been a slow change in the character of these attacks amongst those surveyed. Large and small organisations appear to be subject to greater targeting by outsiders, with malicious software impacting nearly three-quarters of large organisations and three-fifths of small organisations. There was a marked increase in small organisations suffering from malicious software, up 36% over last years' figures.

69% of large organisations

38% of small businesses

were attacked by an unauthorised outsider in the last year.

▲ Up from 55% a year ago.
▲ Slightly up from 33% a year ago.

Better news for business is that 'Denial of service' type attacks have dropped across the board, continuing the trend since 2013 and giving further evidence that outsiders are using more sophisticated methods to affect organisations.

30% of large organisations

16% of small businesses

were hit by DoS attacks in the last year.

▼ Down from 38% a year ago.
= The same as 16% a year ago.

The Human Factor

Staff-related breaches feature notably in this years' survey. Three-quarters of large organisations suffered a staff-related breach and nearly one-third of small organisations had a similar occurrence (up from 22% the previous year).

75% of large organisations

31% of small businesses

suffered staff related security breaches in the last year.

▲ Up from 58% a year ago.
▲ Up from 22% a year ago.

When questioned about the single worst breach suffered, half of all organisations attributed the cause to ***inadvertent*** human error.

50% of the worst breaches in the year were caused by inadvertant human error.

▲ Up from 31% a year ago.

"The Ten Steps" guidance and Cyber Essentials build on previous years progress

The percentage of organisations using the HMG "Ten Steps to Cyber Security" increased from just over one-quarter in 2014 to almost one-third in 2015. Allied to this was an increase in organisations using Government alerts to inform their awareness of threats and similar vulnerabilities.

32% of respondents use the Ten Steps guidance.

▲ Up from 26% a year ago.

The survey also found that nearly half of all organisations are badged to the HMG Cyber Essentials and Cyber Essentials Plus scheme, are on their way to accreditation or plan to be badged. ISO27001 remains the leading standard for security management.

49% of respondents badged to Cyber Essentials or Cyber Essentials Plus, on their way to accreditation or plan to be badged.

Understanding, communication and effective security awareness

The organisations surveyed continue to place importance on security awareness training. For large organisations, ongoing security training has increased since the 2013 figure of 58%, up to this year's figure of 72%; for small organisations, there has been an increase of a similar order of magnitude, up from 48% in 2013 to 63% this year.

72% of large organisations

63% of small businesses

provide ongoing security awareness training to their staff.

▲ Up from 68% a year ago.
▲ Up from 54% a year ago.

14% of respondents have never briefed their board on security risks.

Furthermore, 21% of organisations have not briefed their board in the last year.

33% of large organisations say responsibilty for ensuring data is protected is not clear.

However, 26% of organisations stated that responsibility for ensuring data is protected is very clear.

72% of companies where the security policy was poorly understood had staff related breaches.

There is a slight increase in the percentage of organisations where senior management is viewed as giving information security a 'high' or 'very high' priority.

82% of respondents report that their senior management place a high or very high priority to security.

▲ Up from 79% a year ago.

However, in some circumstances, respondents cited that a 'lack of priority' from senior management was a contributing factor in their single worst breach.

28% of the worst security breaches were caused partly by senior management giving insufficient priority on security.

▲ Up from 7% a year ago.

Information security expenditure levelling out

There is a difference in levels of security spending between organisations, based on their relative size. 44% of large organisations increased their information security expenditure, whereas in 2014, it was over half. Looking to the future, 46% of large firms expected Information Security expenditure to increase in the coming year – less than the 2014 prediction.

Small organisations reported a slightly different picture: 44% increased their information security expenditure, which is up from the previous year. However, only 7% of small firms believed that information security expenditure would increase in the coming year - significantly down from the previous year's expectations.

44% of large organisations

44% of small businesses

increased information security spend in the last year.

▼ Down from 53% a year ago.
▲ Up from 27% a year ago.

46% of large organisations

7% of small businesses

expect information security spend to increase in the next year.

▼ Down from 51% a year ago.
▼ Down from 42% a year ago.

The Telecoms sector had a sharp increase – more than doubling the percentage of their IT budget spent on security from 13% in 2014 to 28% in 2015.

Financial Services, Professional Services, and Property and Construction had levels of spending broadly in line with 2014 figures.

The survey uncovered that nearly one third of organisations had not conducted any form of security risk assessment on their enterprise. This reverses the trend of the past two years and questions whether businesses have the skills or experience to perform these to an adequate degree.

32% of respondents in 2015 haven't carried out any form of security risk assessment.

▲ Up from 20% a year ago.

60% of respondents are confident they have sufficient security skills to manage their risks next year.

= Similar to 59% a year ago.

26% of respondents don't evaluate how effective their security expenditure is.

▼ Down from 33% a year ago.

Businesses need to manage the risks associated with new technology

Innovation often brings new risks; there has been an increase in information security breaches caused, or enabled by technology meant to improve productivity and increase collaboration.

13% of large organisations had a security or data breach in the last year relating to social network sites.

= Similar to 12% a year ago.

15% of large organisations had a security or data breach in the last year involving smartphones or tablets.

▲ Up from 7% a year ago.

7% of respondents had a security or data breach in the last year relating to one of their cloud computing services.

= Similar to 5% a year ago.

3% of worst breaches were due to portable media bypassing defences.

▼ Down from 10% a year ago.

Organisations are seeking new ways to manage security risks

The difference between the higher levels of uptake of cyber threat intelligence and cyber liability insurance coverage reflects the different rates of maturity across industry of how security risks are managed. Although there appears to be a large drop in insurance coverage, this may be due to a greater understanding of the cover provided by standard business disruption insurance policies in the event of an information security breach.

39% of large organisations

27% of small businesses

have insurance that would cover them in the event of a breach.

▼ Down from 52% a year ago.
▼ Down from 35% a year ago.

63% of respondents currently invest in or plan to invest in threat intelligence (actively monitor cyber threats to their organisations).

▼ Slightly down from 69% a year ago.

Key observations of the year

1. The number of security breaches has increased, the scale and cost has nearly doubled. Eleven percent of respondents changed the nature of their business as a result of their worst breach.
2. Not as many organisations increased their spending in information security, and fewer organisations than in previous years expect to spend more in the future.
3. Nearly 9 out of 10 large organisations surveyed now suffer some form of security breach – suggesting that these incidents are now a near certainty. Businesses should ensure they are managing the risk accordingly.
4. Despite the increase in staff awareness training, people are as likely to cause a breach as viruses and other types of malicious software.
5. When looking at drivers for information security expenditure, 'Protecting customer information' and 'Protecting the organisation's reputation' account for over half of the responses.
6. The trend in outsourcing certain security functions and the use of 'Cloud computing and storage' continue to rise.

1 INCIDENTS AND BREACHES

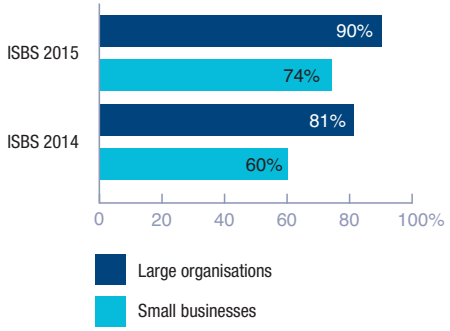
1.1 Trends in data breach

There has been an increase for both large and small organisations suffering breaches. Overall, 90% of large organisations and 74% of small organisations reported that they had suffered any form of security breach. This represents a 9% year on year increase for large organisations, and over 20% for smaller businesses.

Furthermore, two-thirds of large organisations reported suffering from non-malicious or accidental breaches – the same level as last year – and one-quarter of small organisations suffered a similar type of incident. Both large and small organisations predicted that there will be more security related incidents in the future.

How many respondents had any form of security breach in the last year?

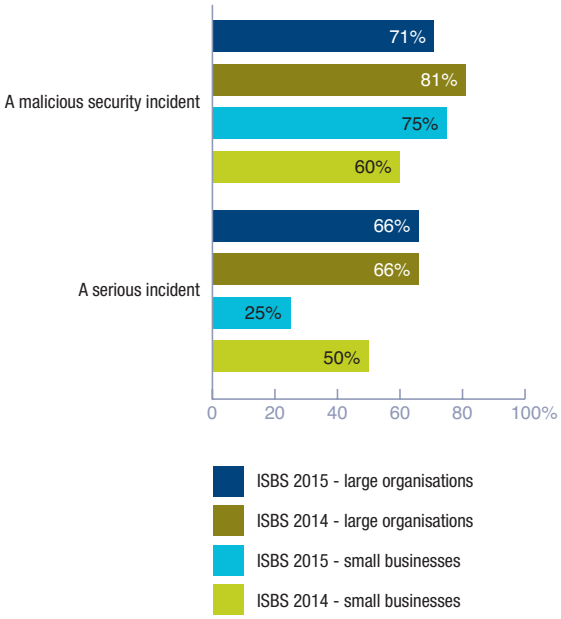
(Based on 256 responses)



The percentage of organisations, both large and small, who have reported having a security incident has risen this year, most noticeably for small organisations, and an overwhelming majority expect that the trend will continue upwards. In fact, nearly 9 out of 10 large organisations now suffer security breaches. This underlines the importance of making sure basic controls are in place, such as following the HM Government's "Ten Steps to Cyber Security" or implementing the Cyber Essentials scheme. Increased cyber awareness across all sizes of organisation allied to better detection of malicious software and infiltration, may help to explain why organisations are reporting a higher number of breaches in 2015.

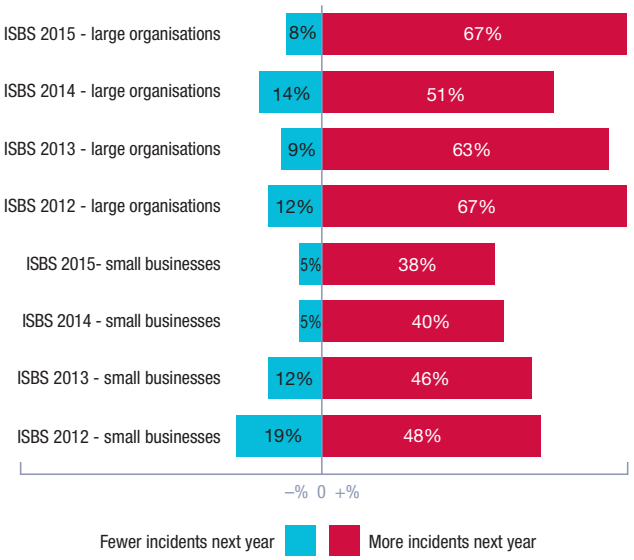
In the last year, how many respondents had...

(Based on 177 responses for large and 76 responses for small)



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

(Based on 141 responses)



1.2 Types of data breach

An increase in targeted attacks

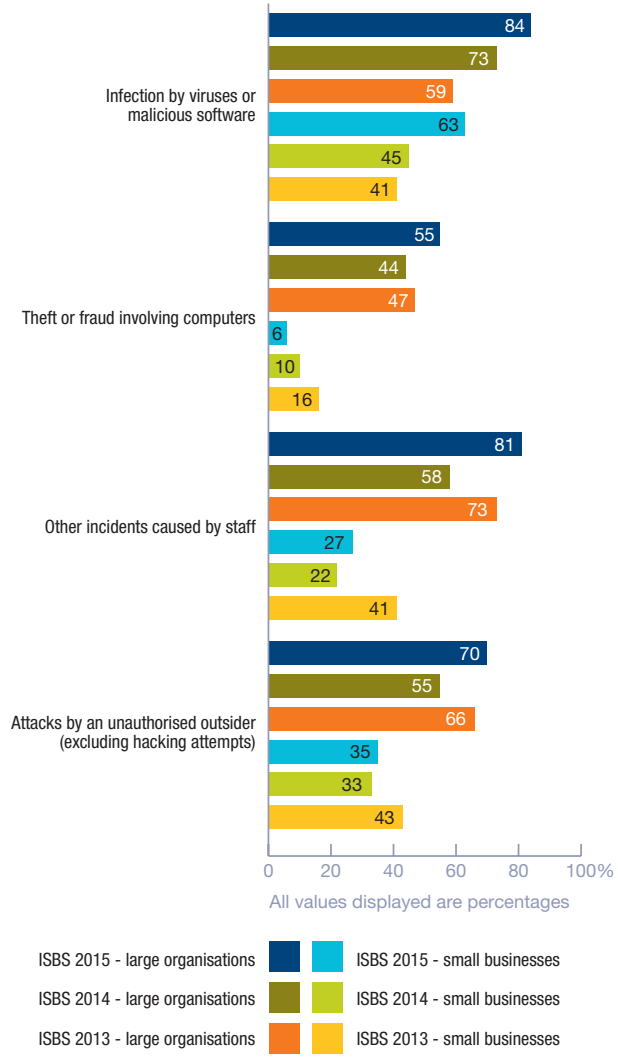
Many organisations suffered an infection by malware, with large organisations (84%) ahead of their smaller counterparts (63%). This was also an increase in the equivalent 2014 figures of at least 15%.

Eighty-one percent of large organisations stated that there was an element of staff involvement in some of the breaches that they suffered; this was an increase of nearly 40% year on year. For small organisations, the figure was 27%, up from last year's figure of 22%. Staff-related breaches are examined in more detail later in the report.

When asked what was the worst single incident suffered by organisations, there was a shift in responses from the previous year.

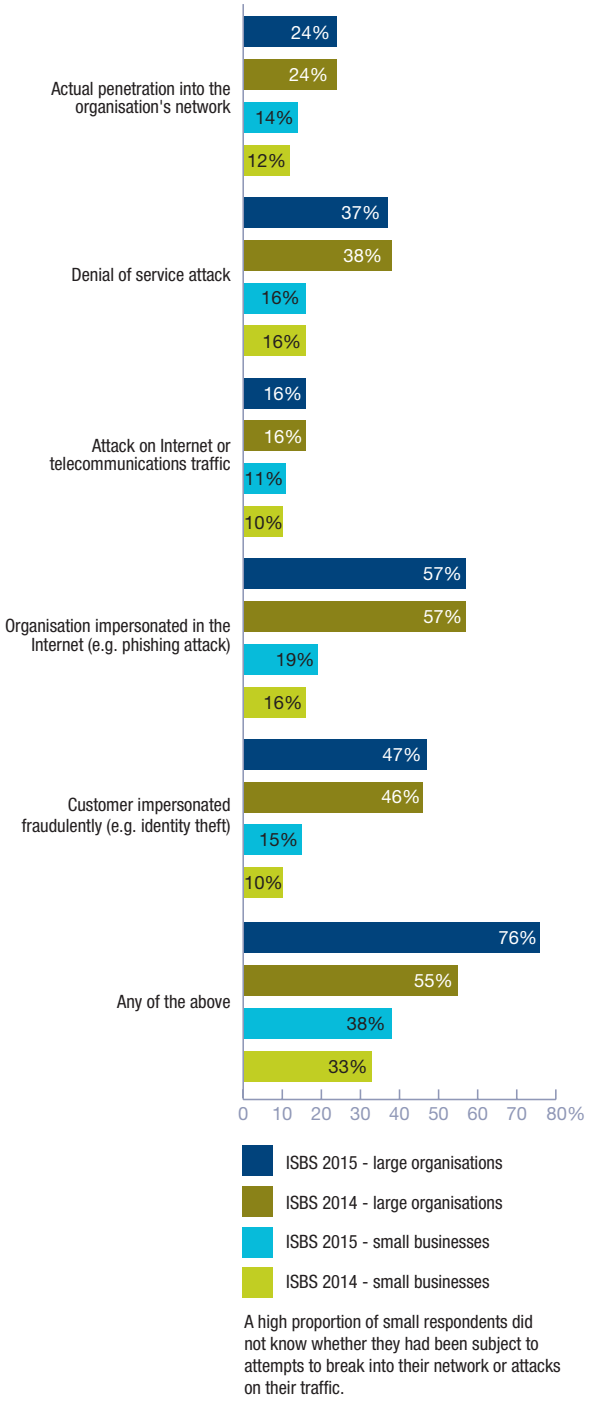
What type of breaches did respondents suffer?

(Based on 584 responses for large and 355 responses for small)



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

(Based on 140 responses for large and 90 responses for small)



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.

For large organisations, the proportion of single worst incidents caused by malware related incidents has halved, a trend which is further reduced in small organisations. Instead, 'Theft or unauthorised disclosure of confidential information,' and 'Attack or unauthorised access by outsiders' were the two highest scored responses for both large and small organisations.

Considering all breaches, there was a noticeable 38% year on year increase of unauthorised outsider attacks on large organisations, which included activities such as penetration of networks, denial of service, phishing and identity theft. Overall, three-quarters of large organisations suffered from this type of attack in 2015, up from just over half the previous year.

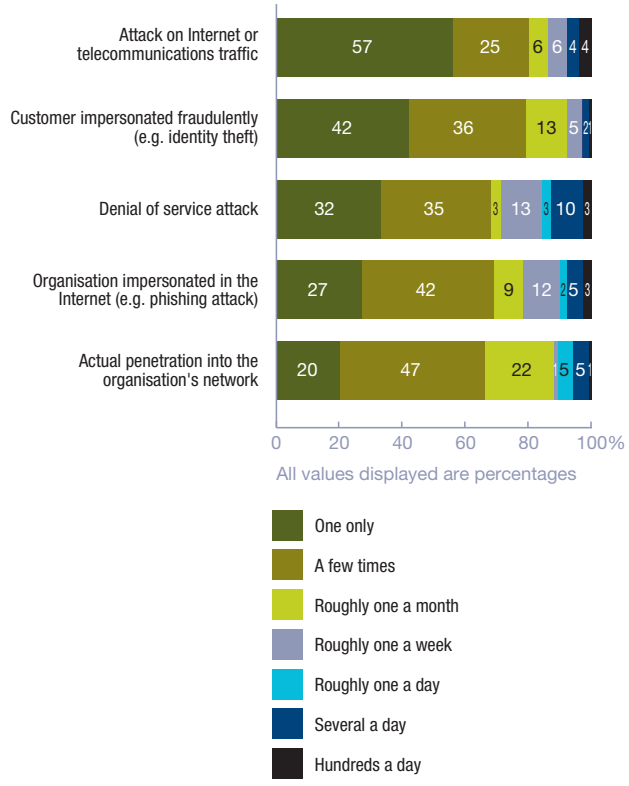
The small organisations surveyed also experienced an increase in these types of attacks but not yet at same level as their larger counterparts; 38% of small organisations suffered unauthorised outsider attacks, up from 33% in 2014. This could reflect either their reduced scale and visibility to attackers or because they do not have the same capability to detect attacks

The survey also found that the frequency of penetration into an organisation's network had increased year on year. In 2014, a single instance of network penetration was reported by 54% of those who responded; this year, the single instance figure had dropped to just 20% whereas those experiencing penetration 'a few times' throughout the year had nearly doubled to 47%.

In contrast, frequent large and unsophisticated attacks seem to be declining amongst those surveyed. The percentage of organisations suffering daily and hourly attacks of this nature has either dropped or remained static. For example, when asked about attacks on internet or telecommunication traffic, 57% of organisations reported suffering a single instance. Asked the same question about instances of Denial of Service (DoS) attacks, two thirds of organisations responded that it had happened 'only once' or 'less than a few times.'

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

(Based on 368 responses)



These results point to some changing trends in the type of breaches that are affecting businesses. Firstly, malicious software continues to disrupt business but there is a trend away from them being the main cause of the single worst incident.

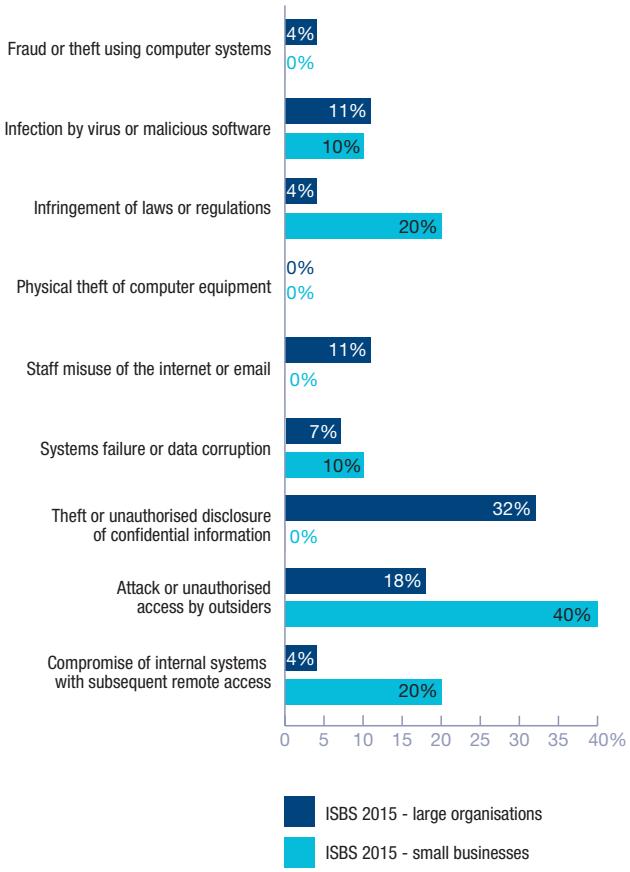
Secondly, the nature of the most serious incidents is changing to become more targeted; small businesses should not presume that they will escape targeted attacks. All businesses should ensure they understand their information assets and manage the risk to them accordingly.

