

Global Privacy & Identity Research

Preview of two new studies

2009 Digital ID World Conference

Dr. Larry Ponemon
September 15, 2009
Las Vegas, Nevada

Proposed Agenda

- Introduction
- Accenture study: Review the results of a new study about the privacy perceptions, beliefs and attitudes of business practitioners in 19 countries:
 - Attitudes about privacy
 - Attitudes about identity management
- ThreatMetrix study: Study about consumer perceptions about device fingerprinting and the impact of privacy.
- Discuss implications for IDM
- Audience questions

Ponemon Institute LLC

- ✓ Ponemon Institute is dedicated to advancing responsible information management practices that positively affect privacy and data protection in business and government.
- ✓ The Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations.
- ✓ The Institute has assembled leading multinational corporations called the **RIM Council**, which focuses on the development and execution of ethical principles for the collection and use of personal, sensitive or confidential information.

About Global Privacy Perceptions

Research Sponsor: Accenture

Forthcoming white paper available upon request

Introduction

- The purpose of this research is to better understand how business practitioners in different countries around the world are responding to privacy and data protection issues. This is the first truly “global” study that attempts to compare and contrast how individuals in different nations are responding to growing privacy and data protection threats.
- Working in partnership with Accenture, Ponemon Institute independently conducted studies in 19 countries. Our research methods included a combination of secure web, telephone and interview methods.
- The survey instrument contained a series of objective, fixed formatted questions. While questions were held constant across national samples, the instrument was translated into the natural language of participants with minor wordsmithing for cultural differences that may interfere with local interpretation and clarity.
- In addition to responses to specific questions, results were used to compile a global privacy index drawing from positive and negative responses to key questions about privacy and data protection within each one of 19 countries studied.

Description of 19 national samples

The two letter country abbreviation is used in graphical analysis

Conducted by Accenture & Po

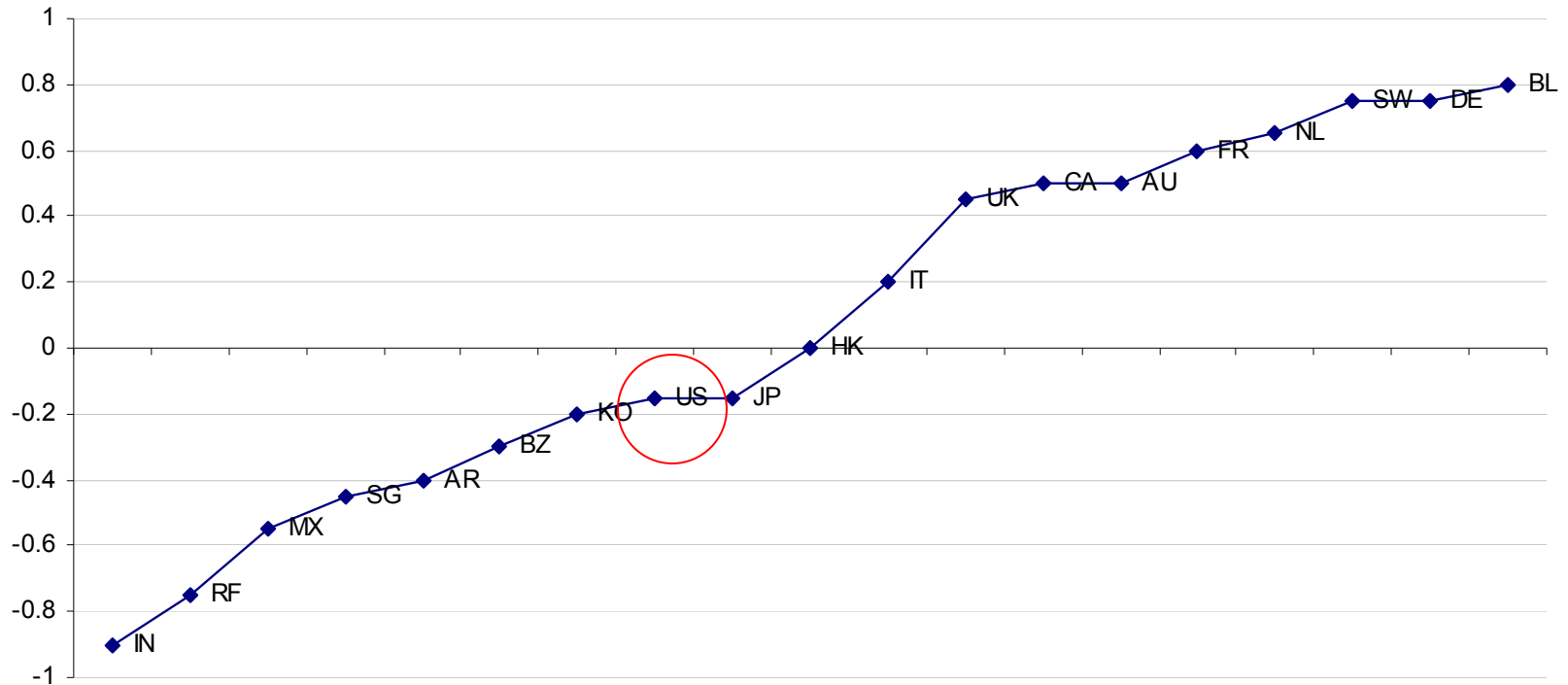
- ✓ Nineteen (19) separate country level samples were studied in March and April 2009.
- ✓ The survey instrument attempted to capture individual perceptions about privacy and data protection.
- ✓ The researcher utilized either secure web or telephone based survey methods in all countries.
- ✓ The sampling frame included only business and IT practitioners presently employed.
- ✓ The number of targeted respondents exceeded 109k individuals.
- ✓ The total response rate after adjusting for unreliable survey results is 5,512, which represents a 5% overall response rate.
- ✓ The margin of error on all adjective and binominal survey items is $\leq 5\%$.

