

INTERNATIONAL TRENDS IN CYBERSECURITY

Summary for the United Kingdom



April 2016

EXECUTIVE SUMMARY

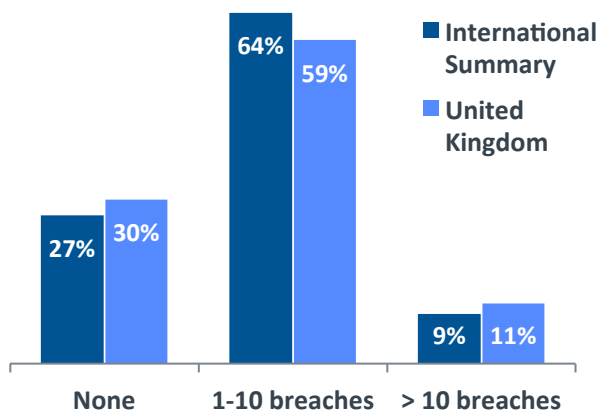
The importance of information technology (IT) security continues to grow. About 8 in 10 managers responsible for security at their firms across the 12 countries covered in CompTIA's *International Trends in Cybersecurity* expect security to become an even higher priority over the next two years (79% net of moderately higher + significantly higher). Anticipated priority two years from now is significantly higher among firms in Maturing Economies (86% net higher) vs. those in Mature Economies (68% net higher). Nearly two-thirds of businesses in the United Kingdom (UK) expect IT security to grow in importance (66% net higher).

Due to the evolving nature of IT, the great majority of organisations have had to respond by changing the way their company approaches security. In the UK, similar to many of the other countries, the greatest factor has been the change in IT operations, especially as firms move to the cloud or implement new mobility strategies.

Another significant driver of change in security approach is internal security breaches. Furthermore, across all the companies surveyed, nearly three-quarters report having at least one security breach/incident* in the past 12 months (73%).

OCCURRENCE OF SECURITY BREACHES

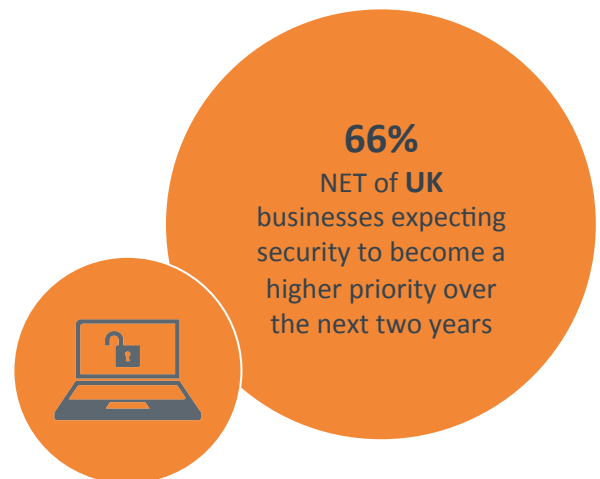
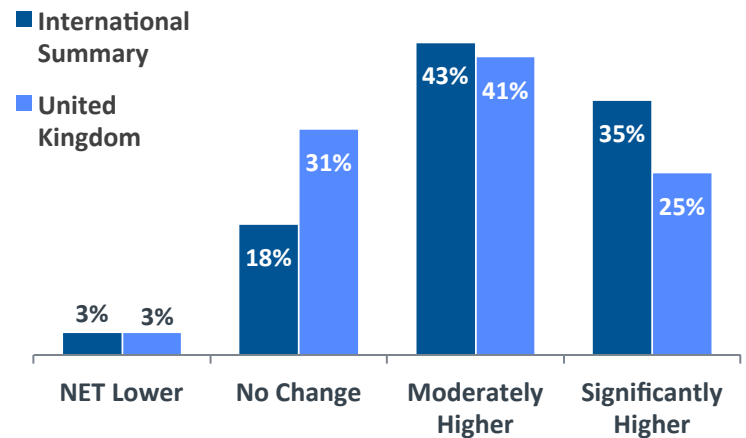
Over the past 12 months



*Stemming from internal or external causes.

IMPORTANCE OF CYBERSECURITY

Expected priority in 2 years from today



TOP DRIVERS FOR CHANGING APPROACHES TO CYBERSECURITY

Among UK businesses

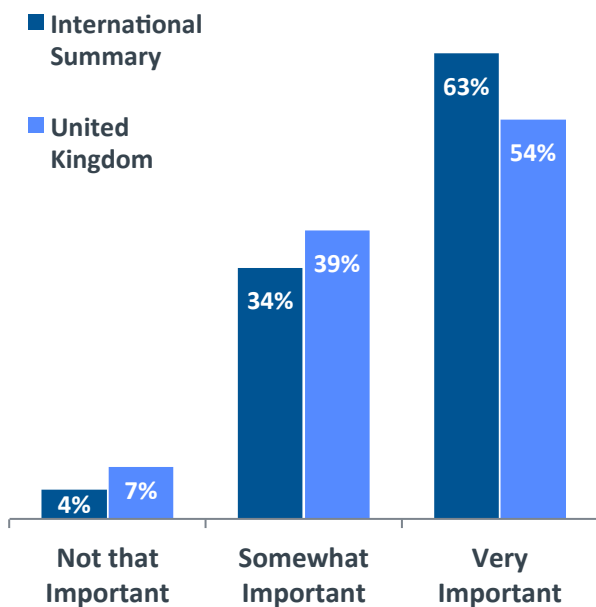
1. Change in IT operations (e.g. cloud, mobility)
2. Internal security breach or incident
3. Change in business operations or client base
4. Reports of security breaches at other firms
5. Change in management

Note: see the last page for which countries are categorised in Maturing Economies vs. Mature Economies.