Network and DoS attacks still happen and organisations need to be prepared, but the frequency has dropped by about a half. At the same time, the success attackers are having in penetrating networks is increasing, providing the evidence that breaches are becoming more targeted and less opportunistic.

> A large London based insurance firm suffered reputational damage as a result of a third party breach in which customers' data was stolen. The contract with the supplier stipulated certain controls which turned out not to be in place.

What was the worst security incident faced by respondents?

(Based on 28 responses for large and 10 responses for small)



A large organisation based in the east of England had two separate but linked malware attacks within six months of each other. This was as a result of using an unpatched application component (self-contained units of code which integrate with other systems) provided by a third party. Following the attack the firm changed its ways of working with suppliers to ensure that all application components were identified and patched to protect them from malicious exploitation of known vulnerabilities; the incident was also logged with ActionFraud. Having secure configuration features is one of the activities in the HM Government's "Ten Steps to Cyber Security;" by applying updates and patching systems, organisations can help ensure they are protected against the latest versions of malware in circulation.

A small consultancy and professional services firm with UK operations had its VoIP (network based voice communication) servers compromised as a result of a brute force attack. Passwords were obtained and the attackers then made a significant amount of international calls at no cost. Following the incident, top management placed a very high priority on information security and invested in new technical controls, a managed security service and outsourcing to obtain the required skills.

1.3 Staff use and misuse of systems

As noted above, 81% of large organisations stated that there was an element of staff involvement in some of the breaches they suffered.

The types of incidents reported by large organisations included:

- Unauthorised access to systems or data (for example, using someone else's ID) – 65% in 2015, up from 57% in 2014;
- Breach of data protection laws or regulations – 57% in 2015, up from 45% in 2014; and
- Loss or leakage of confidential information – 66% in 2015, up from 55% in 2014.

Twenty-seven percent of small organisations suffered an incident caused by staff.

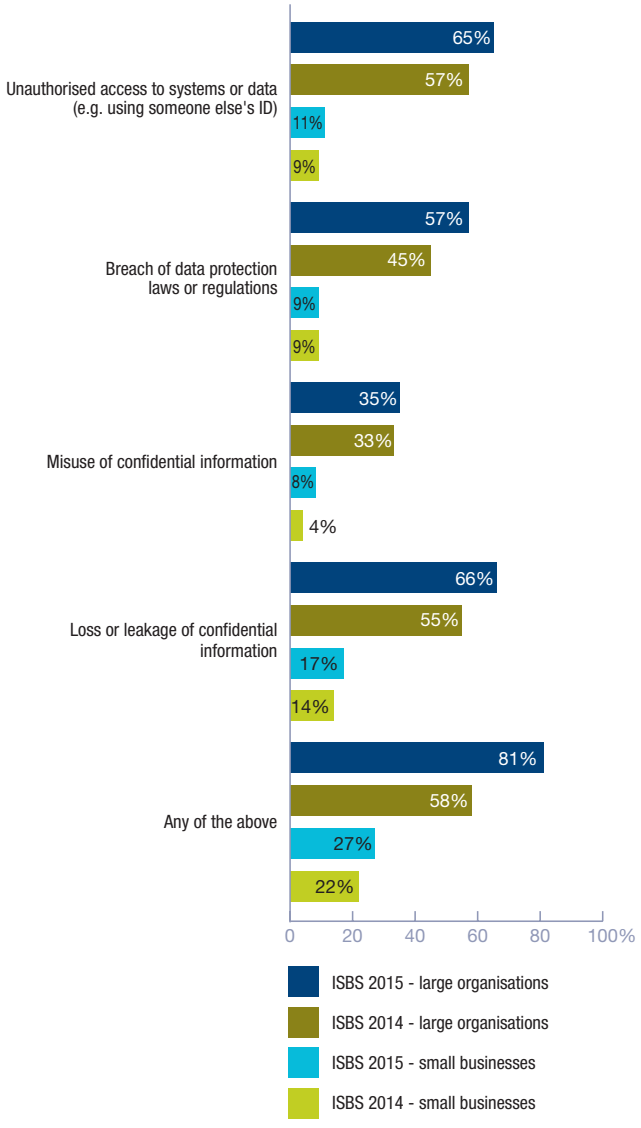
Examining the types of incident suffered, there was broadly an increase in every type of incident – the highest reported incident type being 'Loss or leakage of confidential information' at 17%.

People are the main vulnerabilities to a secure enterprise. Respondents believe that inadvertent human error (48%), lack of staff awareness (33%) and weaknesses in vetting individuals (17%), were all contributing factors in causing the single worst breach that organisations suffered.

Furthermore, 28% of respondents reported that the worst security breach was partly caused by senior management giving insufficient priority to security within their organisation.

What type of staff related incidents did respondents suffer?

(Based on 148 responses for large and 90 responses for small)



What was the origin (threat actor / source) of the breach?

(Based on 39 responses)

In light of this, organisations should consider whether enough attention and investment is being directed at these issues. Section 2.1 examines where the spending is going in relation to security controls.

Deliberate or accidental breaches?

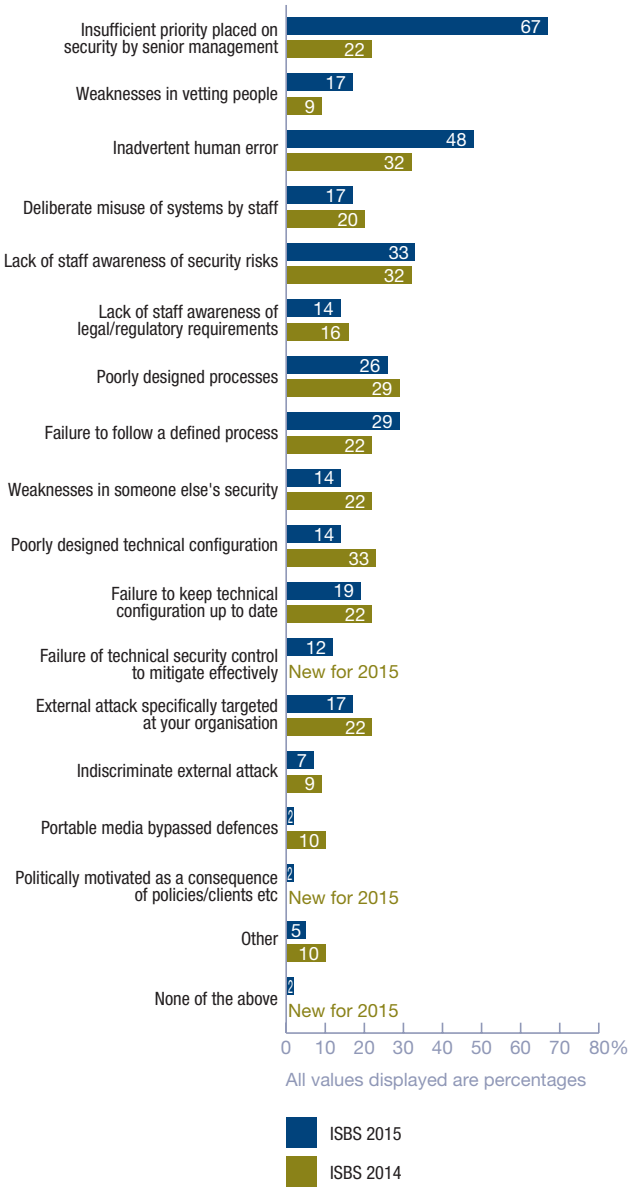
Delving a little deeper into the statistics reveals that inadvertent human error caused half of the single worst security breaches for all respondents in 2015. This was a marked increase of over 60% year on year, and continues the trend since 2013 where accidental or inadvertent action by individuals was the main cause for the single worst breach.

In contrast to the high level of accidental loss, deliberate misuse of systems by internal sources – employees and contractors – accounted for 18% of the single worst security breaches for all sizes of organisation.

Again looking at the single worst breach suffered in 2015, human factors – accidental and deliberate, inside an organisation and within the supply chain – account for over half (21 cases out of the 39 recorded) of all sources of a breach. This is over twice that of 'Organised crime' which was reported as being responsible for 23% of incidents (9 out of the 39 recorded).

Which of the following factors contributed to the incident occuring?

(Based on 42 responses)



Whilst the internet and email has revolutionised how people communicate in the workplace, the rise of technology designed to improve collaboration, productivity and innovation has been matched by a rise of employee-related breaches affecting organisations.

Regardless of the motivation of an insider – be it a deliberate act of theft or designed to embarrass an organisation; or if the breach was inadvertent due to a lack of internal controls – the threat from 'insiders' has not diminished across the UK. Neither is this isolated to one type of breach, as "virus infection," "theft" and "unauthorised access" – all very different types of information breach – increased for all sizes of organisation from 2014 to 2015.

One approach by organisations has been to invest in staff training, which now sees 90% of large organisations and 78% of small businesses having this on induction, with 72% of large organisations and 63% of small businesses having ongoing awareness and education programmes. These figures are also an increase on the 2014 level, indicating that organisations are trying to address the vulnerability.

Given the levels of staff-related breaches, it is clear that training is important but organisations should consider how effective their current offering is if the number of these incidents continue to increase. A number of government supported resources are available, including the Open University Cyber Security online education course, as well as a number of certified training courses backed by CESG (Communications-Electronics Security Group).

Boards and senior management should consider whether they are taking sufficient steps to ensure a culture of security in their organisation at a time when internal, accidental factors remain the largest cause of information security breaches. Organisations should examine how effective their training really is – whether it is mandatory, interactive, tested and engaging; or if it is optional and suffers from low take up.

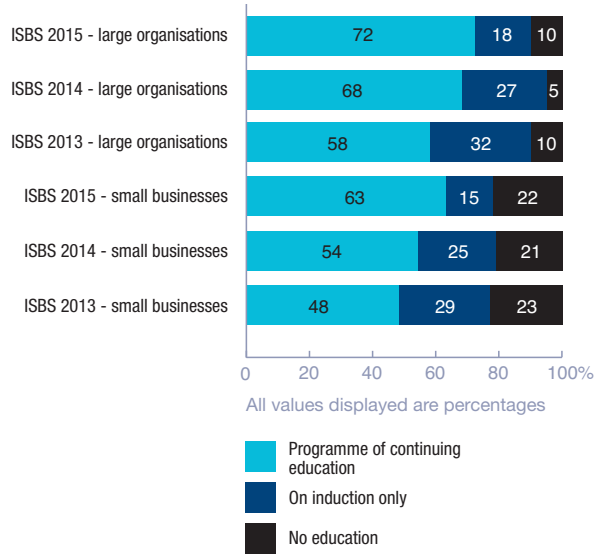
90%

of large organisations had a security breach (up from 81% a year ago)

An employee of a large consultancy firm based in the south east of England obtained sensitive client data and used it for business development purposes without permission. The incident caused reputational damage and resulted in the engagement of legal counsel and revenue loss of over £500,000. Following the incident, the firm implemented targeted security training for its staff.

How do respondents ensure staff are aware of security threats?

(Based on 152 responses for large and 87 responses for small)



A medium sized technology company with UK operations had a malware infection resulting from an employee downloading files from a peer-to-peer file sharing website onto a company laptop. It had a serious impact on business operations as it took over a week to recover. Over £100,000 in revenue was lost as a result of the incident and over £250,000 was spent on addressing the breach.

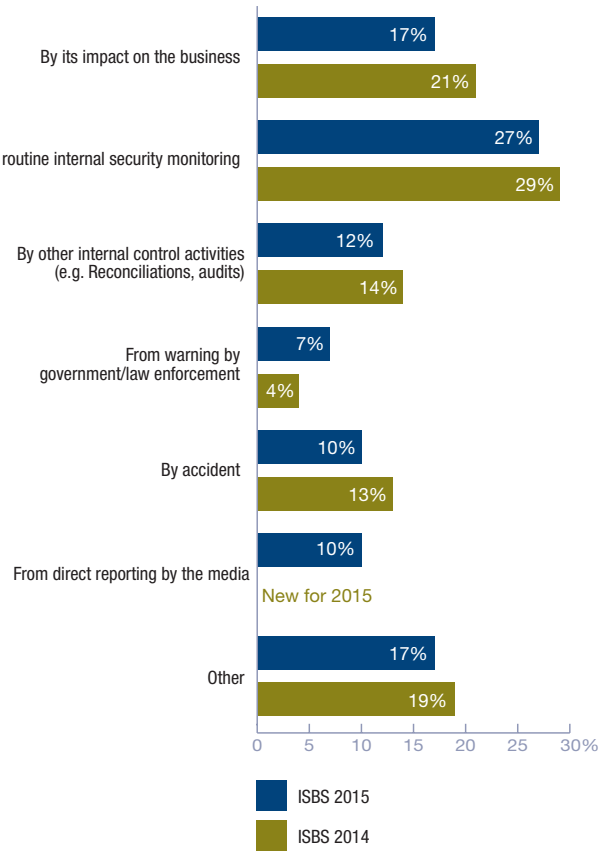
1.4 Identifying infiltration

Given that, 90% of large organisations and 74% of small organisations suffered a 'Malicious security incident' in the past year, it is important to understand how effective organisations are in identifying these incidents.

Of the 39 organisations who responded to this section, just over a third spotted incidents (36%) either immediately or within a few hours; an additional 31% found the incident within a week. Although this implies that two-thirds of organisations are spotting breaches within seven days of an incident occurring, this does mean that the remaining third are taking anywhere from one week to over 100 days to identify an incident.

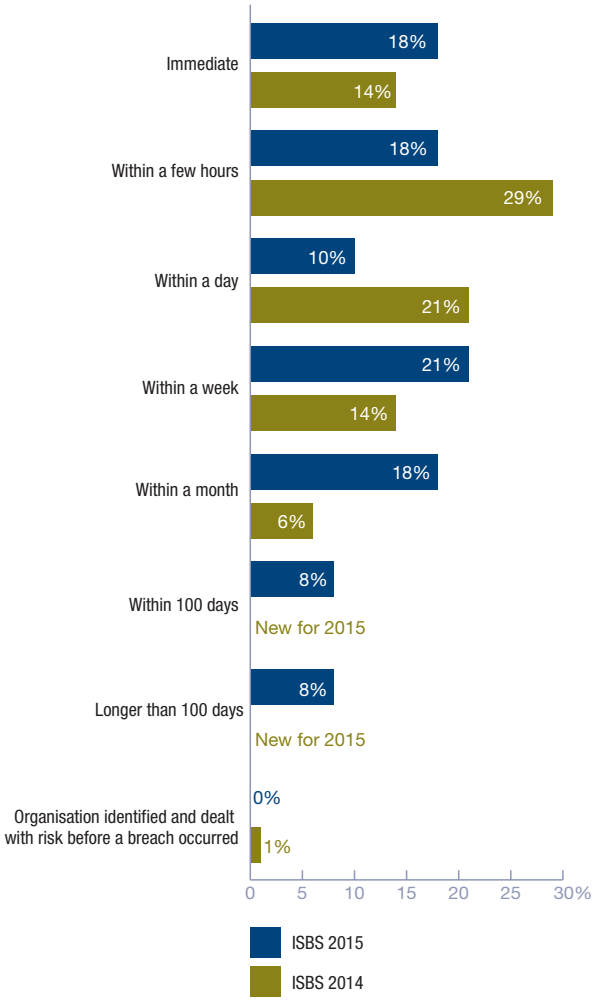
How was the incident identified?

(Based on 41 responses)



How long was it between the breach occurring and it being identified as a breach?

(Based on 39 responses)



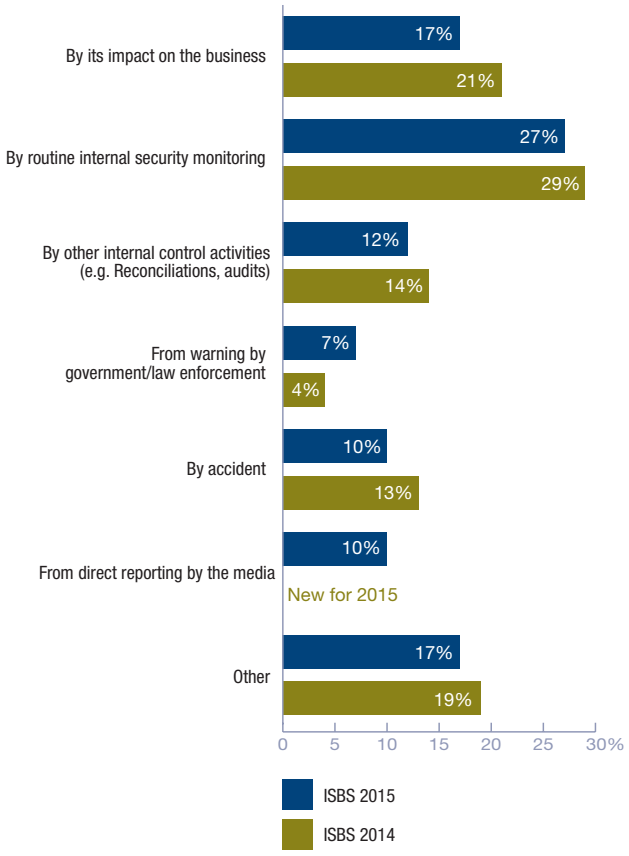
There appears to be four 'waves' to spotting an incident – either it is identified immediately, between a day and a week, within a month or longer than one month. Three out of 39 organisations took longer than 100 days to identify an incident; in some cases only finding a breach when there was a change in processes or infrastructure.

Of course, these figures only relate to breaches which have been discovered; many more will persist undetected. Recent stories in the press highlight that many firms are only aware of a data breach if confidential details are posted on social media, and indicates that the time to infiltrate an organisation is measured in days, whereas the time to detect is measured in months.

Traditionally, internal security monitoring and good patch management were relied upon to provide a high level of protection for the enterprise. The survey reports that only 27% of incidents are detected through routine security monitoring and failure to keep patched contributed to 12% of breaches, as far as respondents were aware. It is clear that maintaining patch levels to guarantee enterprise security can no longer be relied upon; whilst important, it should not be the sole method of control, but be one in an array of measures.

How was the incident identified?

(based on 41 responses)



> Police were informed after a member of staff of a large government organisation misused their position to obtain data. It took the organisation a few months to identify the breach. This had a serious impact on the organisation even though the incident was only made known internally.

1.5 Reporting

When asked which agencies and authorities were notified on the occasion of the worst breach in 2015, there was no outstanding response. One in 10 organisations reported breaches to ActionFraud – the national fraud and Internet crime reporting centre; 14% reported it to the Police and 19% reported it to other government Agencies.

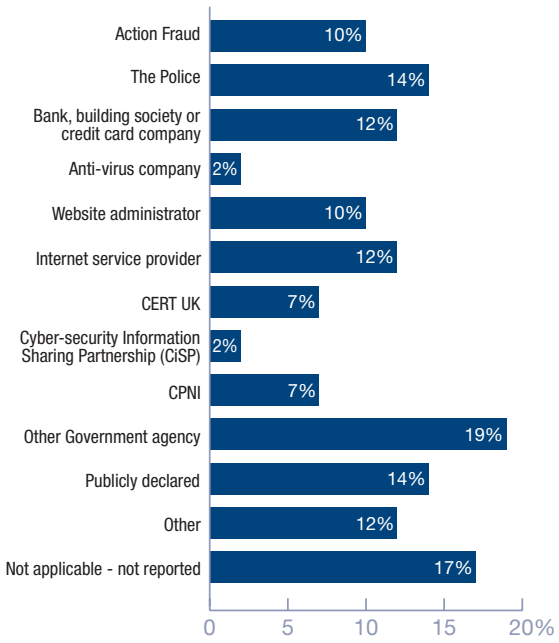
With reference to the single worst data breach, 14% of all respondents were unaware of the relevant legal regulations or what action to take in the event of a breach. Only 22% of organisations thought they knew what they should do and followed with actions.

It appears that law enforcement agencies are not being informed of all attacks. This makes it challenging for the agencies to estimate the scale and types of crimes that are being committed and respond accordingly.

Interestingly, only 2% of organisations passed information of their worst breach to an anti-virus company. However, anti-virus companies can only make improvements to systems and products if they are aware of attack vectors, methodologies and scale.

Who was this breach reported to?