Country	Country abbreviations	Panel	Sample	Response
United States	US	14,865	689	4.6%
United Kingdom	UK	5,442	511	9.4%
The Netherlands	NL	4,598	219	4.8%
Switzerland	SW	3,890	150	3.9%
Singapore	SG	2,547	77	3.0%
Russian Federation	RF	5,370	173	3.2%
Mexico	MX	4,133	301	7.3%
Korea	KO	3,779	228	6.0%
Japan	JP	5,064	180	3.6%
Italy	IT	4,092	225	5.5%
India	IN	11,041	581	5.3%
Hong Kong	HK	2,558	118	4.6%
Germany	DE	5,222	314	6.0%
France	FR	4,794	224	4.7%
Canada	CA	8,293	403	4.9%
Brazil	BZ	9,200	339	3.7%
Belgium	BL	4,164	248	6.0%
Australia	AU	4,902	263	5.4%
Argentina	AR	5,559	269	4.8%
Totals		109,513	5,512	5.0%

Global Privacy Index (ratio score)

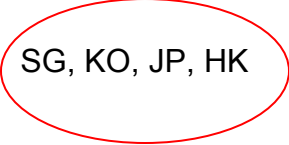
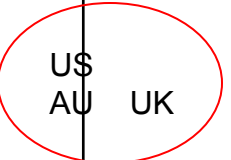
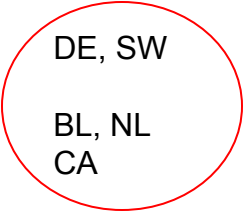
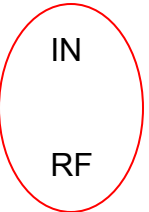
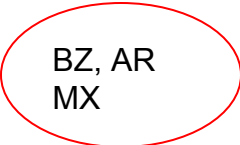
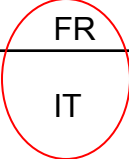
A total of 40 survey questions were used to construct this index. For each question, +.025 was assigned for countries responding above the mean response and -.025 was assigned for countries responding below the mean response. Thus, the maximum potential score is +1 and the minimum potential score is -1.