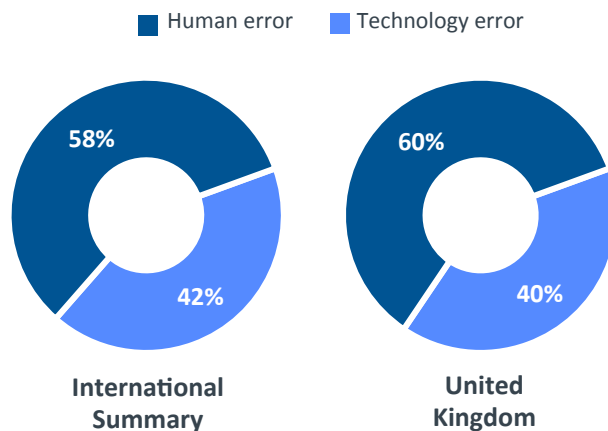
While 7 in 10 UK organisations experienced at least one security incident, slightly over half had one or more serious breaches. Human error is becoming more of a factor in security breaches for most companies, especially for those in Maturing Economies (64% net overall significantly more + moderately more). In the UK, it is more of a factor now vs. two years ago for more than half (56% net human error more of a factor).

On the brighter side, roughly 9 in 10 firms use some type of security training to assess or improve security knowledge among employees such as new employee orientation, ongoing security training programs, random security audits, online courses, etc. (92% overall and 90% in the UK). And most managers believe it is important to test after IT security training to confirm knowledge gains (93% net very important + somewhat important in the UK). Moreover, employers in Maturing Economies especially find IT security certifications to be very valuable (49%) compared to those in Mature Economies (25%). Nearly two-thirds of UK managers indicate that IT security certifications are very valuable (33%) or valuable (32%) in terms of validating security-related knowledge/skills or evaluating job candidates.

IMPORTANCE OF TESTING AFTER CYBERSECURITY TRAINING



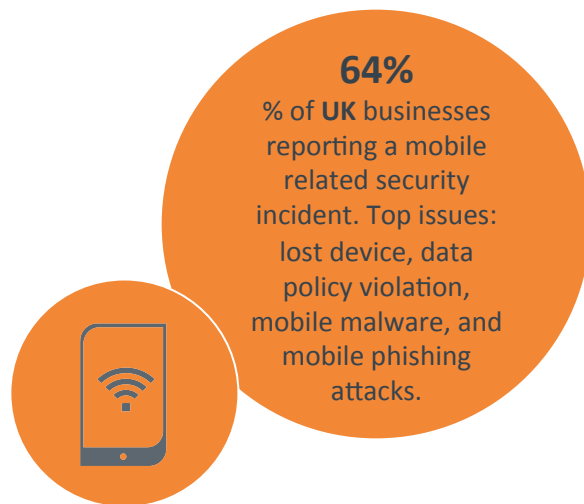
HUMAN ERROR A MAJOR CONTRIBUTOR TO SECURITY RISK



TOP SOURCES OF HUMAN CYBERSECURITY ERROR

Among UK businesses

1. General carelessness
2. IT staff failure to follow policies and procedures
3. End user failure to follow policies and procedures
4. Lack of expertise with networks, servers and other infrastructure
5. Lack of expertise with websites and applications
6. Failure to get up to speed on new threats



RESEARCH METHODOLOGY

CompTIA's *International Trends in Cybersecurity* was conducted to collect and share quantitative information on behaviors, techniques, and opportunities associated with IT security across 12 countries. More information and all country snapshots are available at CompTIA.org/internationalsecurity.

A total of 1,509 IT and business executives participated in the online survey during January – February 2016, yielding an overall margin of sampling error at 95% confidence of +/- 2.5 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimise its influence.

CompTIA is a member of the Marketing Research Association and abides by its guidelines for survey best practices and research ethics.

CompTIA is responsible for all content contained in this report. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.

Job Role

22%	Executive Mgt. (CEO, President, Owner, etc.)
23%	Senior Mgt. – IT function (CIO, CSO, VP, etc.)
10%	Middle Mgt. – IT function (Director, Team Lead)
11%	Staff level – IT function
21%	Senior Mgt. – Business function (CFO, VP, etc.)
6%	Middle Mgt. – Business (Director, Team Lead)
8%	IT Consultant

SURVEY DEMOGRAPHICS

Firm Size

5%	Micro firm (5 to 9 employees)
34%	Small firm (10 to 99 employees)
30%	Medium firm (100 to 499 employees)
30%	Large firm (500 or more employees)

Primary Industry

20%	Information Technology (IT)
14%	Manufacturing (other than IT related)
11%	Professional services (other than IT related)
10%	Retail/Wholesale (other than IT related)
6%	Healthcare/Medical
8%	Financial/Banking/Insurance
2%	Media/Publishing/Entertainment
3%	Government (federal, state, local)
7%	AMTUC (Agriculture, Mining, Transportation, Utilities, Construction)
6%	Education
3%	Hospitality
9%	Other industry

Countries

n	Maturing Economies	n	Mature Economies
126	Brazil	125	Australia
131	India	125	Canada
125	Malaysia	125	Germany
126	Mexico	125	Japan
125	South Africa	125	UK
125	Thailand		
126	UAE		
884	Total Maturing	625	Total Mature
1,509	Total number of respondents in the study		



ABOUT COMPTIA

CompTIA is the voice of the world's information technology (IT) industry and workforce.

Its members are the companies at the forefront of innovation; and the professionals responsible for maximising the benefits organisations receive from their investments in technology.

CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications, and public policy advocacy.