(Based on 42 responses)

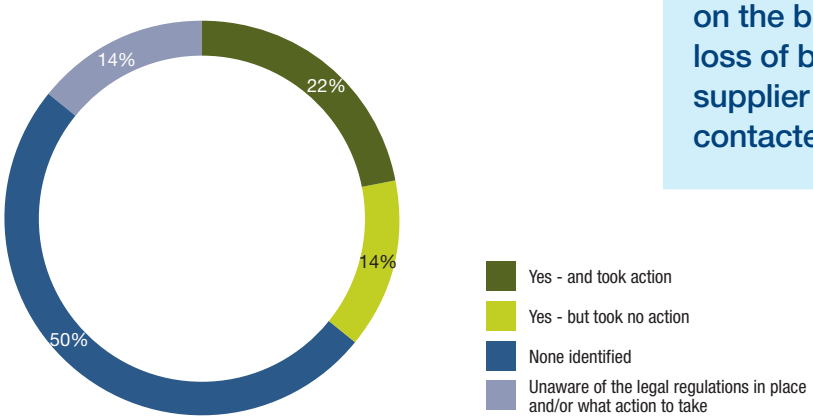


This year's survey echoes previous findings that the level of reporting in the UK remains low. Perhaps the fear of reputational damage and potential compensation costs, along with the lack of reporting culture in this area, means that most organisations are not willingly admitting to information security breaches.

> A small technology company based in London experienced a system failure which corrupted data and resulted in business disruption. This was caused by data centre outage, which was caused by a leased backup Internet line failing. This had a serious impact on the business, resulting in revenue loss of between £1000 and £9,999. The supplier and customers affected were contacted.

Did you identify any legal implications due to the nature of the breach?

(Based on 36 responses)



A large charity based in the south west of England suffered reputational damage when its customers' credit card data were compromised and used on a third party system. It took the charity over a week to restore operations to normal and it spent between £10,000 and £49,999 responding to the incident. The charity involved the Payment Card Industry (PCI) Forensic Investigator and the bank.

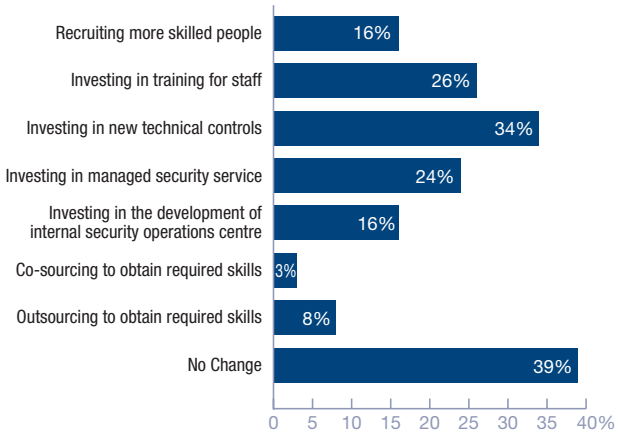
2 COSTS AND CONSEQUENCES

2.1 Where is the investment in cyber security going?

As the result of a breach, over 60% of organisations undertook at least one action to try to ensure there would not be a repeat. One-third of respondents decided to invest in technical controls, one-quarter (26%) invested in the training of staff, while just under a quarter (24%) decided to outsource some of their security through a managed service, reflecting the growth in the outsourcing sector.

As a consequence of the incident, have you changed your investment in cyber security?

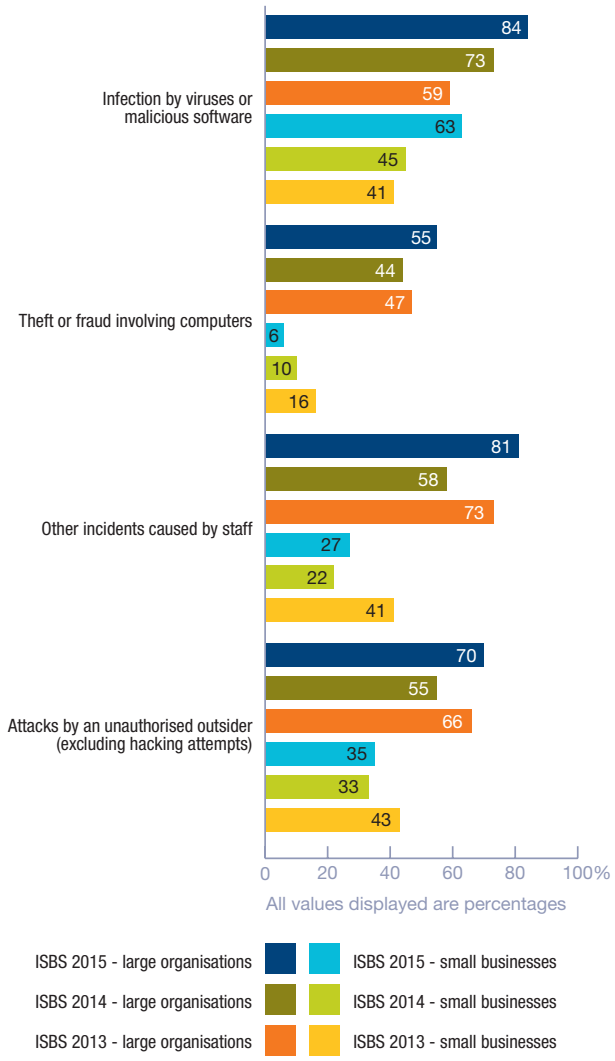
(Based on 38 responses)



The survey also established that 39% of organisations had not changed their investment in cyber security despite suffering from an incident.

What type of breaches did respondents suffer?

(Based on 584 responses for large and 355 responses for small)



As the findings above show, breaches are increasingly due to people within an organisation – often inadvertently. Whilst technical controls have their place, organisations should take the opportunity to question the balance between their investment in technical controls and measures to address the human factors present in Information Security breaches. The increasing involvement of internal security experts (explored in more detail below) may help senior management and boards direct spending appropriately.

Controls still have their place

The number of virus and malware infections suffered by small organisations dropped by a noticeable 40% from last year, indicating that the small organisations surveyed are becoming more serious about their package of defences against these types of attack. It certainly appears that small organisations have improved their virus and malware defences, and further explains the increase in the proportion of serious breaches being targeted, as opposed to blanket infections.

2.2 The reputational impact of a breach

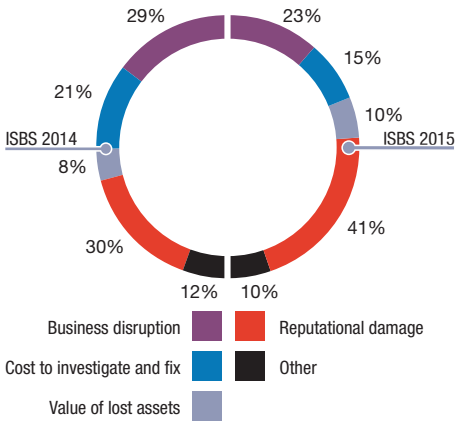
When asked what made a particular incident 'the worst', 16 out of the 39 organisations who responded cited that it was the damage to their reputation which had the greatest impact. This is an increasing trend, up from 30% of respondents in 2014 to 41% this year.

The figures from the survey also identified that 35% of large organisations stated that their most serious incident had resulted in 'extensive adverse' or 'some adverse' media coverage, an increase in both categories over the combined level of 18% in 2014.

Equivalent statistics for small organisations show that 13% of them stated that their most serious incident had resulted in some adverse media coverage – also an increase over last year's reported 4%.

What made this incident the worst of the year?

(Based on 39 responses)

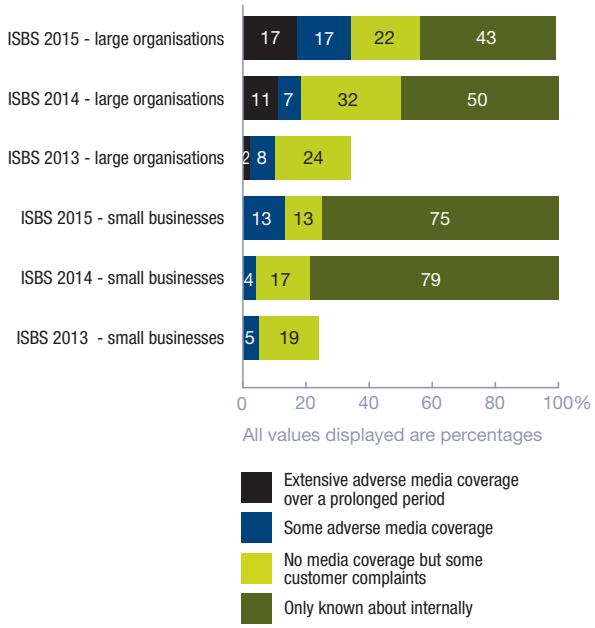


Radical changes caused by social media, a more demanding general public and increasing social activism have created a new dynamic where organisations are becoming increasingly worried about how they are perceived. This has transformed how organisations operate and communicate.

The increase in the media coverage of breaches may also reflect increased awareness of the cyber threat in the general population.

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

(Based on 23 responses for large and 8 responses for small)



> A large government organisation based in the south of England had a sensitive data disclosure breach due to human error following the amendment of a report by a member of staff. This had a serious impact on the organisation resulting in reputational damage. The 400 clients affected were notified via email or post.

A large telecommunications organisation's corporate website was taken offline for a short period of time. This meant customers were unable to access their accounts and the organisation was unable to sell their products and services online. This impacted business operations and their reputation.

2.3 The most disruptive incidents

The survey found that four of the 36 organisations who responded, were still suffering either 'serious' or 'very serious' disruption a month after their worst single incident occurred. On a more positive note, 16% of organisations encountered a similar level of 'serious' or 'very serious disruption' for less than a day, implying that business resilience procedures stood up well in these circumstances. Section 2.5 examines responses to incidents in more detail.

A large financial services company based in the south east of England suffered an attack which compromised their website with malicious code making it unusable. There were no contingency plans in place. The breach had a serious impact on business operations as it took between a week and a month to restore them to normal.

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

(Based on 36 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	19%	8%	3%	3%	6%
Serious disruption		8%	3%	8%	6%
Minor disruption		3%	11%	6%	3%
Insignificant disruption		3%	6%	3%	3%

2.4 Cost of dealing with security incidents

Every year, the survey seeks to understand the cost of dealing with security incidents, taking into account the activities which organisations must perform to operate securely once more. In 2015, the response rate to this set of questions was low, perhaps indicating a reluctance to share further details of their worst single breach, or else not having the in-depth knowledge to explain how the costs were accumulated

From the information provided, the survey did find that the total cost of dealing with incidents continues to increase. Looking at the single worst breach suffered, the costs to large organisations range from just under £1.5 million (£1,455,000) to £3.14 million. For small organisations, the range starts at £75,200 to £310,800. These figures account for activities such as business disruption, days spent responding to an incident, loss of business, regulatory fines and loss of assets.

Using past surveys as a foundation, these numbers continue the upward trend seen since 2012. The cost of dealing with the single worst incidents for large and small organisations being reported as follows:

(Based on 75 responses for large and 47 responses for small)

	ISBS 2015 small businesses	ISBS 2015 large organisations
Business disruption	£40,000 - £225,000 over 2 - 12 days	£800,000 - £2,100,000 over 4 - 11 days
Time spent responding to incident	£3,000 - £10,000 13-24 man-days	£10,000 - £30,000 40-80 man-days
Lost business	£25,000 - £45,000	£120,000 - £170,000
Direct cash spent responding to incident	£250 - £500	£100,000 - £155,000
Regulatory fines and compensation payments	£150 - £300	£70,000 - £100,000
Lost assets (including lost intellectual property)	£6,500 - £14,000	£275,000 - £375,000
Damage to reputation	£3,000 - £16,000	£80,000 - £310,000
Total cost of worst incident on average	£75,200 - £310,800	£1,455,000 - £3,140,000
2014 comparative	£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

To gain further insight how breaches are affecting organisations, the survey explored the individual activities and categories which made up the total cost.

The survey did find the largest component of the total amount was 'Business disruption', which cost small organisations in the range of £40,000 to £225,000, and larger organisations a minimum of £800,000 and extended as far as £2.1 million.

The costs involved in 'Lost assets and lost intellectual property' made up the second largest category, despite the challenges in valuing intellectual property. For large organisations, the average costs range from £275,000 to £375,000; and small organisations £6,500 and £14,000.

The survey also identified that nearly one in 10 large organisations spent more than £500,000 on regulatory fines and compensation payments, whereas no small organisations reported spending more than £999 on this outlay.

Confidential information worth more than £500,000 was stolen by a staff member of IT from a large utilities business. This seriously affected business operations and resulted in reputational damage. It took between a week and a month to restore business operations, cost £100,000 to £249,999 to respond to the incident and also resulted in revenue loss of between £100,000 to £249,999.

Turning to the 'Lost business' category, small organisations seem to be disproportionately affected by their single worst breach. For these organisations, the estimated loss ranged from £25,000 to £45,000; whereas the upper limit for large organisations was £170,000 – still a significant amount but much less than the cost of a 'Business disruption'. One possible reason for this could be that even though large organisations suffer loss of business in the event of a breach, their continuity and resilience procedures are sufficiently more mature to enable the business to continue to fulfil new orders and sales. Small organisations on the other hand may not have the same resilience, meaning that any breach is more likely to impact sales and be more visible to customers than compared to larger organisations.

The costs on large and small organisations due to security incidents continue to increase year on year – and it's not just the loss of potential sales which are impacting organisations.

One third of the large organisations who responded to the question reported that they spent more than £500,000 in the recovery of lost assets and intellectual property. Eleven percent of organisations changed the nature of business carried out following the worst single incident – the same percentage as in 2014. Given this, it remains unclear the role recovery costs and loss of intellectual property play in the remediation of the worst breach and subsequent decision to change the nature of the business carried out.

Due to a missed patch update, a large financial services firm with UK operations suffered a website breach which resulted in the attacker being able to take control of particular systems. As a consequence of the breach, not only did the firm suffer reputational damage, but it lost more than £500,000 in revenue and spent between £250,000 and £499,999 responding to the incident. It took more than a month to restore its operations back to normal.

2.5 Responding to security incidents

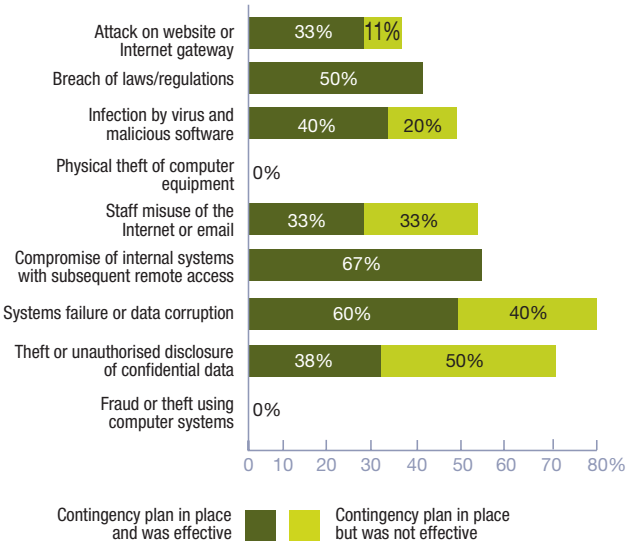
The survey examined the types of incidents that organisations plan for, and assesses the effectiveness of the planning.

The survey found only two scenarios where contingency plans proved to be effective for more than 50% of the respondents – 'Compromise of internal systems with subsequent remote access', and 'Systems failure or data corruption'. For the other scenarios tested in the survey, which included 'Attacks of websites or gateways', 'Infection by malicious software', and 'Staff misuse of the internet' – the survey recorded that plans were not in place or not effective for the majority of respondents.

The survey asked what other measures respondents put in place following the single worst breach. Half of all organisations invested in more security training, broadly in line with the 2014 figure of 54%. Thirteen percent of organisations conducted additional vetting of staff or contractors, an increase from last year's figure of 9%, indicating a realisation that staff are usually at the centre of an information security breach.

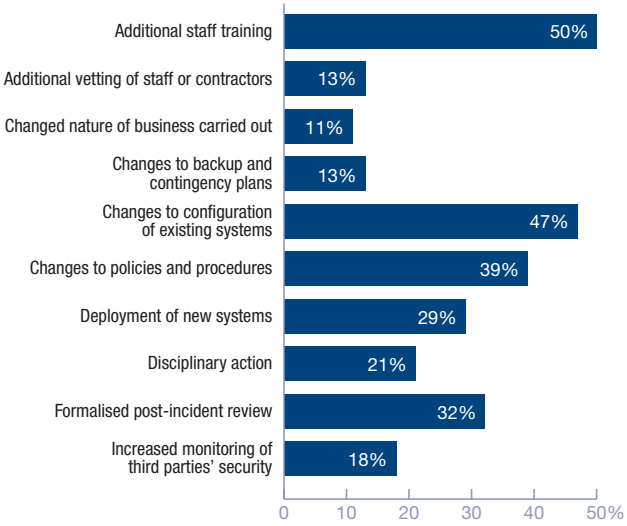
What type of security incidents do organisations plan for; and how effective are these contingency plans?

(Based on 35 responses)



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

(Based on 38 responses)



Thirty-nine percent of organisations made a change to their policies and procedures after they suffered their worst security breach – a noticeable decrease from 46% in 2014. This indicates that businesses increasingly understand that policies on their own are not an effective tool to stopping information security breaches and should be accompanied with a series of other tools and activities to protect the organisation.

The survey found that just one-third of organisations conducted a formal post-incident review following the single worst breach. It is concerning that two-thirds of organisations have not taken the time to assess what happened, understand the causes and implement measures which would prevent breaches from recurring. Failure to perform a review and learn the lessons will most likely increase the chance of a recurrence.

32%

of respondents carried out a formalised post-incident review.

3 ATTITUDES AND TRENDS

3.1 What is driving information security expenditure?

For the second year running, 'Protecting customer information' is the single largest driver for information security expenditure with 34% of respondents selecting this response. This represents a 9% year on year increase from the 2014 survey, indicating the priority this is taking in organisations.

The second highest driver was 'Protecting the organisation's reputation' at 21%. This is a significant increase from last year, with a 50% year on year increase.

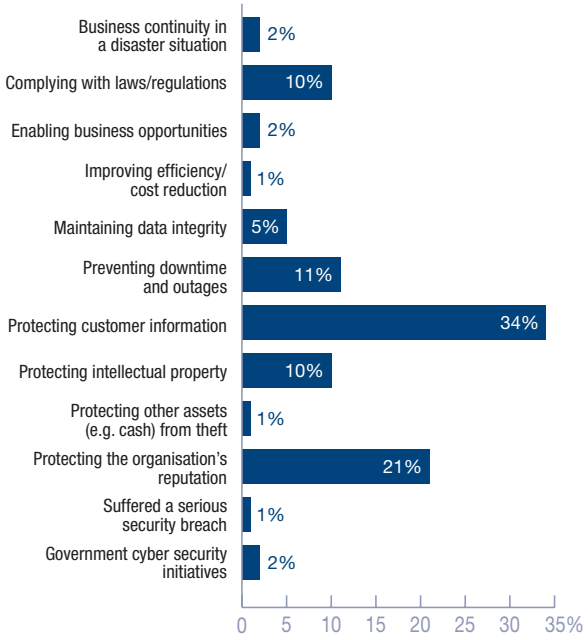
Combining both expenditure drivers, they account for over half (55%) of all the responses to this question. 'Efficiency improvements', 'Maintaining intellectual property' and 'Complying with laws and regulations' all scored 10% or lower.

Recent data breaches demonstrate that disclosure of customer and personal information can have implications on share prices and personal careers. For those organisations who suffered a breach in the past year, 41% felt that the greatest impact suffered was to their reputation – nearly twice as high as the next largest impact, which was to actual business operations (23%).

Looking at the other drivers of expenditure which all scored lower than the responses above, namely 'Business continuity in a disaster situation', 'Complying with laws and regulations' and 'Improving efficiency/ cost reduction', all fell in 2015 compared to the previous year. Whilst these remain important issues for organisations, it seems that the public's reaction to poor management of customer data is now the main concern of budget holders and is driving spending accordingly.

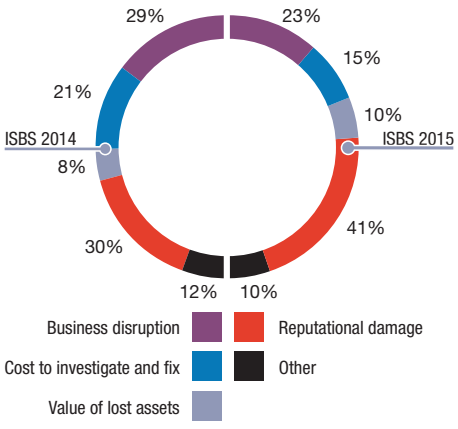
What is the main driver for information security expenditure?

(Based on 310 responses)



What made this incident the worst of the year?

(Based on 39 responses)



A large government organisation in the north west of England suffered a sensitive data disclosure breach when a member of staff accidentally sent sensitive information to the wrong e-mail address. This had a serious impact on the organisation and resulted in reputational damage.

