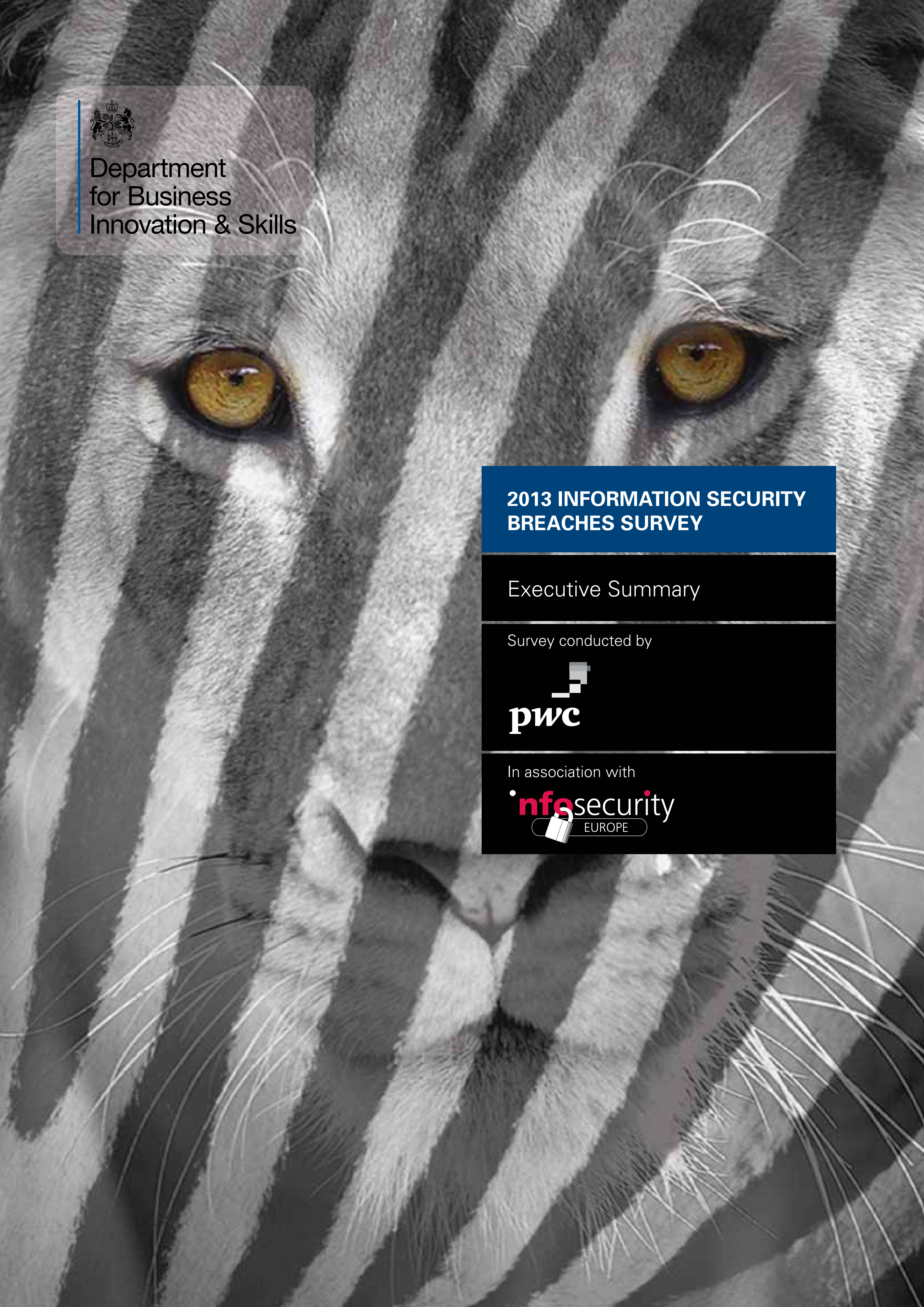

Department
for Business
Innovation & Skills

2013 INFORMATION SECURITY BREACHES SURVEY

Executive Summary

Survey conducted by

pwc

In association with

infosecurity
EUROPE

Executive Summary

Security breaches reach highest ever levels

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

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

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

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

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

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

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

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

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

Both external attacks and the insider threat are significant

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

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

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

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

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

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

Understanding and communicating the risks is key to effective security

The vast majority of businesses continue to prioritise security.

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

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

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

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

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

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

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

Many struggle to implement basic security

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

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

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

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

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

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

Any enquiries regarding this publication should be sent to:

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

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

BIS/13/P184 - ES