IDC
Analyze the Future

IDC ANALYST CONNECTION

Kevin Bailey
Research Director, European Security Software, IDC

Kensington: Security Focus on Non-Standard IT Devices (BYOD)

Sponsored by: Kensington Europe

September 2012

Executive Summary

The adoption of "bring your own device" (BYOD) is a major security issue for all organizations as individuals embrace the evolution of consumerization to enhance their personal productivity, but lack the experience and/or expertise of the associated security risks. Use of non-company-standard devices raises the issue of data loss, device loss, and corporate intellectual property (IP) sprawl, requiring control mechanisms that do not restrict usage but manage and assist in the individual's activity on these devices.

The IDC survey commissioned by Kensington Europe obtained responses from 756 sales and marketing professionals in the U.K., Germany, and France, across all industry classifications and four organizational segments.

Small business organizations drive a higher adoption than the more (assumed) established corporates. Much of this evidence could be associated with the higher levels of generation Y and Z employed, and the creative/flexible nature of smaller organizations compared with internal standards and regimentation of midmarket/enterprise organizations.

It is evident that the respondents continue to favor their personal data over business content, although the enterprise segment survey respondents show a distinct awareness of personal/business data collocation compared with the small business respondents that may treat any corporate or personal data on their device as their "own" data and as such see very little differentiation in its management, increasing the opportunity for security breaches.

IDC Opinion

IDC believes that the survey conveys a clear indication that the respondents continue to value their own personal data over the corporate data that is resident on or accessible via their non-standard IT devices, without appreciation that those devices (tablet, smartphone, ultra book, notebook, etc.) contain the same or greater capabilities of their corporate PC/desktop computer, while also failing to recognize the tangible and inferred value of the corporate data held on the device(s).

Although BYOD can improve productivity, business agility, cost reductions, and employee engagement, it is evident from the survey that the loss of device and/or data causes minimal concern to the respondent(s). Brand image, identity, and reputation will be negatively affected as the correlation between the device user and their employer is realized, providing an opportunity for lost data (and devices) to be exploited for unintentional purposes by criminals, competitors, or any other malicious individual. Organizations can address these risks through the prioritization of education, policies, and security solutions that prevent loss or minimize risk of theft, and processes related to the management, usage, and security risks involved when implementing a BYOD adoption strategy.

The investment that organizations deploy today for BYOD will minimize the security risks as BYOD evolves into bring your own technology (BYOT) and bring any device (BAD).

Questionnaire Review and Analysis

Q1. *Does anyone in your organization use their own, non-standard IT issued devices, such as tablets (e.g., iPads) or smartphones (e.g., iPhone), to connect to the network or perform their daily tasks such as email?*

The respondent feedback clearly shows that employees in the U.K. have a more favorable approach to BYOD than in France and Germany, with almost 75% of respondents using a personal device as a company tool. French respondents have a slightly more cautious approach to this adoption, with a 60/40 split embracing BYOD utilization. Germany has a 70/30 split, which aligns to the average percentage across the three countries.

The distribution of BYOD across the sales and marketing respondents has a comparable adoption split (66%–68% "yes" and 32%–34% "no"). It is evident that the larger enterprise 1,000+ employee organizations have a slower adoption rate of BYOD than the three other segments, with organizations of up to 100 employees being the most adoptive. (The 500–999 segment has a larger percentage, but the sample size of 74 is lower than IDC's target requirement of 100 respondent count for a confident decision outcome.)

For smaller organizations, where in many cases the generation Y and Z employees reside, company enforcement of technology will be less prevalent than in the larger enterprise corporations, where established device type standards may already exist.

Q2. *Does your employer offer security policy or advice support to users who bring their own devices to work?*

The traditional traits of the German market are evident in the data points from the survey. The adoption of policy guidance for BYOD is higher in this market than in the other two countries. The U.K. and France appear to be engaged in a slower policy enforcement approach, engaging in an assumptive "trust" and/or "learn as you use" engagement approach.

Marketing and sales respondents have an equally balanced view on the use of policies and support around BYOD. This would be a normal response for organizations, as the enforcement of policies and support should be a company initiative rather than departmental. An exception to this may exist where the two distinct functions are physically located in disparate locations, such as offices or countries.

A wide difference exists between organizational sizes, with adoption growth increasing based on the size (and assumed maturity) of the company. The smallest segment (>100) has the lowest engagement of BYOD security policies (34%). Further analysis around the type of vertical segment within this group would increase the intelligence of segment profiles to understand the organizational focus between external (revenues, customer engagement, differentiation) rather than risk mitigation activities (data loss, device loss, corporate IP sprawl, etc.). Further data points would ensure that post-survey targeting could assist with higher levels of response ratios.

As you move through the segments the maturity and awareness of the organizations appear to increase, with the enterprise organizations employing policies that may align with other established company guidelines and support structures for IT operations.

Q3. *If you used your own device at work and it was lost or stolen, is it fair to say you would be more concerned about:*

- *Someone else accessing your personal content and social media channels and contacts*

Than about:

- *Possible damage incurred as a result of jeopardizing the protection of confidential, sensitive, or business critical data*

The data points from the respondents provide clear evidence that the personal content either on the device or associated with social media channels is the most valuable asset on their devices.