Inappropriate staff behaviour at a large financial services firm led to unauthorised disclosure of confidential information. It took between a week and a month to restore the business back to normal. Following the breach, the firm conducted additional staff training to address the security issues identified.

3.2 The changing patterns of security expenditure

Levels of expenditure

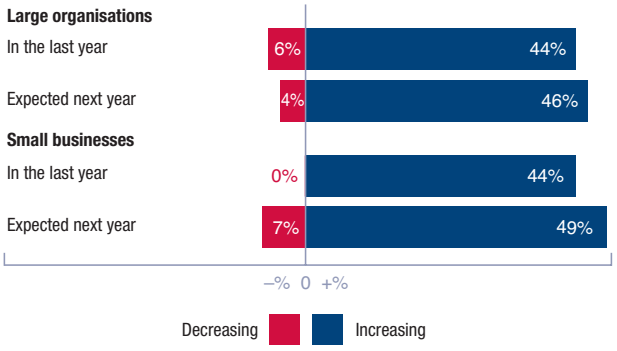
The survey found a difference in levels of security spending between the respondents. Forty-four percent of large organisations increased their information security expenditure; whereas in 2014, 53% of firms increased expenditure.

Looking to the future, 46% of large firms expected information security expenditure to increase in the coming year, which is lower than the last year's figure of 51%.

Small organisations reported a different outlook: 44% increased their information security expenditure, up from 2014 (27%). Only 7% of small organisations expected information security expenditure to increase in the coming year, which is significantly down from the previous year's 42%.

How is information security expenditure changing?

(Based on 241 responses)



Outsourcing expenditure

The survey also found that levels of outsourcing to external providers continue to rise. Business processes; such as corporate email, corporate website maintenance, finance and accounting, and payroll processing have all increased over the last two years. However, there was a marked decrease in the outsourcing of 'Payment processing' (down 70% year on year) and a shorter fall in the percentage of firms outsourcing their sales and marketing function.

Use of outsourced cloud data storage has increased from one-in-five in 2013, to nearly one-in-three this year.

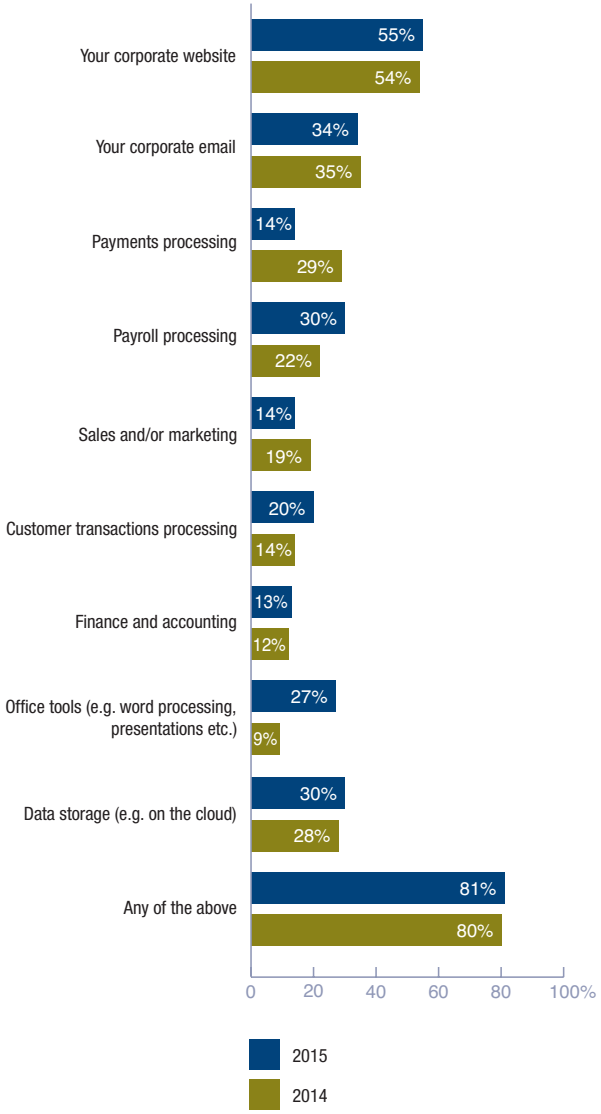
As use of cloud storage and cloud computing resources, such as desktop environments and productivity tools continues to rise, organisations should consider whether current policies, procedures, technology and training are updated in line with its use. Security standards for 'the cloud' are maturing, so all organisations should explore what needs to be implemented to ensure that they have the appropriate levels of controls in place.

Given the dramatic increase in costs to organisations suffering a breach, as explored in Section 2, it is notable there has not been a similar increase in security expenditure. Similarly, there is a question as to why the slight increase in investment has not hampered the frequency or cost of incidents.

Are the days of ever increasing security spending at an end? With the rates of information security expenditure slowing, do organisations now understand their risk appetite and having covered their regulatory and legal requirements, are they now taking a more risk based approach to their spending?

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

(Based on 319 responses)



3.3 Where do organisations go for advice and assurance?

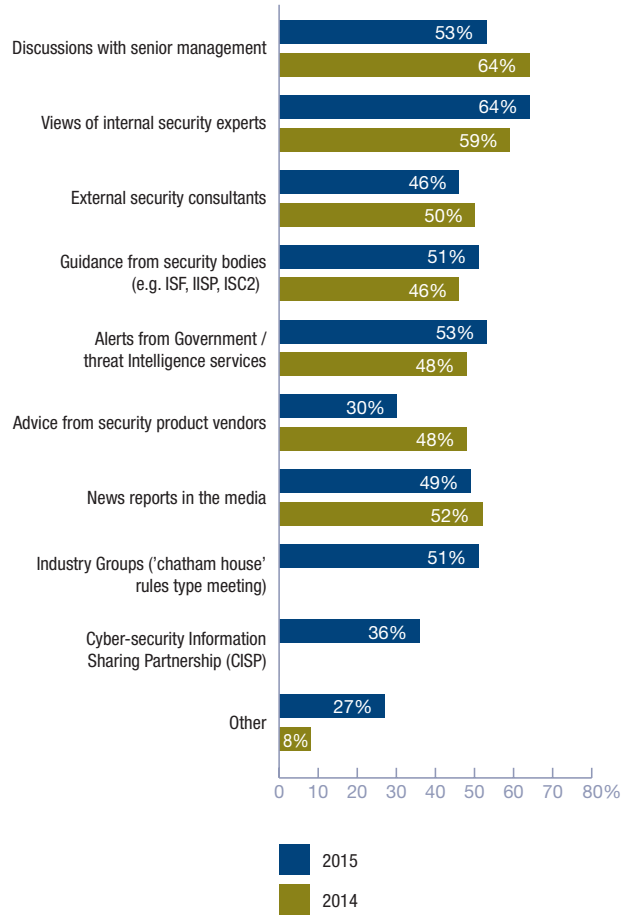
The percentage of organisations using the HM Government's Ten Steps to Cyber Security guidance increased from just over a quarter (26%) in 2014 to almost one third (32%) in 2015. There was also an 11% year on year increase in organisations using government alerts to inform their awareness of threats and similar vulnerabilities.

The survey also reports that nearly half (49%) of organisations are either badged to the HM Government's Cyber Essentials and Cyber Essentials Plus schemes, are on their way to accreditation or plan to be badged in the next year.

There was also an 11% year on year increase in organisations using other recognised advisory bodies - such as the Information Security Forum, (ISC)², and the Institute for Information Security Professionals, for threat evaluation source material. In contrast there has been a reduction (from 48% in 2014 to 30% in 2015) in organisations taking threat evaluation advice from security product vendors.

What information do you use to help you evaluate the security threats that your organisation faces?

(Based on 313 responses)

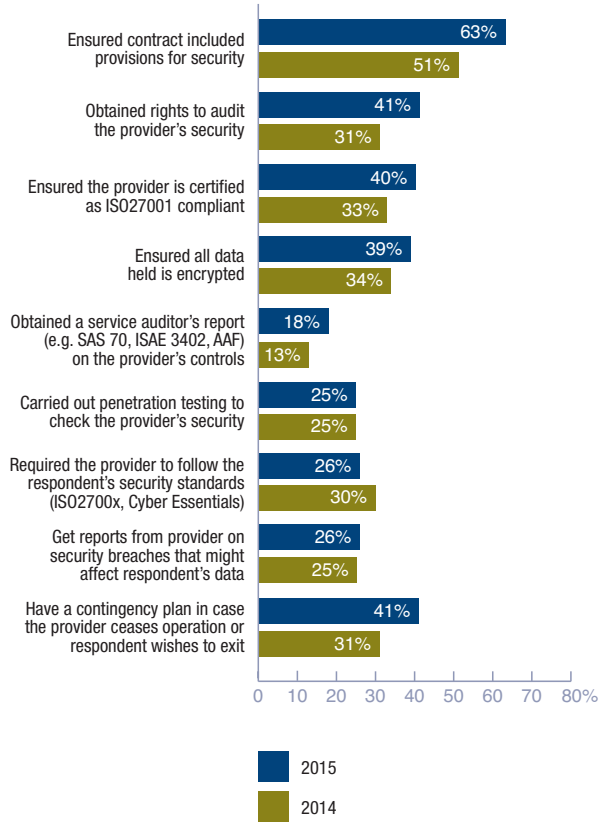


The percentage of organisations which have implemented ISO 27001 – the international standard for Information Security Management Systems – has not changed in any great degree since 2013. However, ISO 27001 remains something which the respondents value, particularly in trying to gain assurance over their supply chain. Forty percent of organisations ensure that a provider of services has ISO

27001 certification when contracting for services. This is a year on year rise of over 20% compared to 2014, indicating that the Standard is increasingly recognised as one method of measuring the level of information security management and maturity in the supply chain.

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

(Based on 273 responses)

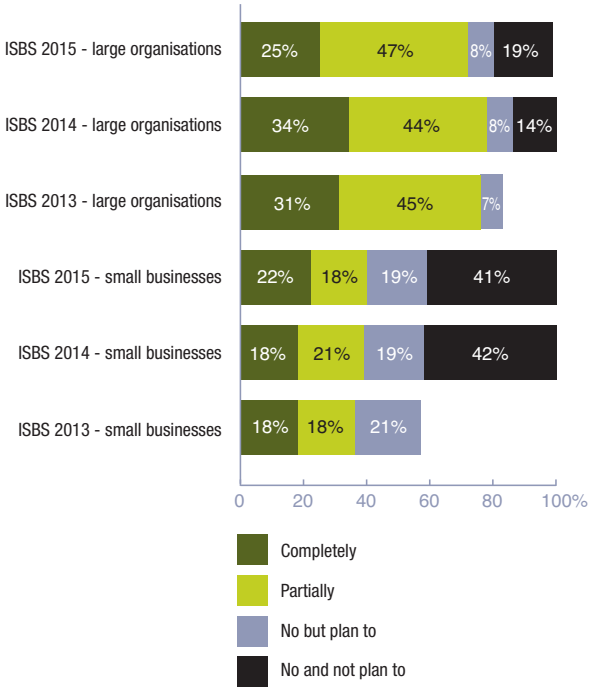


There are three main themes to come out of these set of statistics. The first concerns the role of government in driving information security awareness, setting standards and the tone nationally. The 23% year on year increase in organisations using the Ten Steps to Cyber Security is noticeable and supports the view that clear, accessible and independent guidance is valued by organisations, and suggests that organisations are referring to the government for a common set of cyber security processes and procedures.

Secondly, internal security experts are now more likely to be involved, with 64% of organisations reporting that these individuals would be consulted for threat evaluation – a figure up by 8% over last year.

How many respondents implemented ISO 27001?

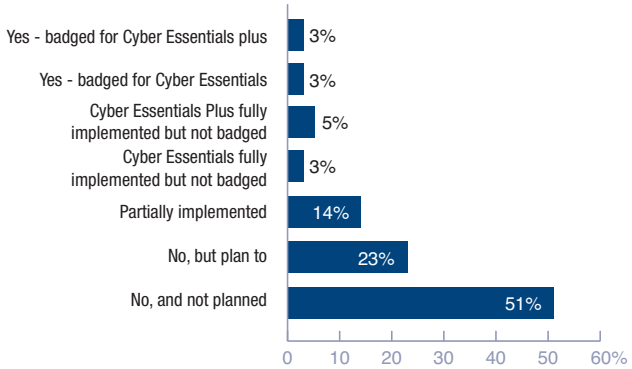
(Based on 142 responses for large and 83 responses for small)



Lastly, the growth in the use of ISO 270001 in the supply chain indicates that the Standard is increasingly recognised as one method of measuring the level of information security management in and maturity of the supply chain; we may see increasing adoption levels for the Standard due to this trend.

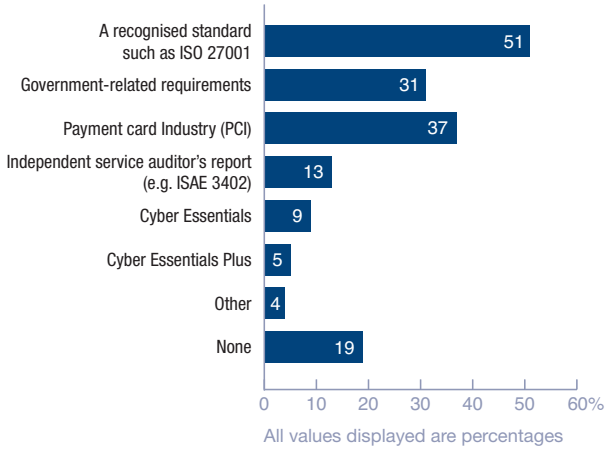
Has your organisation implemented Cyber Essentials and Cyber Essentials plus?

(Based on 256 responses)



Which standards and good practice guides do you ensure your suppliers comply with?

(Based on 304 responses)



A large educational organisation in the south east of England suffered the potential loss of unprotected IP as a result of a successful spear-phishing attack by international attackers. It took more than a month to restore business operations back to normal. Although overall this had a minor impact on business operations, the cost to investigate and resolve the incident made it the organisation's worst breach of the year. The organisation was made aware of this breach by a government organisation.

3.4 Is Cyber insurance properly understood?

One third of the survey respondents believe that they have insurance which would cover them in the event of an information security breach; 39% of large organisations and 27% of smaller organisations. These numbers are lower in 2015 than last year, when the respective percentages were 52% and 35%.

For the organisations who claimed to have coverage, the majority believe that their existing insurance policies would cover their costs in the event of a breach, with a corresponding minority stating that they had purchased a specific Cyber insurance policy.

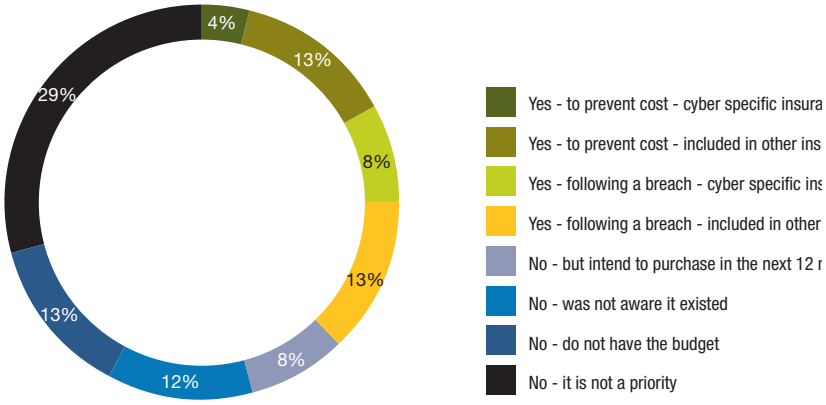
Of the organisations which have not purchased insurance, 12% were intending to purchase a policy in the next year, 47% felt that it was not a priority and 19% were not even aware of the existence of such coverage.

There has been a notable drop in the percentage of organisations who have claimed to have cover. Cyber liability insurance cover has been available in the market for around 10 years, and is mostly used as a risk transfer mechanism in countries that have mandatory data breach notification laws. As such notification is not mandatory in the UK, it is understandable that the uptake level is not as high as other territories, such as the United States, where the vast majority of states have mandatory notification of some form.

That said, the impending revision of EU Data Protection Regulation is expected to include mandatory notification of breaches

Do you have insurance which would cover you in the event of a breach?

(Based on 212 responses)



of personal data, and this may well be the catalyst to change the cyber liability insurance landscape in the UK.

> A medium sized transportation company based in the south west of England had a repeat incident where the phone system was hacked and a series of international premium rate calls were made. As this happened over a weekend the company did not identify the breach until the following Monday morning. As a result of the breach, all premium and international calls were barred from the system. This hindered staff communication to Europe leading to lost revenue of between £1000 and £10,000, making the breach the company's worst. The company was not aware that insurance existed that would cover them in an event of a breach.

One view of the decline in both large and small organisations reporting having insurance is that, having reviewed their policy details, these organisations have discovered that they are not as well covered as previously thought or that insurers have taken steps to exclude cyber liability from general insurance policies. In a nascent market, the terms and coverage of insurance policies vary tremendously; in turn, due to understandable caution, this may be preventing a larger uptake of policies than would otherwise be expected. This slow growth may be compounded by a lack of historical data, which makes it harder for insurers to price cyber risk accurately.

The 2015 joint HM Government and Marsh report 'UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk' found that businesses are overestimating the extent to which their existing insurance provides cover for cyber risk, reinforcing this analysis. The report also highlights the role that insurance can play as part of a company's wider risk management approach.

39% of large organisations

27% of small businesses

have insurance that would cover them in the event of a breach.

▼ Down from 52% a year ago.
▼ Down from 35% a year ago.

4 ASSURANCE AND EFFECTIVENESS

4.1 Mobile devices – risk awareness and policy

This year's survey reports that 15% of organisations suffered from a breach caused by use of a smartphone or tablet device, more than doubling last year's figure of 7%.

The survey also identified that organisations are starting to use a series of measures to address the management of these devices. Roughly half of all large organisations have either defined a strategy for mobile usage (52%), are protecting corporate emails (48%) or are using something for the remote management of devices (49%). Furthermore, 70% of large organisations have issued a policy to cover how these devices should be used.

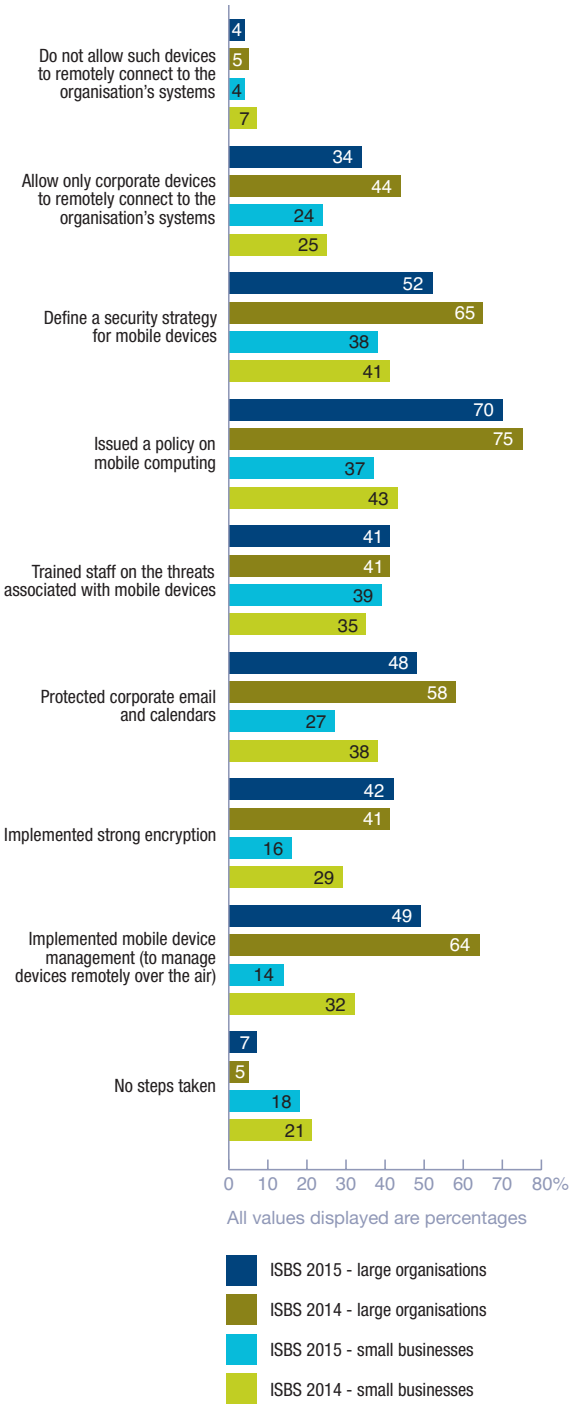
15% of large organisations had a security or data breach in the last year involving smartphones or tablets.

3% of worst breaches were due to portable media bypassing defences.

Equivalent statistics for small organisations show they have further to go, with 38% defining a strategy, 27% protecting corporate email and 14% using remote device management; only 37% have issued a security policy covering smart phone and tablet use.