Global Privacy Index
By ratio score (Max = +1, Min = -1)



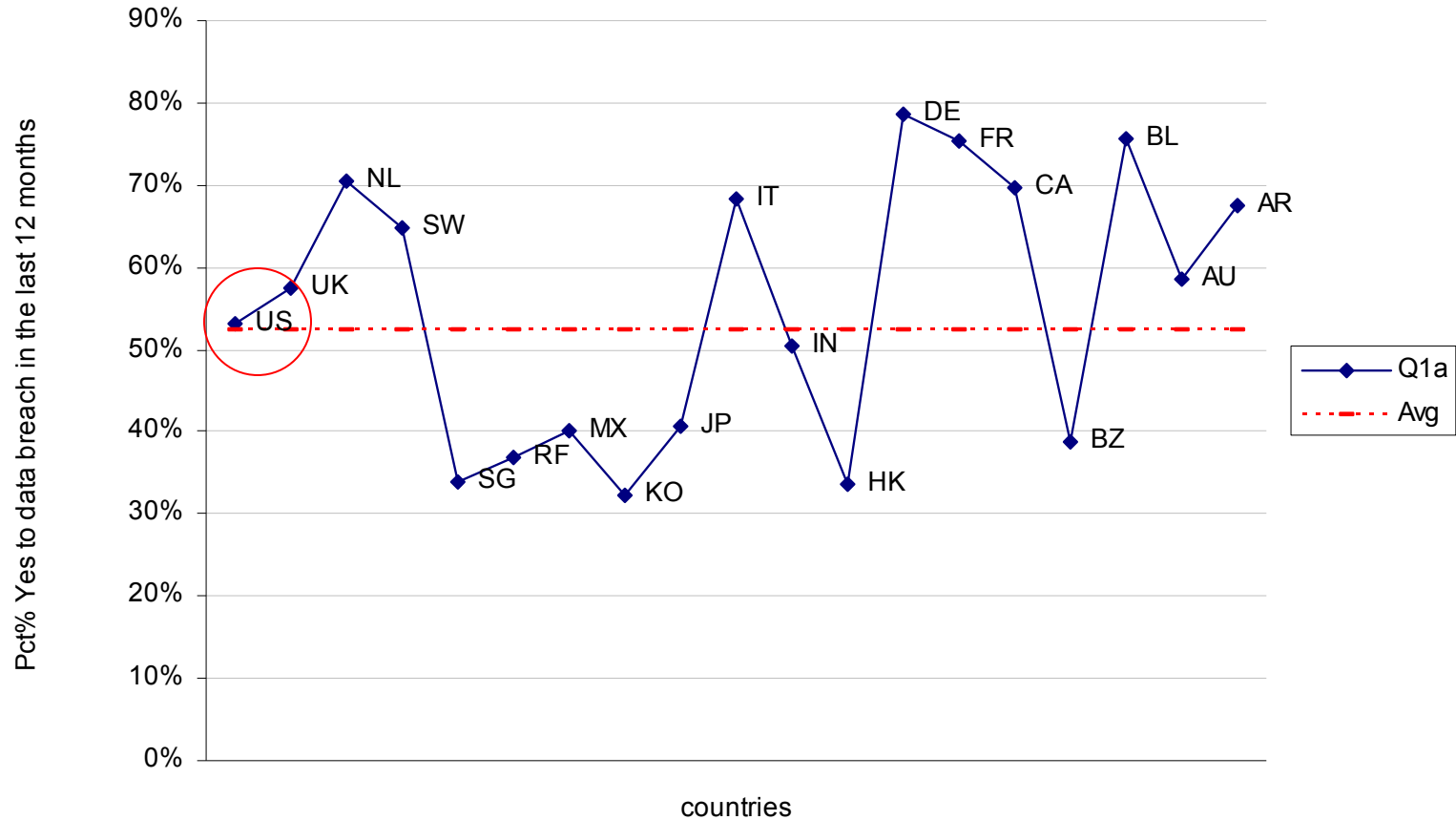
Six response bubbles:

The results of the survey suggest six discernible patterns or “bubbles” of responses based on two criteria: privacy advocacy and data security/compliance.

