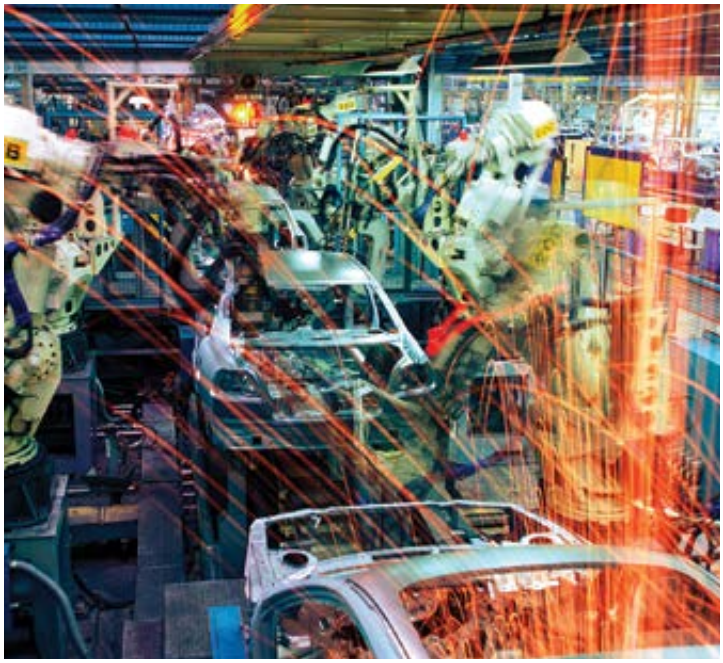
HM Government



2015 INFORMATION SECURITY BREACHES SURVEY

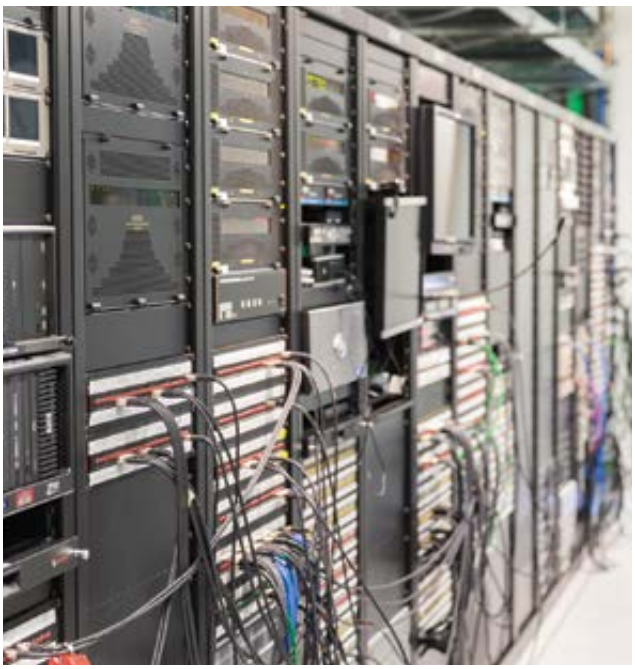
Executive Summary

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.

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.

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.

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/15/303