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

(Based on 138 responses for large and 93 responses for small)



For many years, organisations have understood the information security risks of smartphone use, but the benefits and the cost savings of 'Bring Your Own Device' (BYOD) have outweighed the security concerns for most. This is demonstrated by the fact that only 4% of both large and small organisations put a complete ban on mobile devices connecting to their corporate networks. Furthermore, there is a marked decline in the percentage of firms who only allow corporate devices to connect to the network (from 44% in 2014 to 34% in 2015).

Evidence from the survey demonstrates that organisations are beginning to manage the risks presented by these devices, but we must not be complacent: one in five small organisations (18%) still have not taken any steps with the use of smartphones or tablets, even though the number of breaches through mobile devices more than doubled. HM Government has issued guidance on Bring Your Own Device, which may help firms minimise the risk while maximising the business benefits.

32% of respondents haven't carried out any form of security risk assessment.

60% of respondents are confident they have sufficient security skills to manage their risks next year.

26% of respondents don't evaluate how effective their security expenditure is.

4.2 How effective is security policy?

The Information Security Breaches Survey indicates that 98% of large organisations and 60% of small organisations have a documented information security policy; these figures remain consistent with the previous year. In addition, 46% of all respondents have a formal cyber security policy in place (no comparable figure for 2014).

Having a policy does not mean that an organisation is completely protected against breaches. Of all the organisations where security policy was poorly understood, 72% experienced a staff-related breach, a slight increase on the previous year's figure of 70%.

Fifty-six percent of organisations where security policy is understood still had a breach; this is concerning but is approximately a third lower than those organisations where security policy was not clear. As a further point, there is a noticeable year on year increase of 37% of staff-related breaches in organisations where security policy was meant to be understood.

8% of IT budget is spent on average on security.

▼ Down from 10% a year ago.

What cyber security governance and risk management arrangements do you have in place?

(Based on 308 responses)

44% of large organisations

44% of small businesses

increased information security spend in the last year.

▼ Down from 53% a year ago.
▲ Up from 27% a year ago.

49% of respondents badged Cyber Essentials or Cyber Essentials Plus, on their way to accreditation or plan to be badged.

Whilst having a policy is important in setting out an organisation's objectives in information and cyber security, there are clear benefits in making sure that it is understood and implemented accordingly.

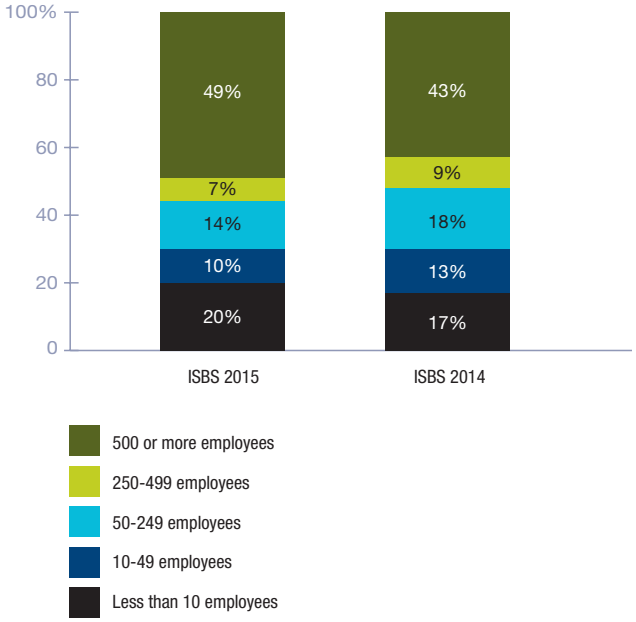
As a final point, it is notable that there has been a lack of progress amongst small organisations in developing information security policies. Since 2012, there has been little change in the percentage of small organisations who have formally documented an information security policy but the trend in those organisations suffering a breach has increased over this same time.

> A large London based travel firm had its control systems infected with malicious software. It required a large amount of work and took over a month to recover from the incident, resulting in significant costs to the business. Consequently, the company made changes to their policy and procedures to overcome the security issue identified.

5 APPENDIX

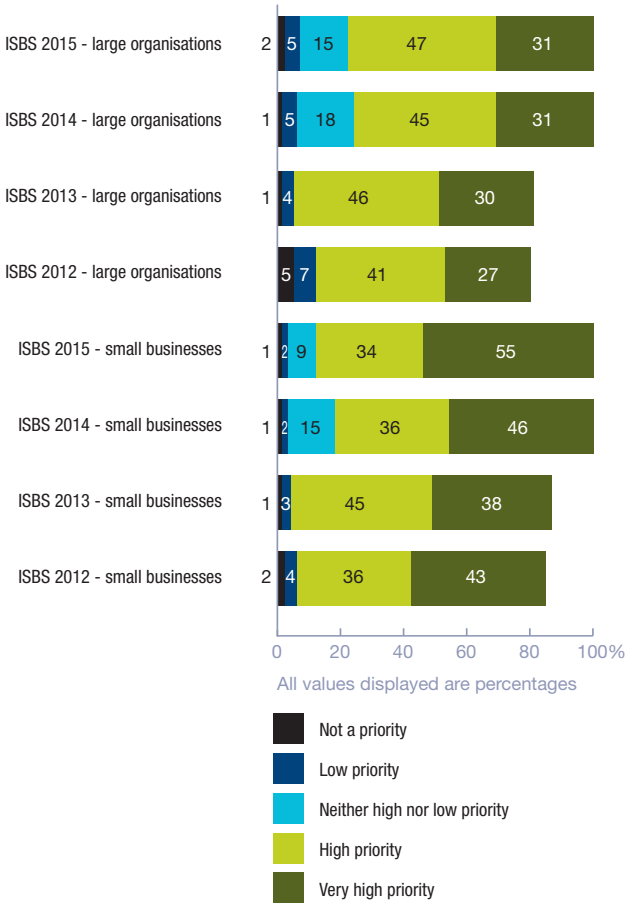
How many staff did each respondent employ in the UK?

Figure 1 *(based on 661 responses)*



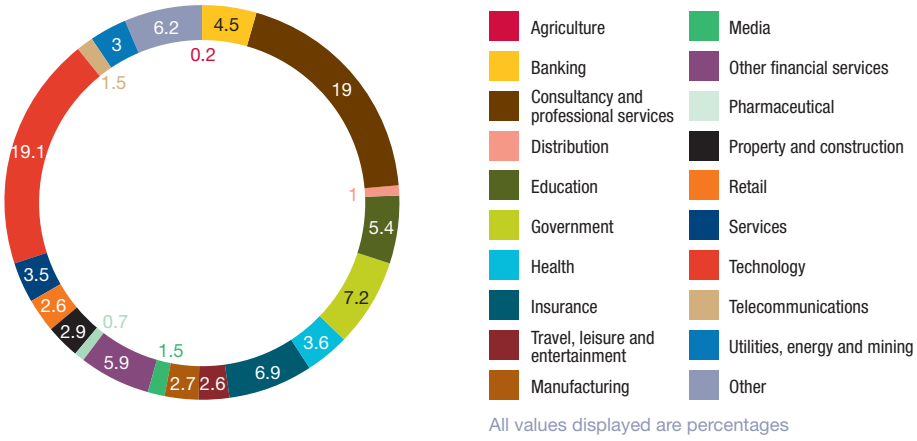
How high a priority is information security to top management or director groups?

Figure 3 *(based on 314 responses for large and 200 responses for small)*



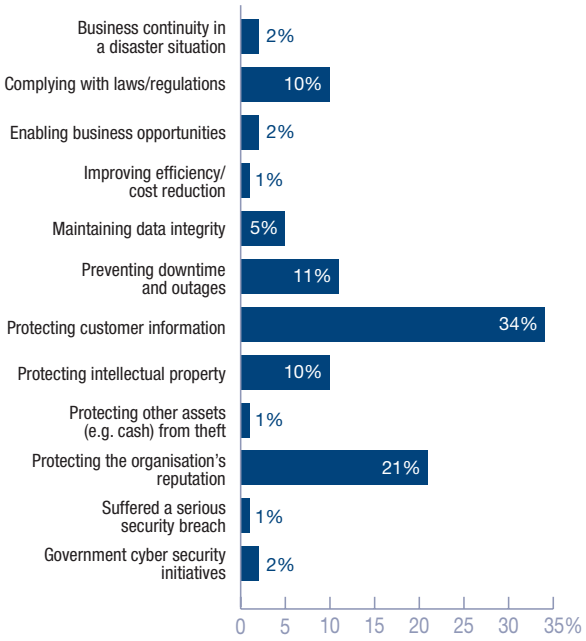
In what sector was each respondent's main business activity?

Figure 2 *(based on 664 responses)*



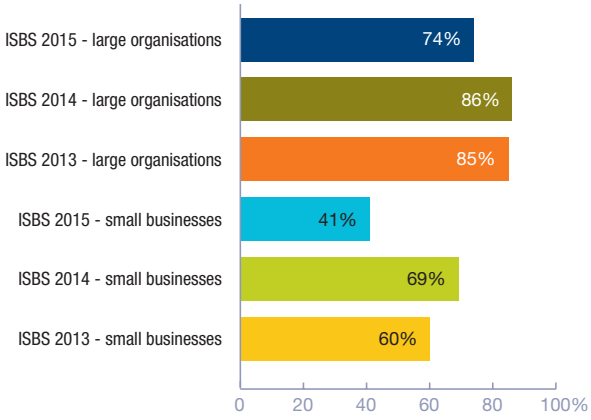
What is the main driver for information security expenditure?

Figure 4 *(based on 310 responses)*



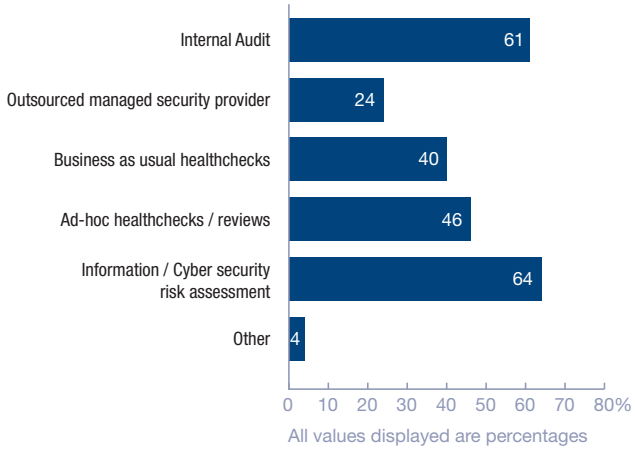
How many respondents carry out security risk assessments?

Figure 5 *(based on 166 responses for large and 90 responses for small)*



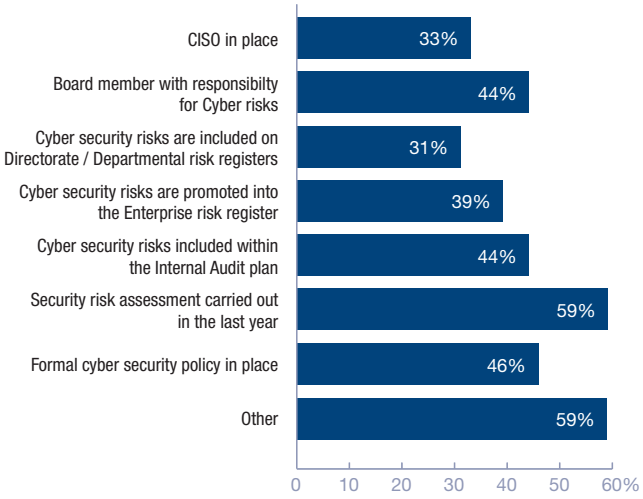
How are cyber security risks identified and assured?

Figure 5.1 *(based on 317 responses)*



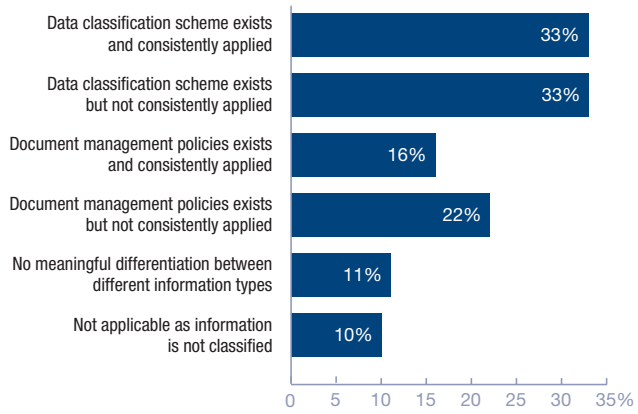
What cyber security governance and risk management arrangements do you have in place?

Figure 5.2 *(based on 308 responses)*



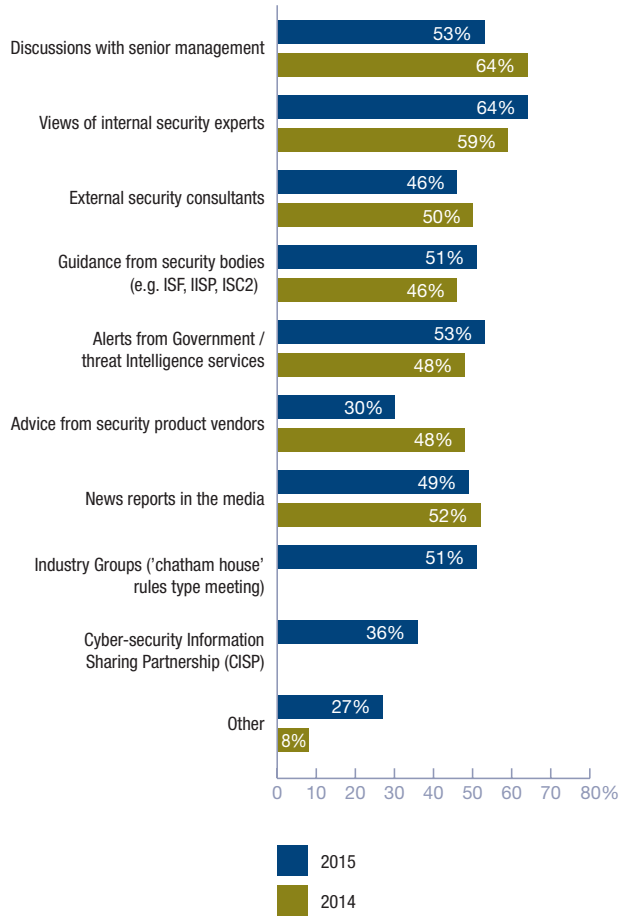
How is information classified within your organisation and is it consistently applied?

Figure 5.3 *(based on 309 responses)*



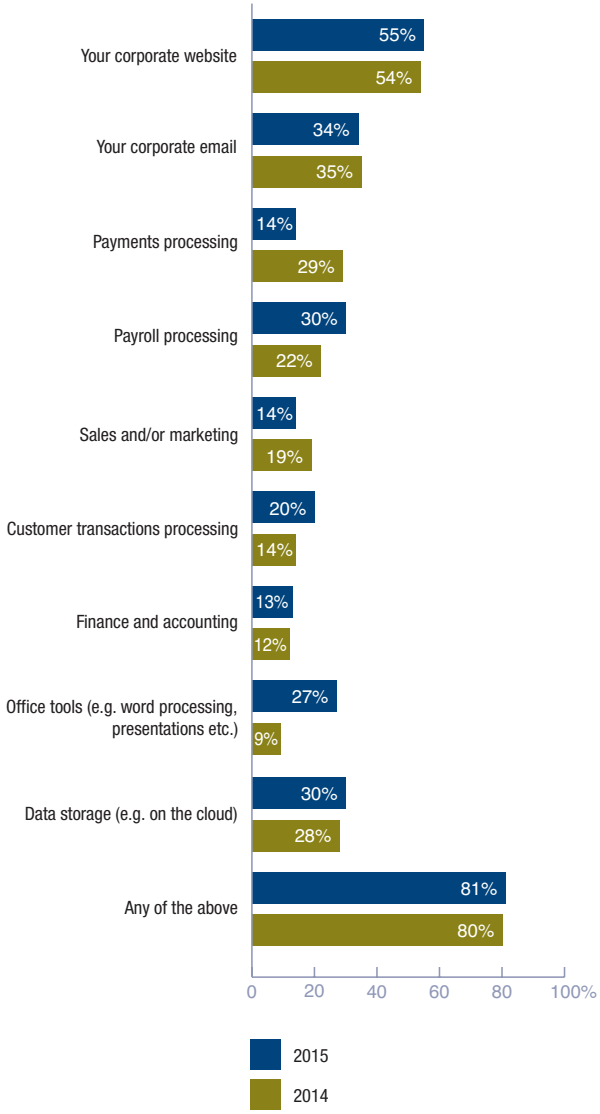
What information do you use to help you evaluate the security threats that your organisation faces?

Figure 5.4 *(based on 313 responses)*



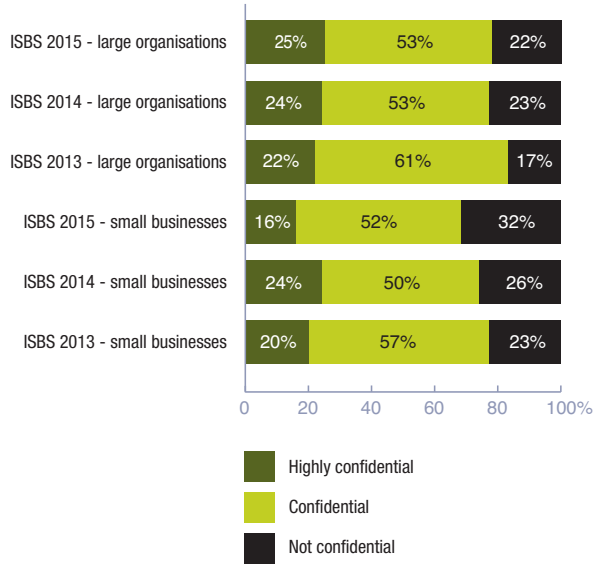
Which business processes have respondents outsourced to external providers over the Internet?

Figure 6 *(based on 319 responses)*



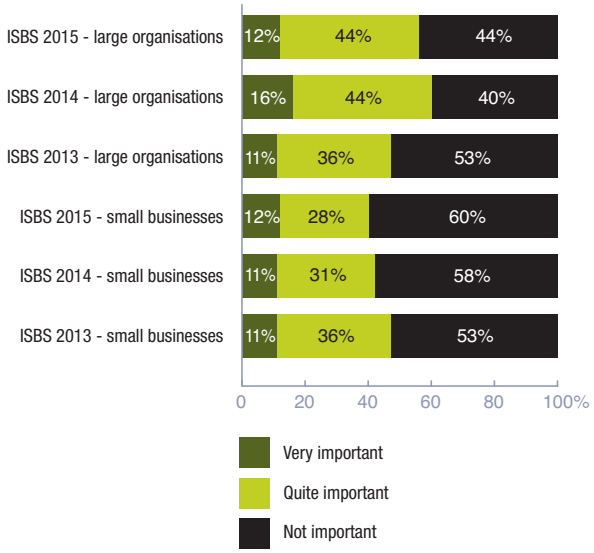
How confidential is the data that respondents store on the Internet?

Figure 7 *(based on 122 responses for large and 81 responses for small)*



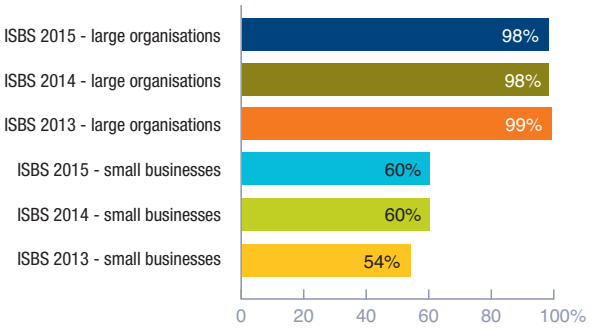
How important is the use of social networking sites to the organisation?

Figure 8 *(based on 135 responses for large and 90 responses for small)*



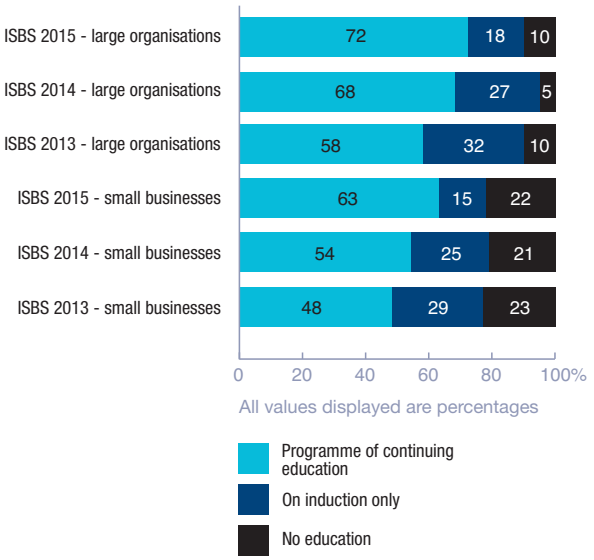
How many respondents have a formally documented information security policy?