Country orientations	Lower privacy orientation	Higher privacy orientation
Higher data security orientation	 SG, KO, JP, HK	 US AU UK  DE, SW BL, NL CA
Lower data security orientation	 IN RF  BZ, AR MX	 FR IT

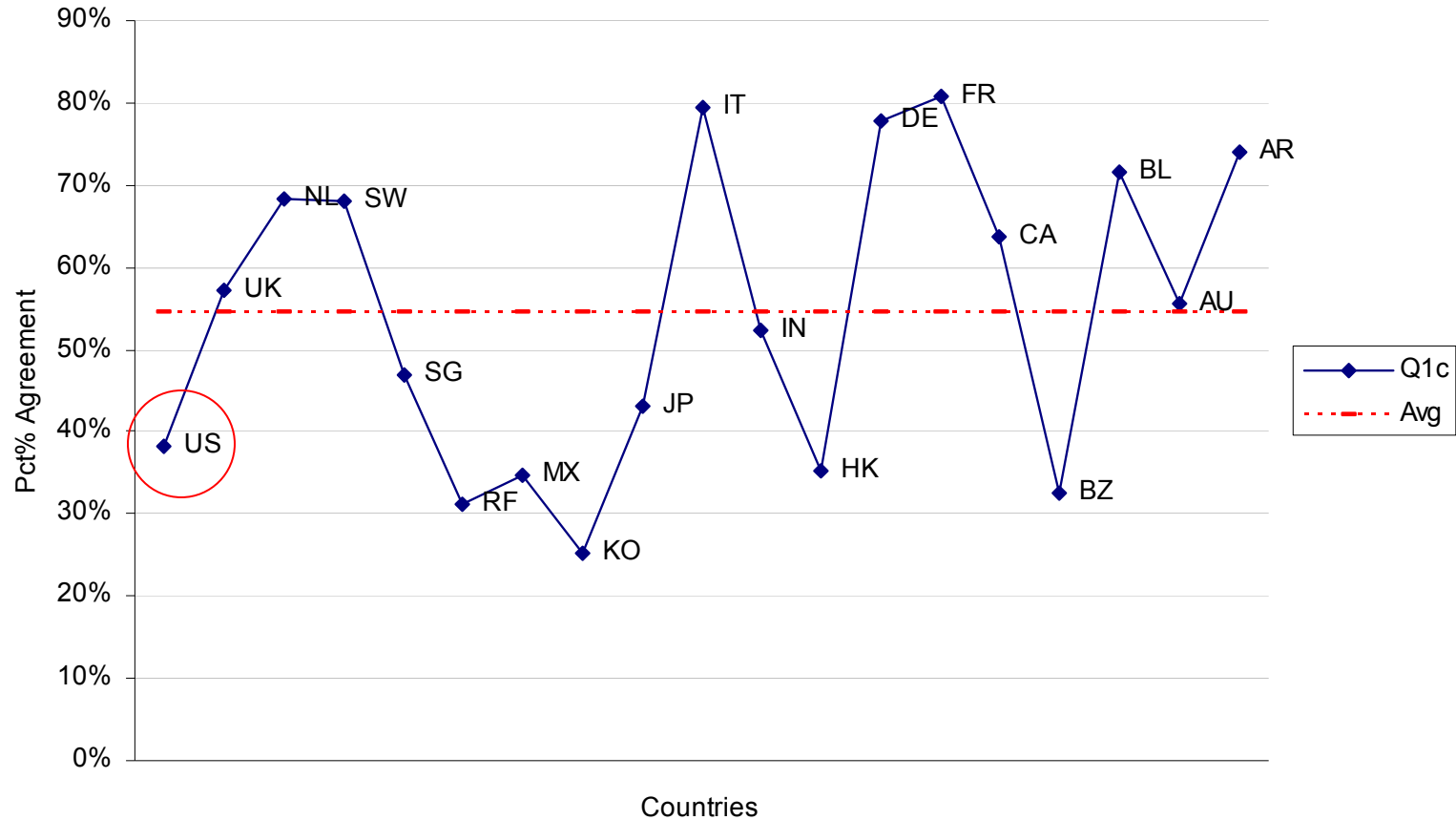
Q1a. Consumers have a right to control information collected about them and their family.