Germany is slightly higher than the U.K. and France, but the mean average identifies that the respondents' two possible determining factors may be:

- The device is still primarily seen as a personal asset with associated data and applications that have greater value to the respondent
- The amount of corporate IP data is minimal and does not register as a security risk either to the respondent or their associated employer

The respondents' roles suggest a leaning more toward concern about their own personal data and social channels than toward corporate IP data. Combining the midmarket segments (100–499 and 500–999 employees) provides a mirror image of the small business (>100) segment, whereas respondents in the largest (enterprise) segment appear to have a slightly higher awareness of the co-location of social/business content and its impact on the business if the device were lost or stolen.

Demographic Questions

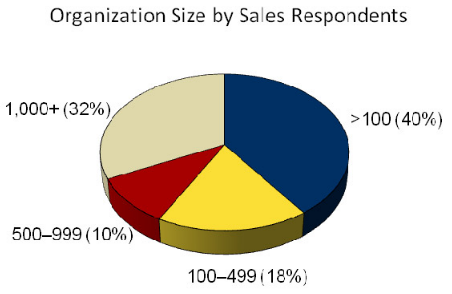
S2. *Which of the following best describes your line of work or department at your organization?*

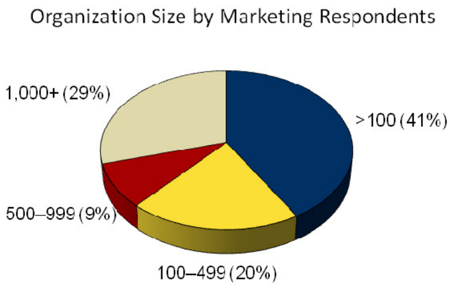
The distribution of respondents across the three countries participating in the survey was 756, with 252 respondents completing the survey from each of the three target countries (the U.K., France, and Germany). The survey targeted sales (69%) and marketing (31%) professionals, as they are perceived to be two of the more progressive lines of business that are adopting BYOD, with sales using it to increase mobile working and productivity, and marketing adopting and using Web 2.0 tools. All other respondents were excluded from further involvement. The respondent counts for sales and marketing professionals ranged from 141 to 305, within each of the organizational segmentation groups, and this provided excellent sample sizes. The 500–999 segment fell short of the "normal distribution" sample that IDC proposes for positive analysis. In appropriate cases IDC has combined the 100–499 and 500–999 segments for a more positive analysis. It is essential that the survey identified which size (segment) of organization that the respondent is aligned to, as this will assist in indicating the differences in BYOD adoption based on company culture, innovation, and priorities. In relation to terminology, IDC has identified the most common segment groupings from the survey:

•	>100	—	Small business
•	100–499/500–999	—	Midmarket
•	1,000+	—	Enterprise

S3. *How many employees does your organization have in country?*

France and Germany have a balanced distribution (~33%) of respondents across the organizational segments, whereas the U.K. returned a bias 54% in the small business segment and 23% in the other segments. Although the respondents entered a valid employee size, further validation may be sought to tighten the understanding if the respondents confirmed that the employee sizes were representative of the country rather than the complete organization size across regional/country boundaries. Alignment of respondents by organizational segments can be seen in the following two figures.





D1. *What industry classification best represents your organization's main area of activity?*

The breakdown between marketing and sales respondents indicates a good representation of field (sales) and operational (marketing) use of BYOD adoption. Each of the respondent groups will have an assumed equal usage of personal and social content activity, whereas business tools outside of email will vary, such as salesforce.com, Eloqua, Oracle, Twitter, SAP, Grader, Klout, and Concur, which will change the level of corporate data being held or accessible via the device(s), either increasing or neutralizing the security risk for BYOD.

The mean average across the industry classifications would be 7.14%. IDC has achieved a positive analysis across four of the industry classifications: business or professional services, manufacturing, retail and wholesale, and telecommunications. Each of these industry markets will have a different approach to their cycle of technology adoption, which infers that their engagement of BYOD and its associated management and security policies will differ.

ABOUT THIS ANALYST

Kevin Bailey is the research director covering European security software at IDC, a wide portfolio covering secure content and threat management (SCTM), identity and access management (IAM), and security and vulnerability management (SVM). Bailey's research provides analysis on strategic trends, and business and competitive intelligence, and delivers key insights and intelligence on the evolving security landscape and its implications for the IT ecosystem. *In addition to syndicated research, Bailey designs and manages bespoke projects which support his clients in their product and marketing strategies, business plans, and research and development.*

Bailey is an experienced public speaker, delivering client relevant keynote and market-specific topics at vendor (direct and channels), industry, and end-user events around the globe. *Before joining IDC, Bailey worked at Symantec as the head of its Global Market Analytics & Strategies team, providing competitive intelligence, analyst and influencer relations, and quantitative/qualitative insights for Symantec's enterprise portfolio of products and services. Prior to Symantec, he was global marketing director for information asset management start-up Njini, and marketing director at StorageTek.*

Bailey holds an MSc from the University of Glamorgan business school, focused on the adoption of social media as a strategic tool in business, and holds the Chartered Institute of Marketing Postgraduate Diploma.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com.