Figure 9 *(based on 153 responses for large and 87 responses for small))*



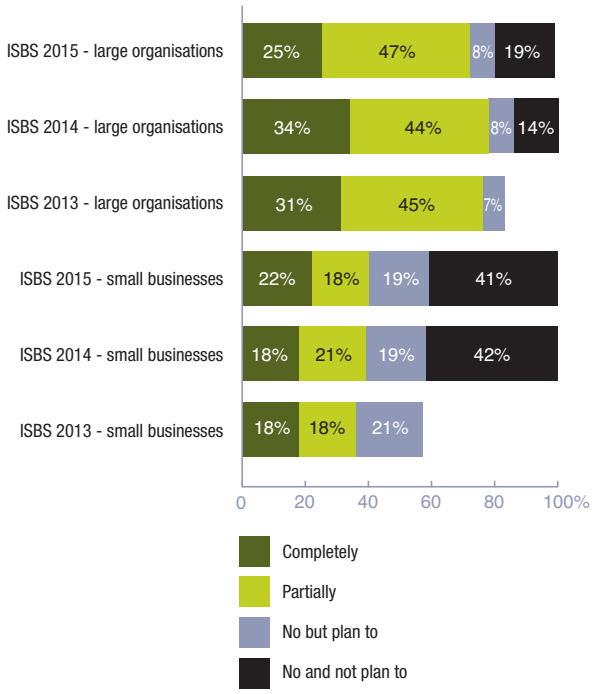
How do respondents ensure staff are aware of security threats?

Figure 10 *(based on 152 responses for large and 87 responses for small)*



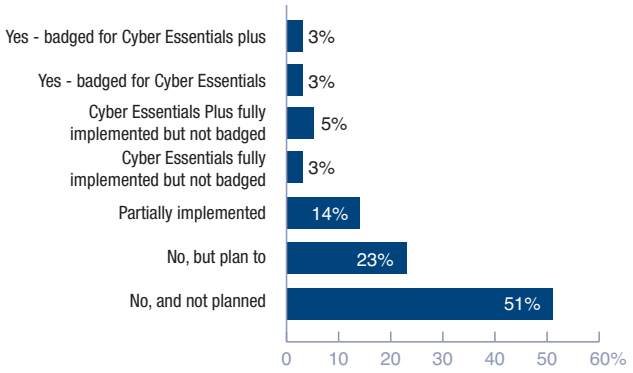
How many respondents implemented ISO 27001?

Figure 11 *(based on 142 responses for large and 83 responses for small)*



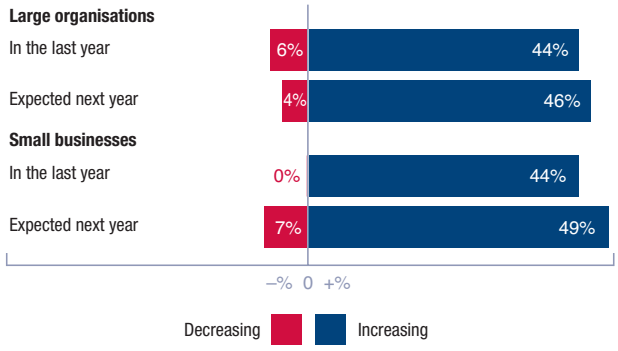
Has your organisation implemented Cyber Essentials and Cyber Essentials plus?

Figure 11.1 *(based on 256 responses)*



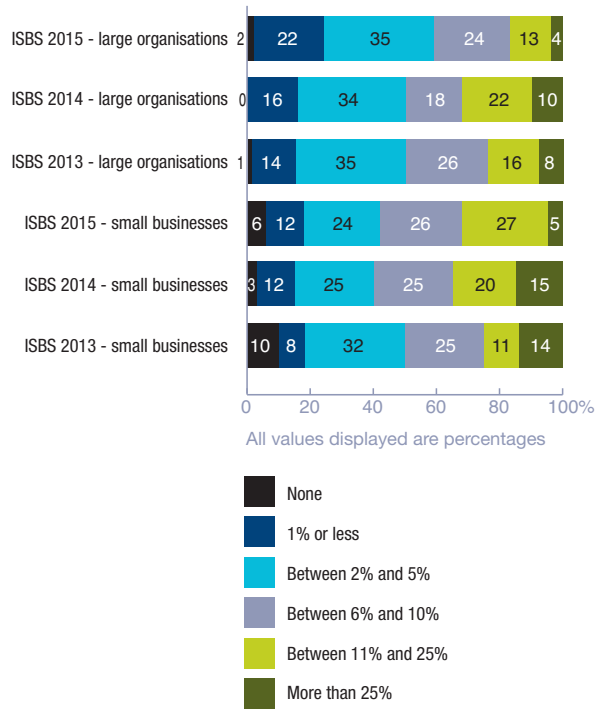
How is information security expenditure changing?

Figure 12 *(based on 241 responses)*



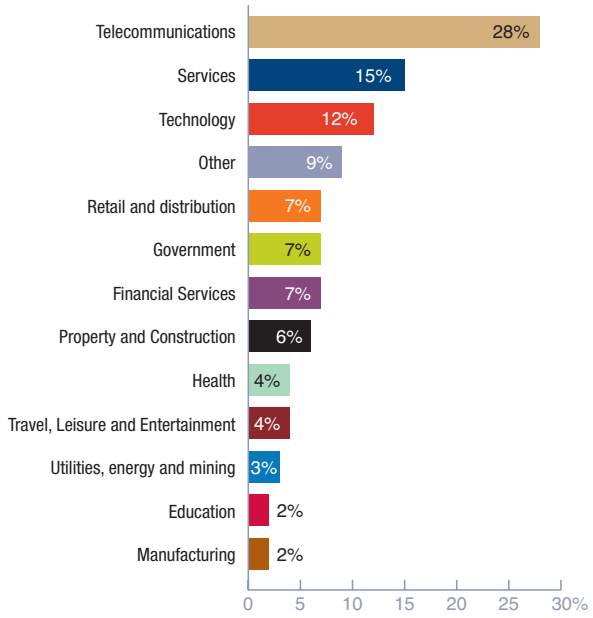
What percentage of IT budget was spent on information security, if any?

Figure 13 *(based on 205 responses for large and 172 responses for small)*



Which sectors spend most on security?

Figure 14 *(based on 241 responses)*

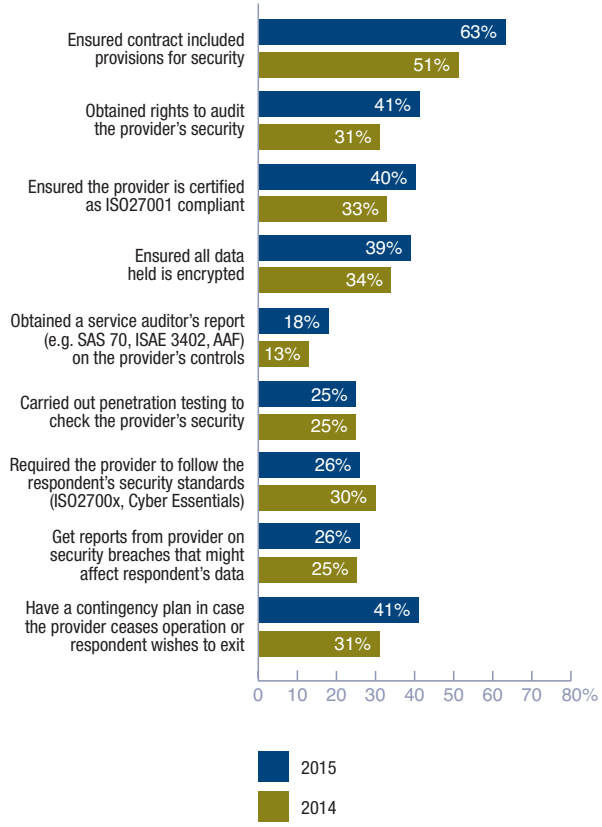


How do respondents measure the effectiveness of their security expenditure?

Figure 15 *(based on 128 responses for large and 86 responses for small)*

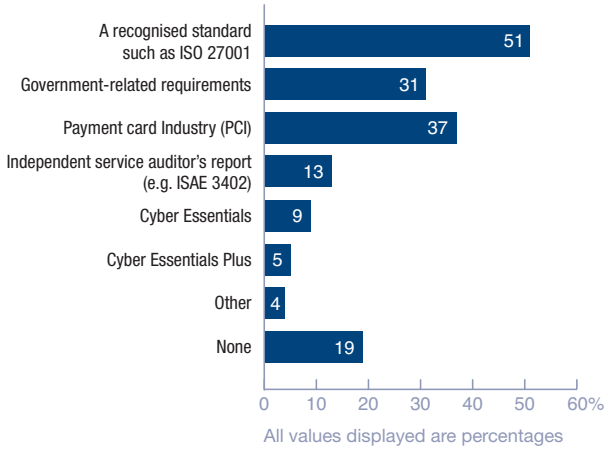
What steps have respondents that use externally hosted services taken to obtain comfort over the external provider's security?

Figure 16 *(based on 273 responses)*



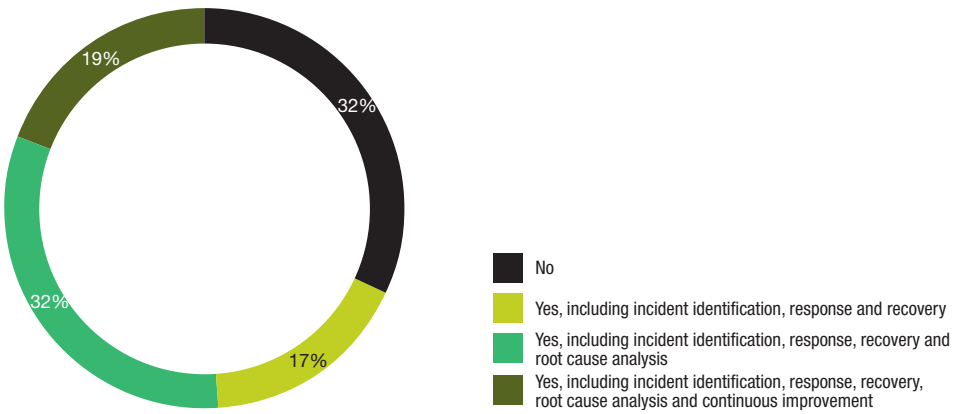
Which standards and good practice guides do you ensure your suppliers comply with?

Figure 16.1 *(based on 304 responses)*



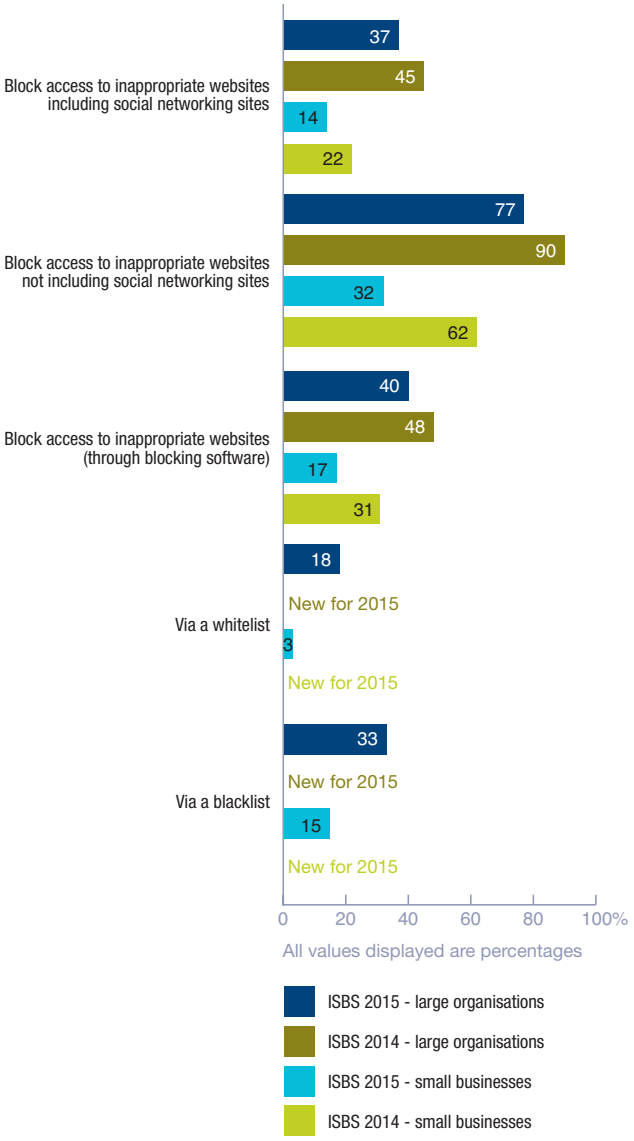
Do you have a formal incident management process?

Figure 16.2 *(based on 293 responses)*



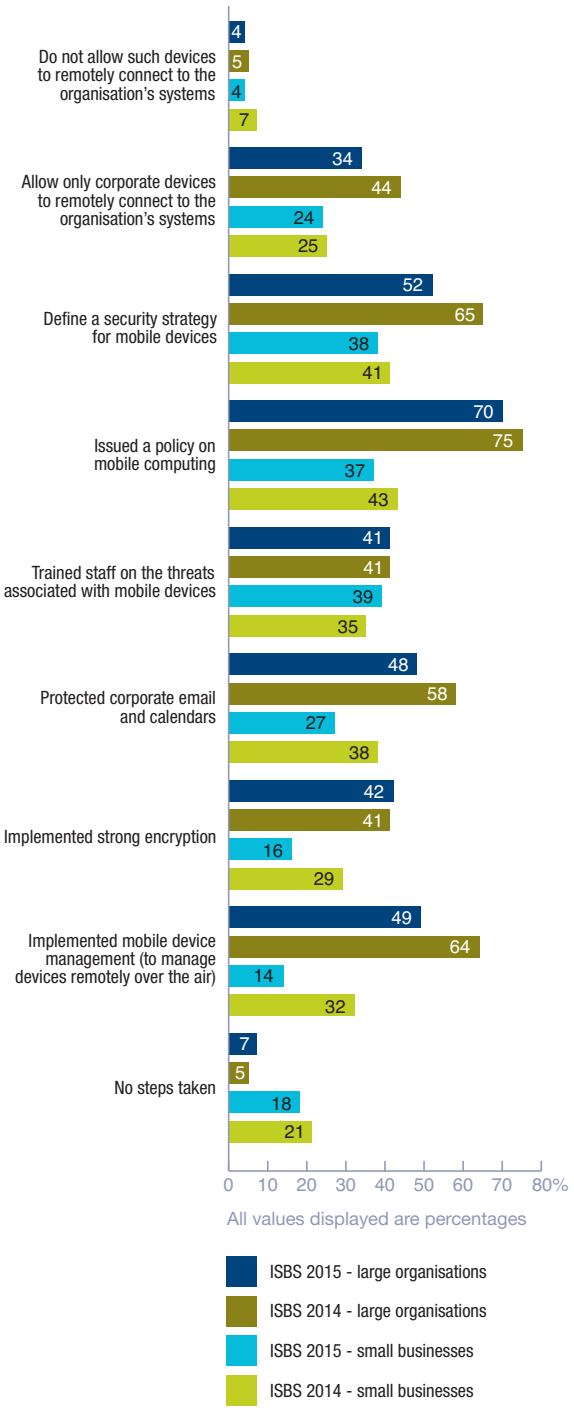
How do respondents prevent staff misuse of the web and social networking sites?

Figure 17 *(based on 147 responses for large and 98 responses for small)*



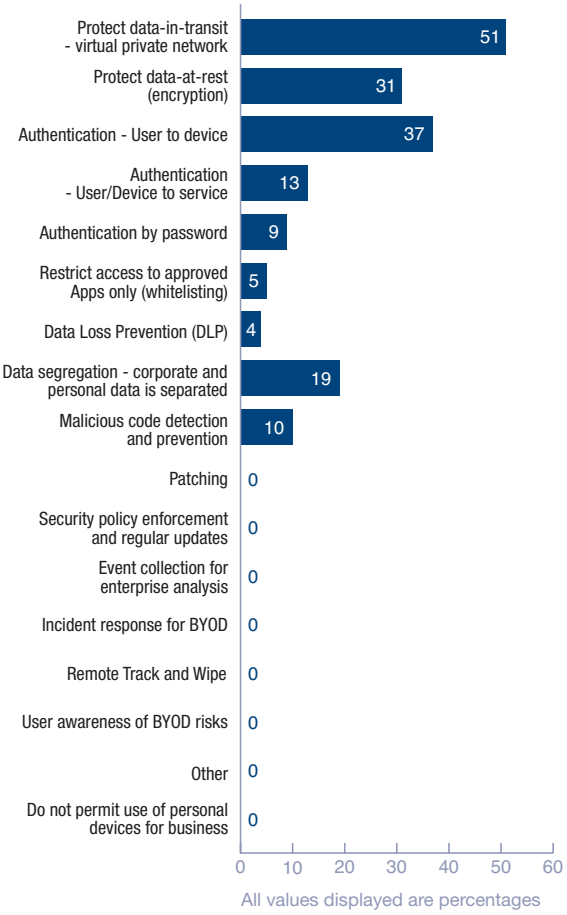
What steps have respondents taken to mitigate the risks associated with staff using smartphones or tablets?

Figure 18 *(based on 138 responses for large and 93 responses for small)*



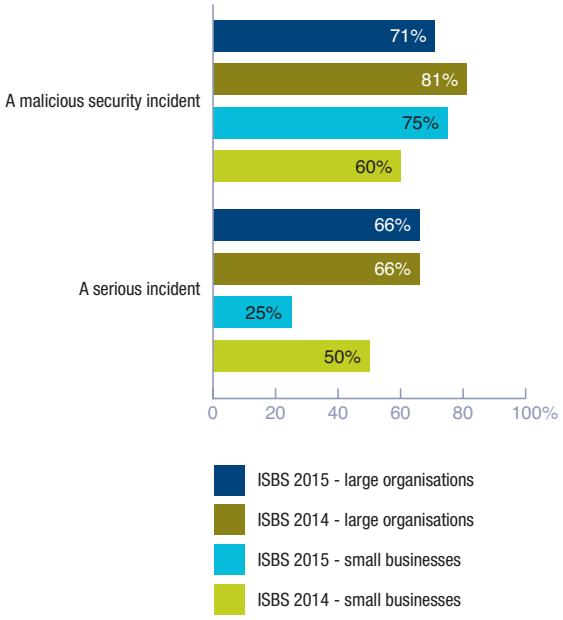
What type of security controls do you use to manage the risks of BYOD?

Figure 18.1 *(based on 304 responses)*



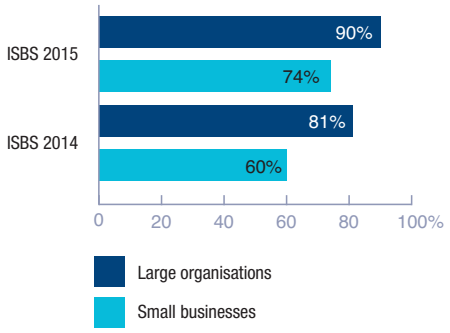
In the last year, how many respondents had...

Figure 19 *(based on 177 responses for large and 76 responses for small)*



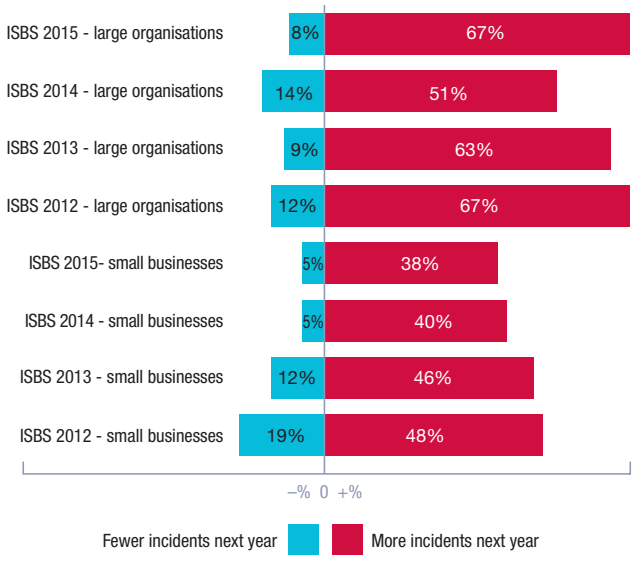
How many respondents had any form of security breach in the last year?