Percentage = strongly agree and agree combined.



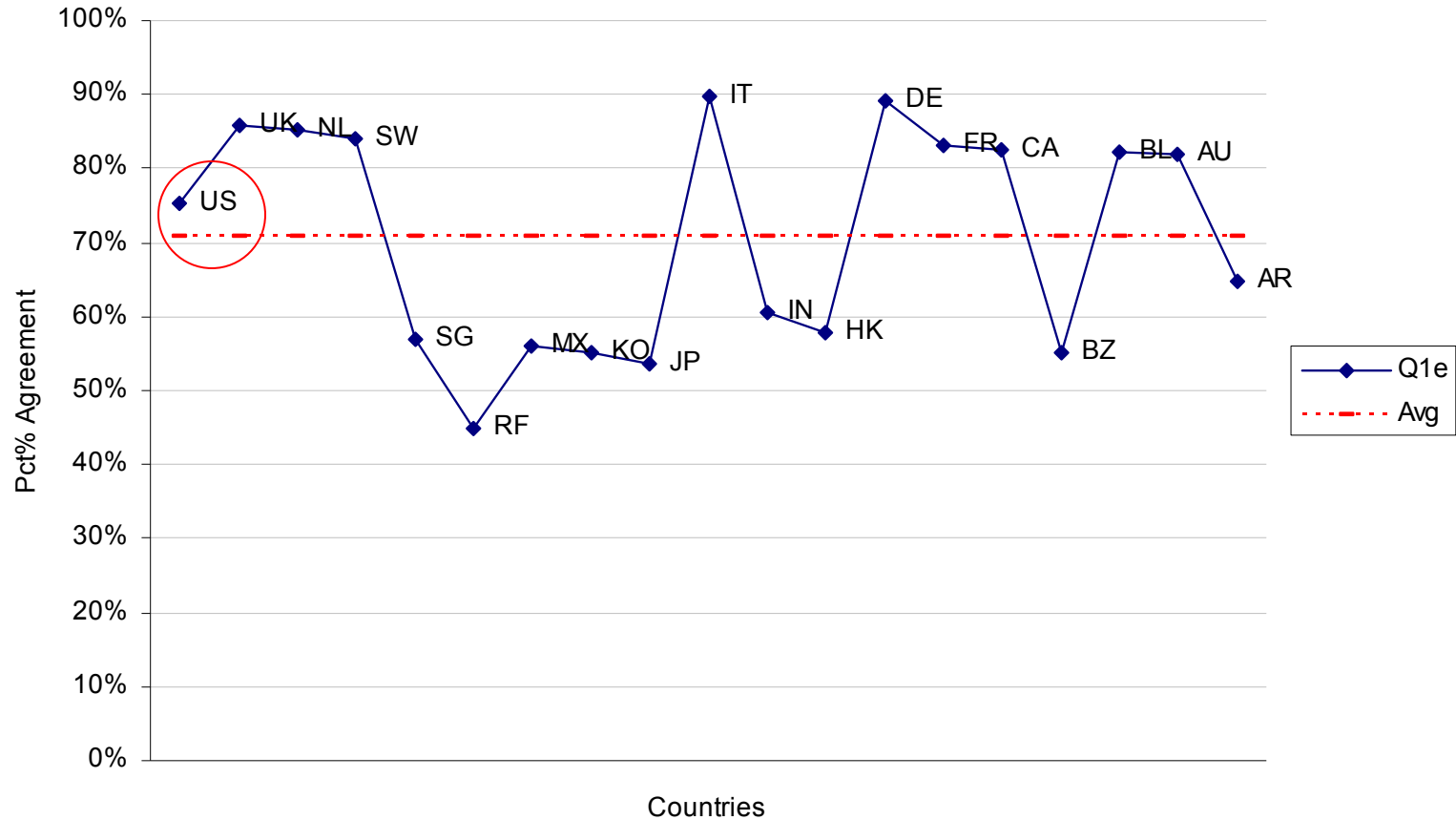
Q1c. Consumers have a right to access and review their personal information collected and used by organizations.

