www.pwc.com

Information security breaches survey

Executive summary

April 2012

infosecurity EUROPE

BIS Department for Business Innovation & Skills

pwc

Executive summary

Increase in cyber-threats keeps cost of breaches high

The vast majority of respondents had a security breach in the last year:

93%	of large organisations
76%	of small businesses

The main cause is an increase in the number of cyber-attacks, especially for large organisations:

54	is the median number of significant attacks by an unauthorised outsider on each large organisation in the last year (twice the level seen in 2010)
15%	of small businesses were hit by denial of service attacks in the last year
15%	of large organisations detected hackers had successfully penetrated their network in the last year

As a result, the cost to UK plc of security breaches remains high, while down somewhat on 2010 levels:

£15k - £30k	is the average cost of a small business's worst security breach of the year
£110k - £250k	is the average cost of a large organisation's worst security breach of the year
Billions	is the total cost to UK plc of security breaches in the last year

It's not just about technology – people are vital too

Most serious security breaches are due to multiple failings in people, processes and technology. Computer frauds, data losses and regulatory breaches (together with hacking attacks) were most likely to result in a very serious breach.

45%	of large organisations breached data protection laws in the last year (and this happened at least once a day at one in ten of them)
18%	of organisations affected by infringement of data protection laws had an effective contingency plan in place
20%	of small businesses lost confidential data (and 80% of these breaches were serious)
19%	of large organisations suffered from staff carrying out computer fraud

The root cause is often a failure to invest in educating staff about security risks, often only recognised after the event:

44%	of large organisations carried out additional staff training after their worst security breach of the year (and 38% changed their policies and procedures)
26%	of organisations with a security policy believe their staff have a very good understanding of it
75%	of organisations where the security policy was poorly understood had staff-related breaches
54%	of small businesses don't have any programme for educating their staff about security risks

Controls are not keeping pace with business changes

The Internet continues to facilitate more sophisticated business relationships:

73%	of respondents have outsourced business processes over the Internet
38%	of large organisations ensure that data held by external providers is encrypted
56%	of small businesses don't carry out any checks of their external providers' security (and rely instead on contracts and contingency plans)

Social networks have become more important over the last two years:

52%	of small businesses depend on social networking sites (up from 32% in 2010)
8%	of small businesses monitor what staff have posted on those sites

Organisations are rapidly opening up their systems to access via mobile devices:

75%	of large businesses allow staff to use smart phones and tablets to connect to their systems
39%	ensure that data on these smart phones and tablets is encrypted
34%	of small businesses allow smart phones and tablets to connect to their systems but haven't done anything to mitigate the security risks

The challenge is to spend money wisely

On average, organisations continue to spend a significant amount on their security defences, as they expect the assault from breaches to continue:

8%	of IT budget is the average amount respondents spent on information security
50%	of large organisations expect to spend more on security next year (versus only 14% who expect to spend less)
67%	of large organisations expect more security breaches next year (versus only 12% who expect fewer)

However, there are some signs of complacency in some large organisations:

12%	say senior management give a low priority to security
20%	spend less than 1% of IT budget on information security

A root cause is that it is hard to measure the business benefits from spending money on security defences. Investing in security can end up losing out against other competing business priorities. Worse still, it's easy to spend money on the wrong things.

80%	of large organisations don't evaluate return on investment on their security expenditure
58%	of small businesses don't try to evaluate the effectiveness of their security expenditure at all

www.pwc.com

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

Design: ML1-2012-03-01-11 49-VF