Figure 20 *(based on 256 responses)*



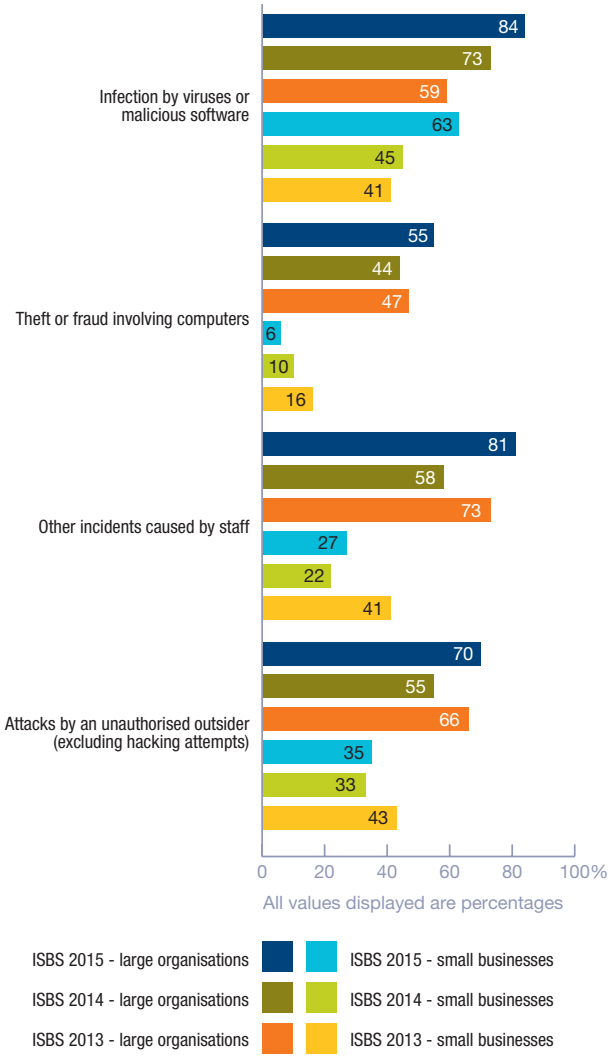
What do respondents expect in the future regarding number of incidents?

Figure 21 *(based on 141 responses)*



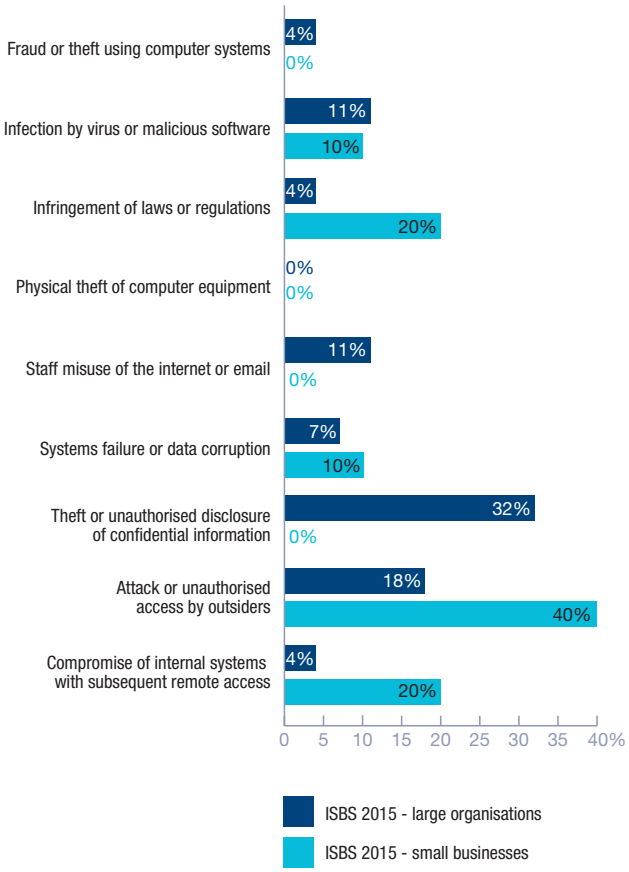
What type of breaches did respondents suffer?

Figure 22 *(based on 584 responses for large and 355 responses for small)*



What was the worst security incident faced by respondents?

Figure 24 *(based on 28 responses for large and 10 responses for small)*



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

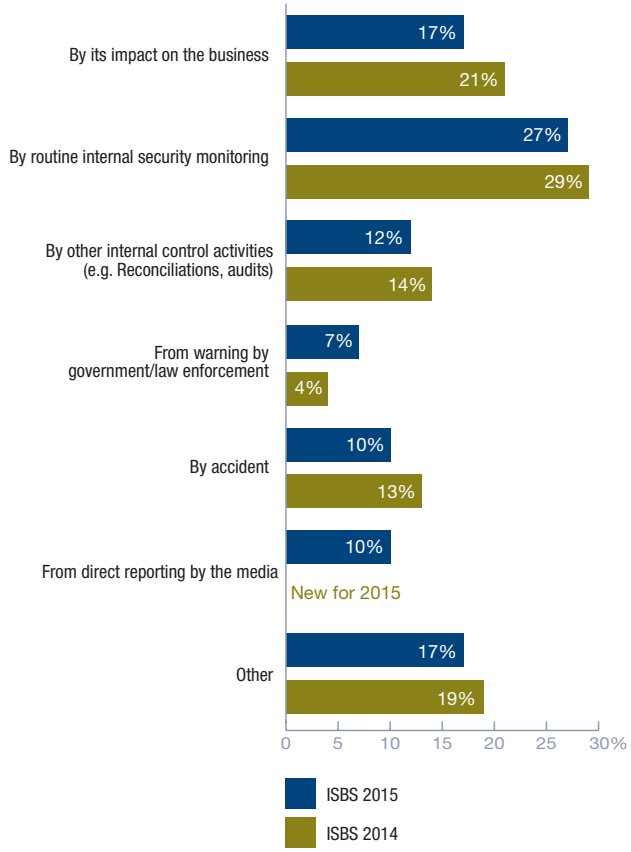
Figure 23 *(based on 316 responses)*

	Large organisations	Small businesses
Infection by viruses or other malicious software	3 (5)	2 (3)
Theft or fraud involving computers	2 (3)	2 (1)
Other incidents caused by staff	6 (6)	2 (3)
Attacks by an unauthorised outsider (excluding hacking attempts)	6 (11)	3 (5)
Any security incidents	14 (16)	4 (6)

Equivalent comparative statistics from ISBS 2014 are shown in brackets

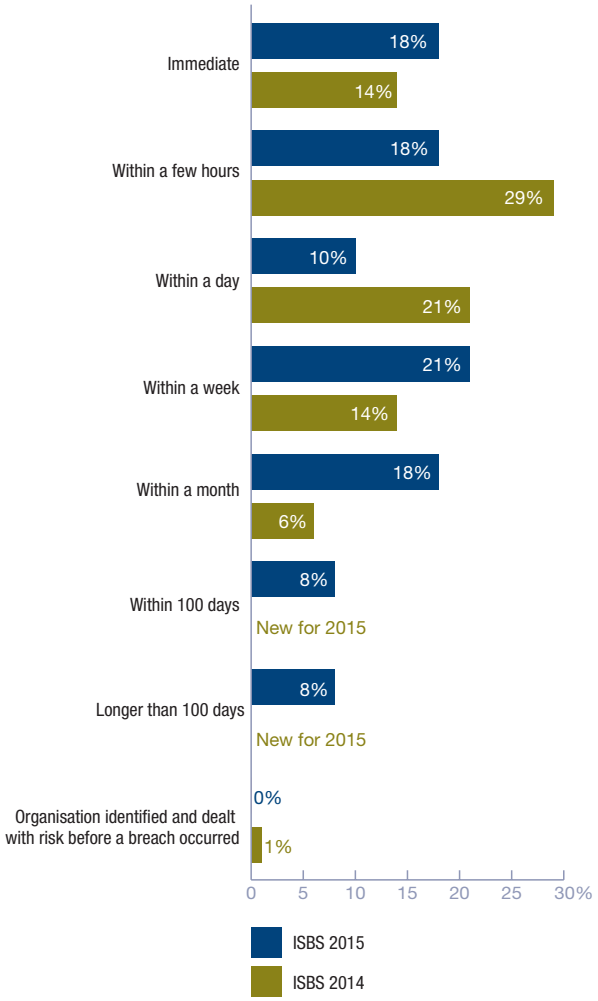
How was the incident identified?

Figure 24.1 *(based on 41 responses)*



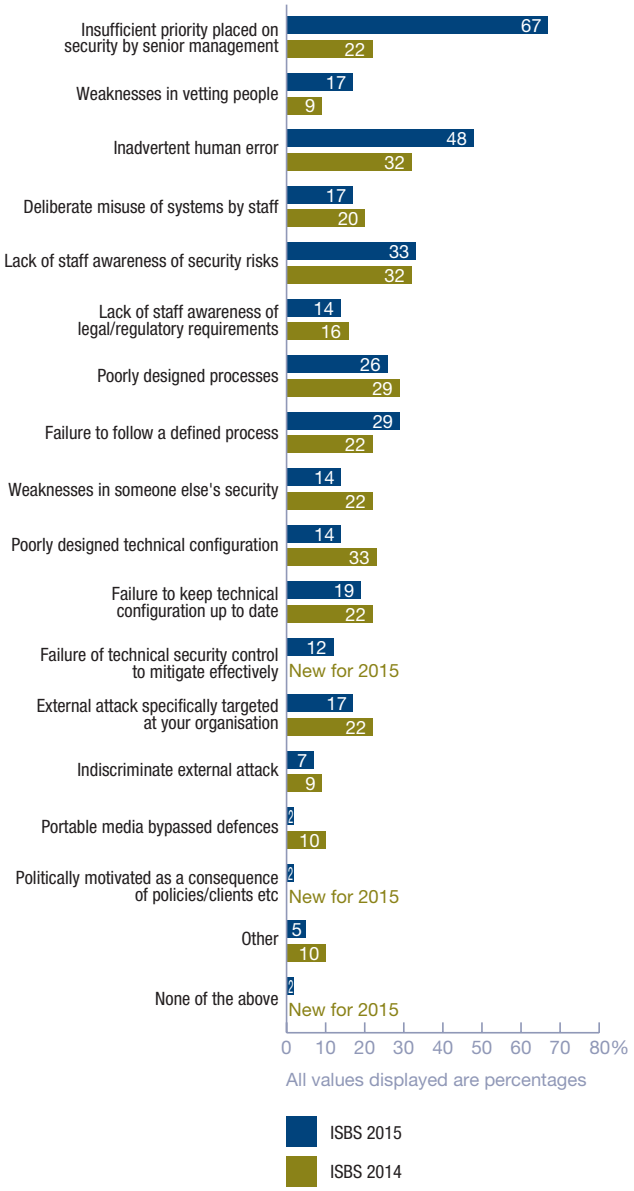
How long was it between the breach occurring and it being identified as a breach?

Figure 24.2 *(based on 39 responses)*



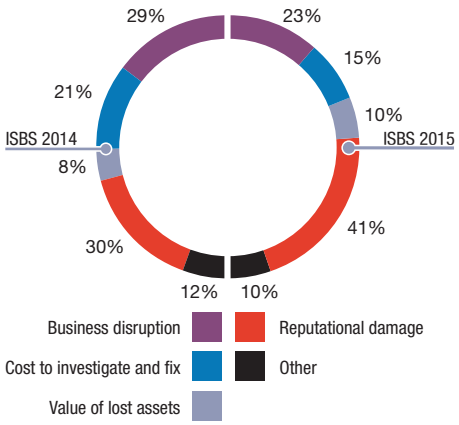
Which of the following factors contributed to the incident occuring?

Figure 24.3 *(based on 42 responses)*



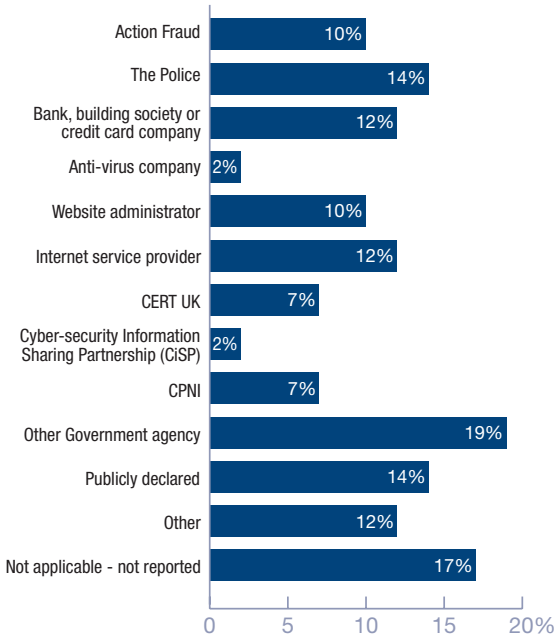
What made this incident the worst of the year?

Figure 24.4 *(based on 39 responses)*



Who was this breach reported to?

Figure 24.5 *(based on 42 responses)*

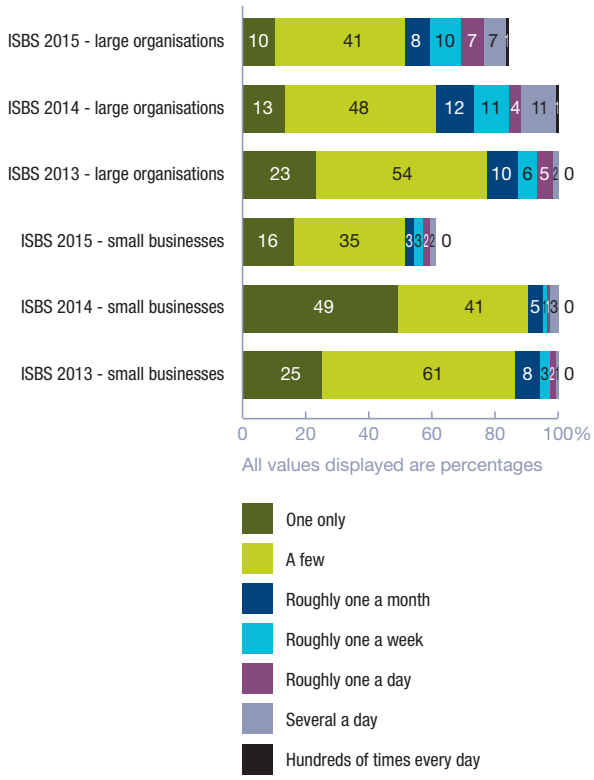


What was the origin (threat actor / source) of the breach?

Figure 24.6 *(based on 39 responses)*

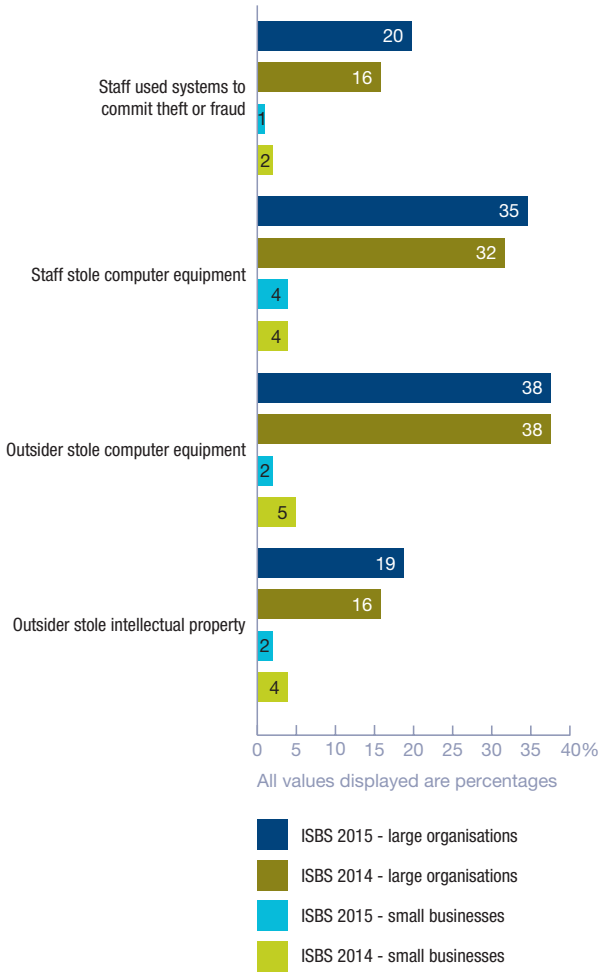
How many malicious software infections did the affected organisations suffer in the last year?

Figure 25 *(based on 232 responses)*



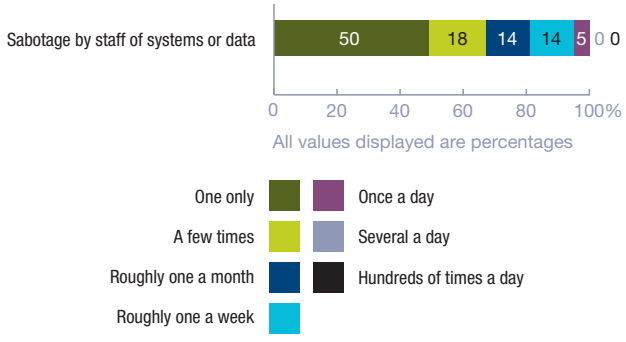
What type of theft or fraud did respondents suffer?

Figure 27 *(based on 513 responses for large and 351 responses for small)*



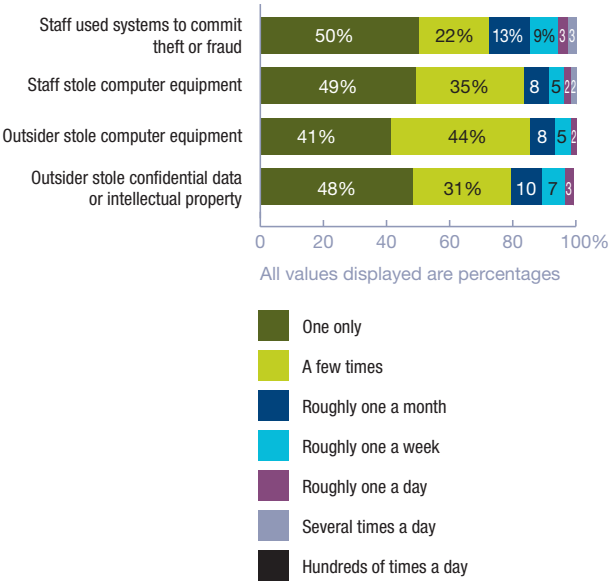
How many systems failures or data corruptions deliberately caused by staff did the affected organisation suffer in the last year?

Figure 26 *(based on 22 responses)*



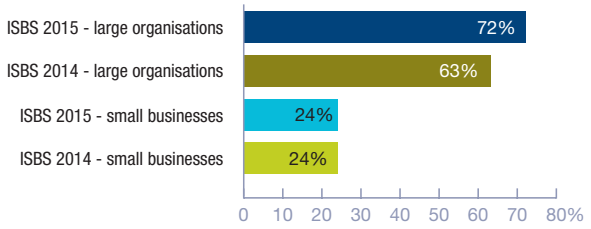
How many thefts or frauds did the affected organisations have last year?

Figure 28 *(based on 189 responses)*



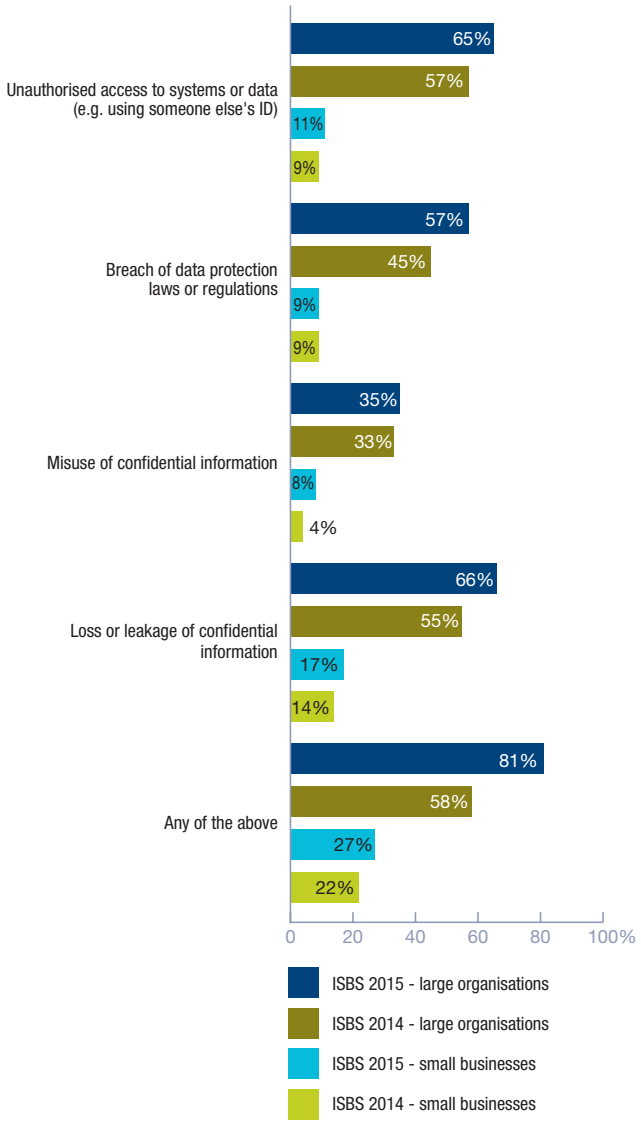
How many respondents have staff related incidents?

