
Department
for Business
Innovation & Skills
2014 INFORMATION SECURITY
BREACHES SURVEY
Executive Summary
Survey conducted by
pwc
In association with
infosecurity
EUROPE

Security breaches levels decreased slightly but much more costly

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

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

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

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

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

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

Cost of breaches nearly doubles in the last year

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

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

Organisations of all sizes continue to suffer from external attacks

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

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

Fewer small businesses experienced attacks than a year ago.

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

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

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

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

"The Ten Steps" guidance continues to be relied on

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

26%	of respondents use "the Ten Steps" guidance

Understanding, communication and awareness lead to effective security

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

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

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

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

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

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

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

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

Businesses need to manage the risks associated with new technology

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

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

Organisations are seeking new ways to gain assurance over security

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

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

Key observations of the year

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

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

Any enquiries regarding this publication should be sent to:

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

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

BIS/14/766