Figure 29 *(based on 166 responses for large and 90 responses for small)*



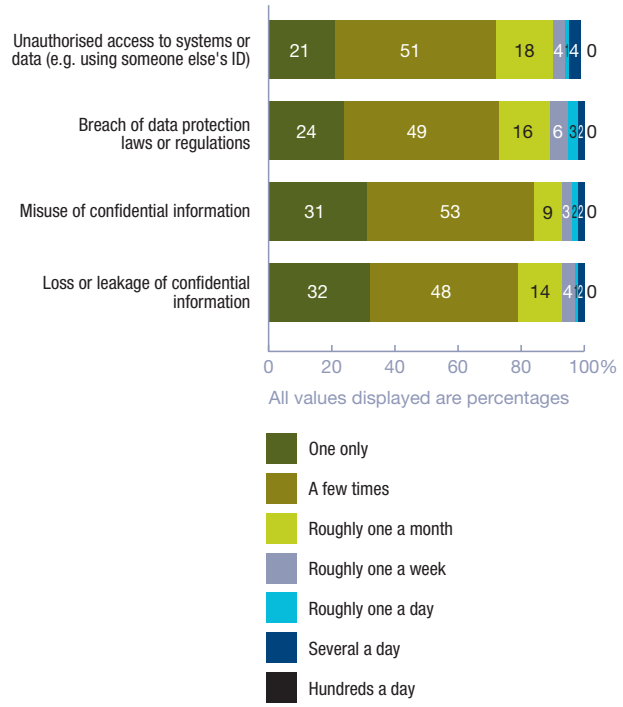
What type of staff related incidents did respondents suffer?

Figure 30 *(based on 148 responses for large and 90 responses for small)*



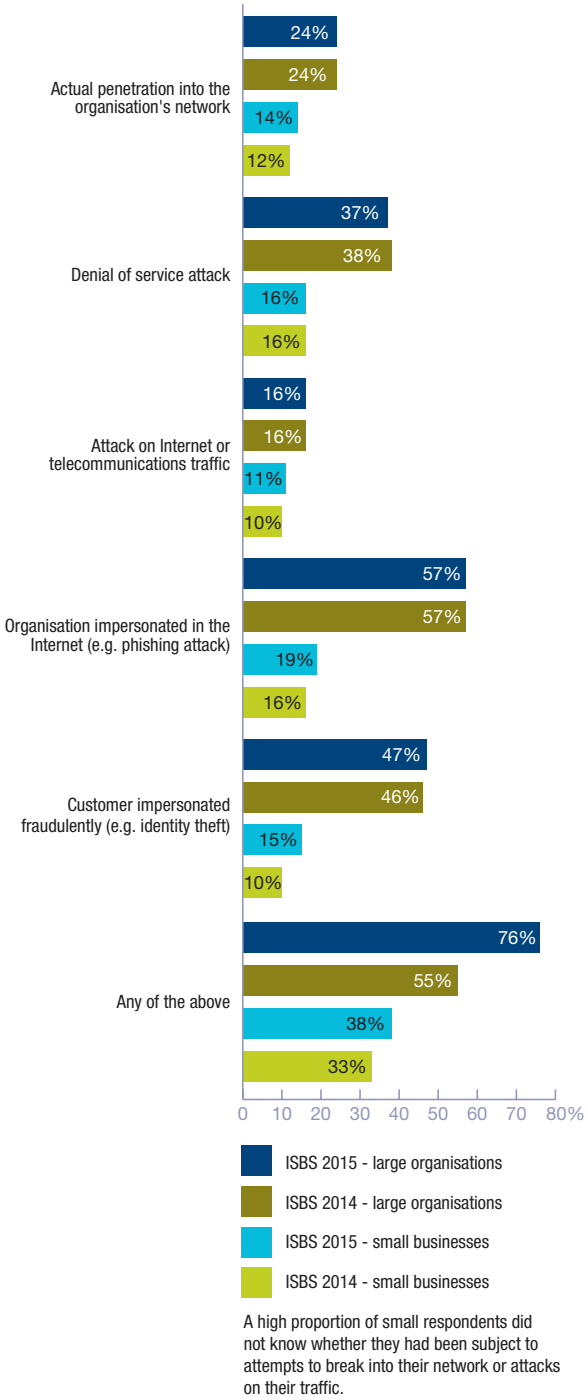
How frequent did the affected organisation have staff related incidents in the last year?

Figure 31 *(based on 424 responses)*



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

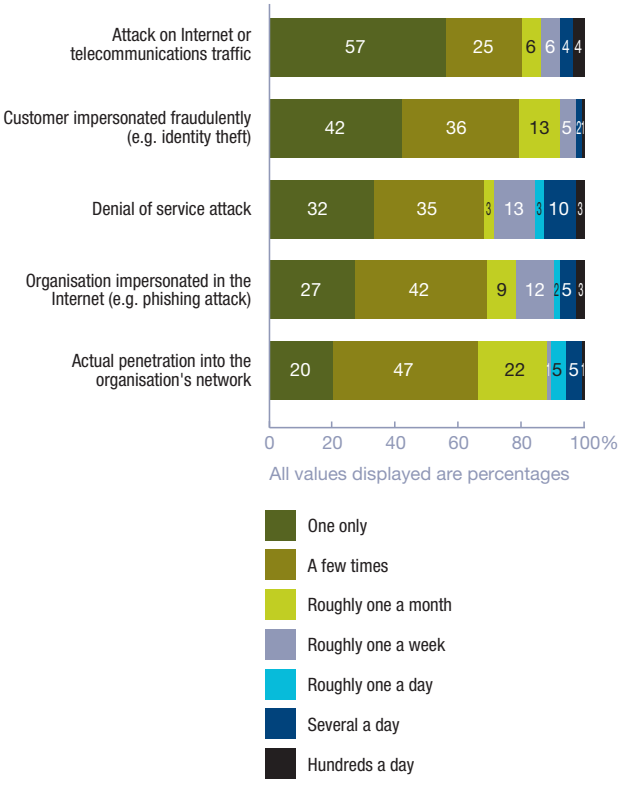
Figure 32 *(based on 140 responses for large and 90 responses for small)*



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.

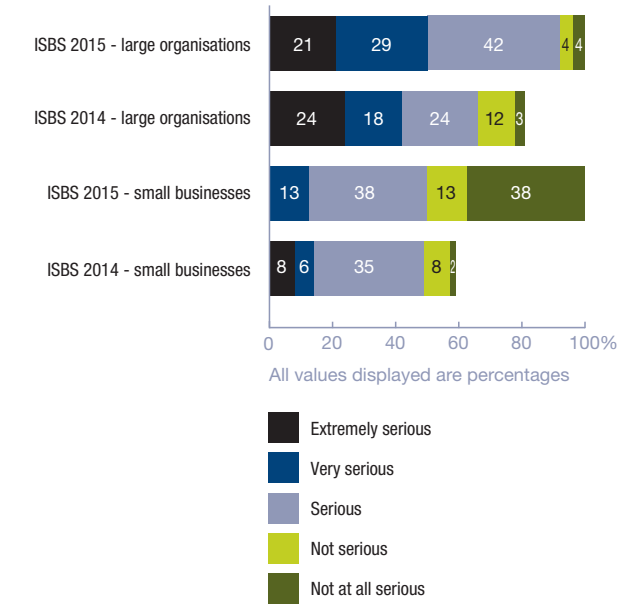
How many incidents did affected organisations have in the last year?

Figure 33 *(based on 368 responses)*



How many respondents had a serious incident?

Figure 34 *(based on 24 responses for large and 8 responses for small)*



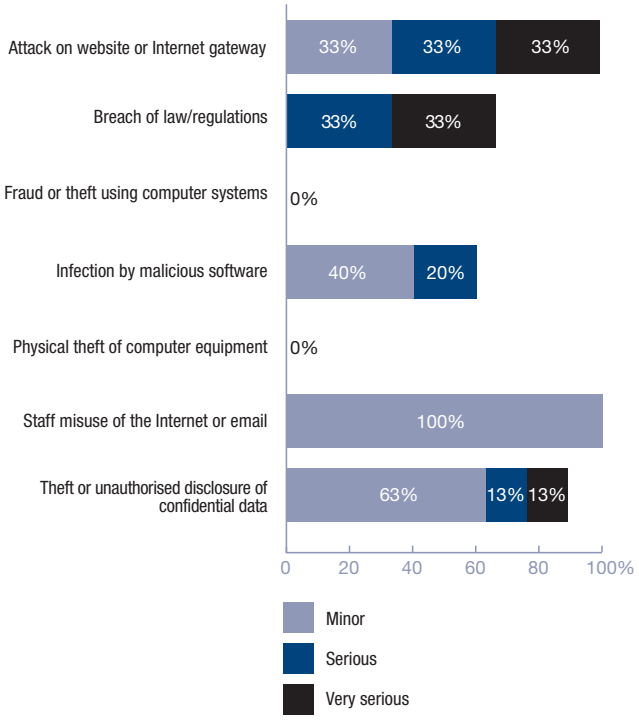
How much disruption to the business did the worst security incident cause?

Figure 35 *(based on 36 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	19%	8%	3%	3%	6%
Serious disruption		8%	3%	8%	6%
Minor disruption		3%	11%	6%	3%
Insignificant disruption		3%	6%	3%	3%

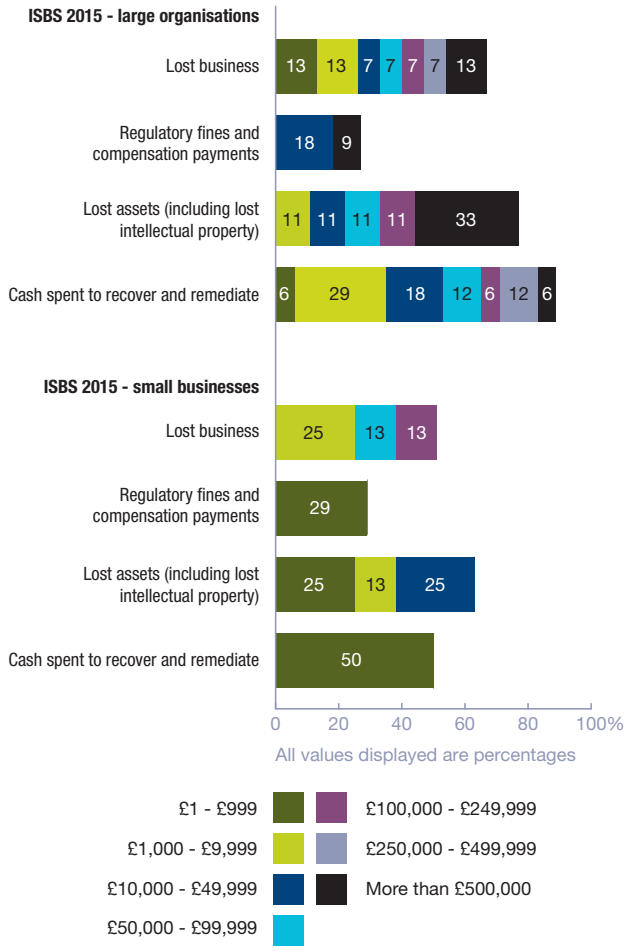
Which incidents were most disruptive to business?

Figure 36 *(based on 28 responses)*



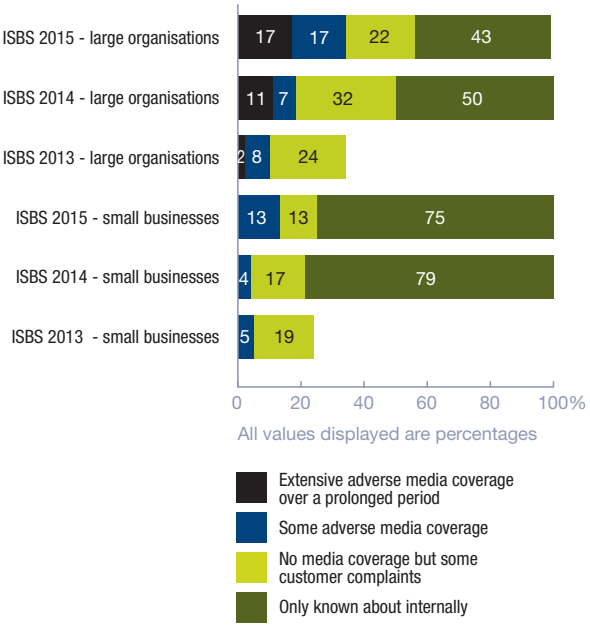
How much cash was lost or spent dealing with the worst security incident of the year?

Figure 37 *(based on 52 responses for large and 31 responses for small)*



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

Figure 38 *(based on 23 responses for large and 8 responses for small)*



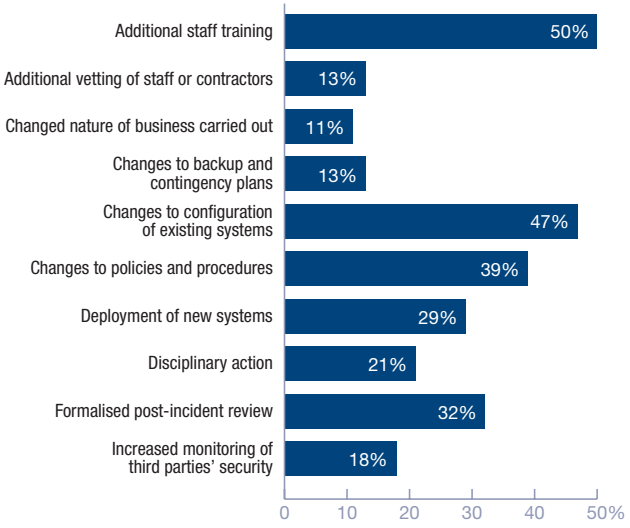
What was the overall cost of an organisation's worst incident in the last year?

Figure 39 *(based on 75 responses for large and 47 responses for small)*

	ISBS 2015 small businesses	ISBS 2015 large organisations
Business disruption	£40,000 - £225,000 over 2 - 12 days	£800,000 - £2,100,000 over 4 - 11 days
Time spent responding to incident	£3,000 - £10,000 13-24 man-days	£10,000 - £30,000 40-80 man-days
Lost business	£25,000 - £45,000	£120,000 - £170,000
Direct cash spent responding to incident	£250 - £500	£100,000 - £155,000
Regulatory fines and compensation payments	£150 - £300	£70,000 - £100,000
Lost assets (including lost intellectual property)	£6,500 - £14,000	£275,000 - £375,000
Damage to reputation	£3,000 - £16,000	£80,000 - £310,000
Total cost of worst incident on average	£75,200 - £310,800	£1,455,000 - £3,140,000
2014 comparative	£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

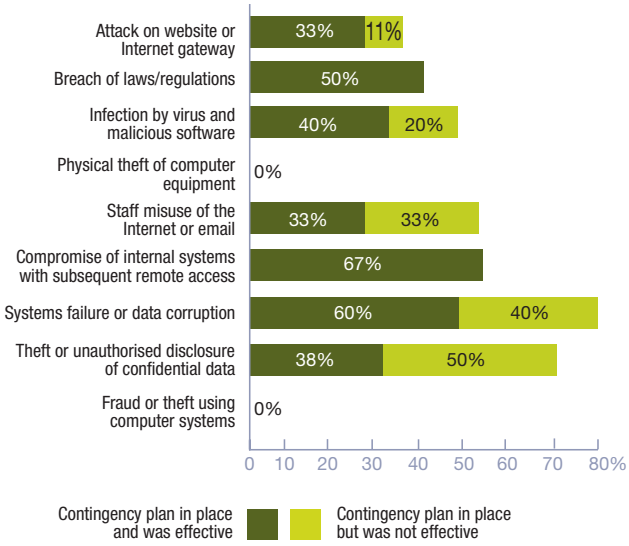
What steps did large organisations take after their worst security breach of the year?

Figure 41 *(based on 38 responses)*



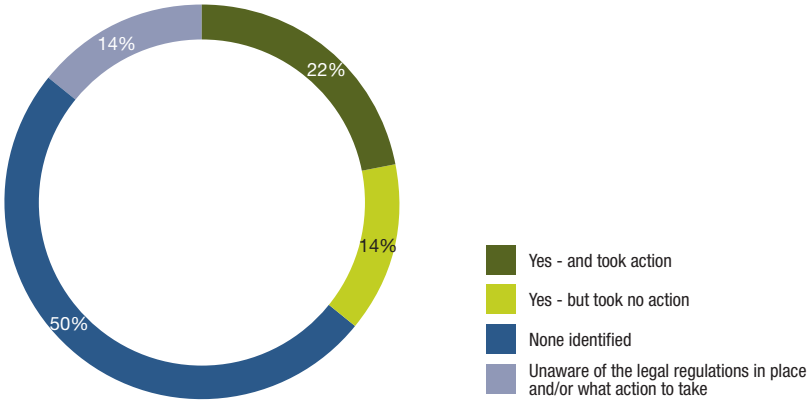
What type of security incidents do organisations plan for; and how effective are these contingency plans?

Figure 40 *(based on 35 responses)*



Did you identify any legal implications due to the nature of the breach?

Figure 42 *(based on 36 responses)*

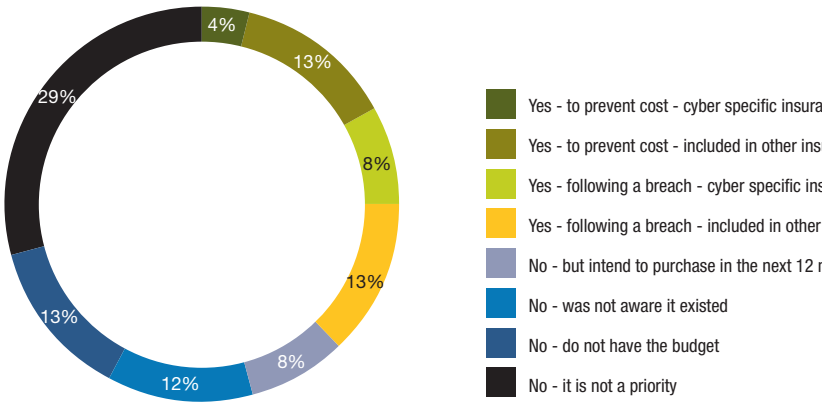


As a consequence of the incident, have you changed your investment in cyber security?

Figure 43 *(based on 38 responses)*

Do you have insurance which would cover you in the event of a breach?

Figure 44 *(based on 212 responses)*



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 Association of the British Pharmaceutical Industry (ABPI) is a trade association which represents the innovative research-based biopharmaceutical companies, large, medium and small, leading an exciting new era of biosciences in the UK.

Our industry is a major contributor to the economy of the UK, bringing 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.

For further information please go to www.abpi.org.uk.

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 144,000 chartered accountants worldwide. 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) The IET is a world leading professional organisation sharing and advancing knowledge to promote science, engineering and technology across the world. The IET has more than 160,000 members worldwide in 127 countries and is a professional home for life for engineers and technicians, and a trusted source of essential engineering intelligence. For further information, please visit www.theiet.org.

The BBA is the leading trade association for the UK banking sector with more than 230 member banks headquartered in over 50 countries with operations in 180 jurisdictions worldwide. Eighty per cent of global systemically important banks are members of the BBA. As the representative of the world's largest international banking cluster the BBA is the voice of UK banking.

Our network also includes over 80 of the world's leading financial and professional services organisations. Our members manage more than £7 trillion in UK banking assets, employ nearly half a million individuals nationally, contribute over £60 billion to the UK economy each year and lend over £150 billion to UK businesses.

BCS, The Chartered Institute for IT, promotes wider social and economic progress through the advancement of information technology science and practice. We serve over 75,000 members and bring practitioners, academics, government and industry together to share knowledge, shape public policy, promote new thinking, inform the design of new curricula and inform the public. We also deliver professional development tools for practitioners and employees and as a leading IT qualification body, we offer a range of widely recognised qualifications. More information is available at www.bcs.org.

CREST is a not-for-profit organisation that represents the technical information security industry, primarily penetration testing, cyber security incident response and security architecture services.

CREST offers public and private sector organisations an assurance that the technical security advisors they appoint are competent, qualified and professional with current knowledge. It also ensures that the CREST member companies they engage with have the appropriate processes and controls in place to perform the services for which they have been appointed and protect sensitive client-based information. www.crest-approved.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.

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.

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.

Cyber Security Challenge UK is a not for profit company that identifies, inspires and informs people with a talent for Cyber Security, and brings them together with leading organisations to raise awareness of learning opportunities and careers.

© Crown copyright 2015

You may re-use this information (not including logos and cover image) free of charge in any format or medium, under the terms of the Open Government Licence. Visit www.nationalarchives.gov.uk/doc/open-government-licence, write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

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.

URN BIS/15/302