Percentage = strongly agree and agree combined.



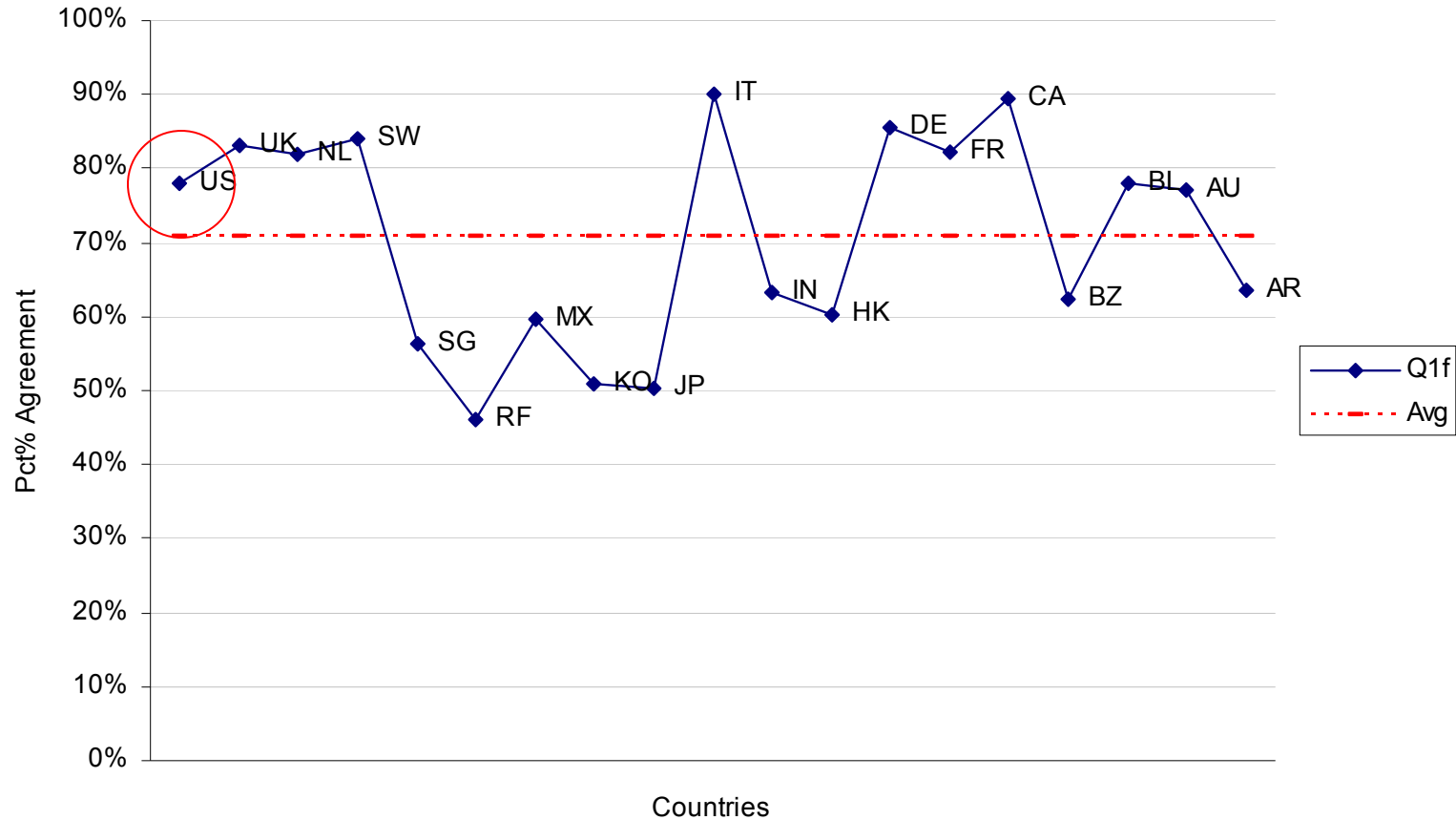
Q1e. Organizations have an obligation to take reasonable steps to secure consumers' personal information.

Percentage = strongly agree and agree combined.



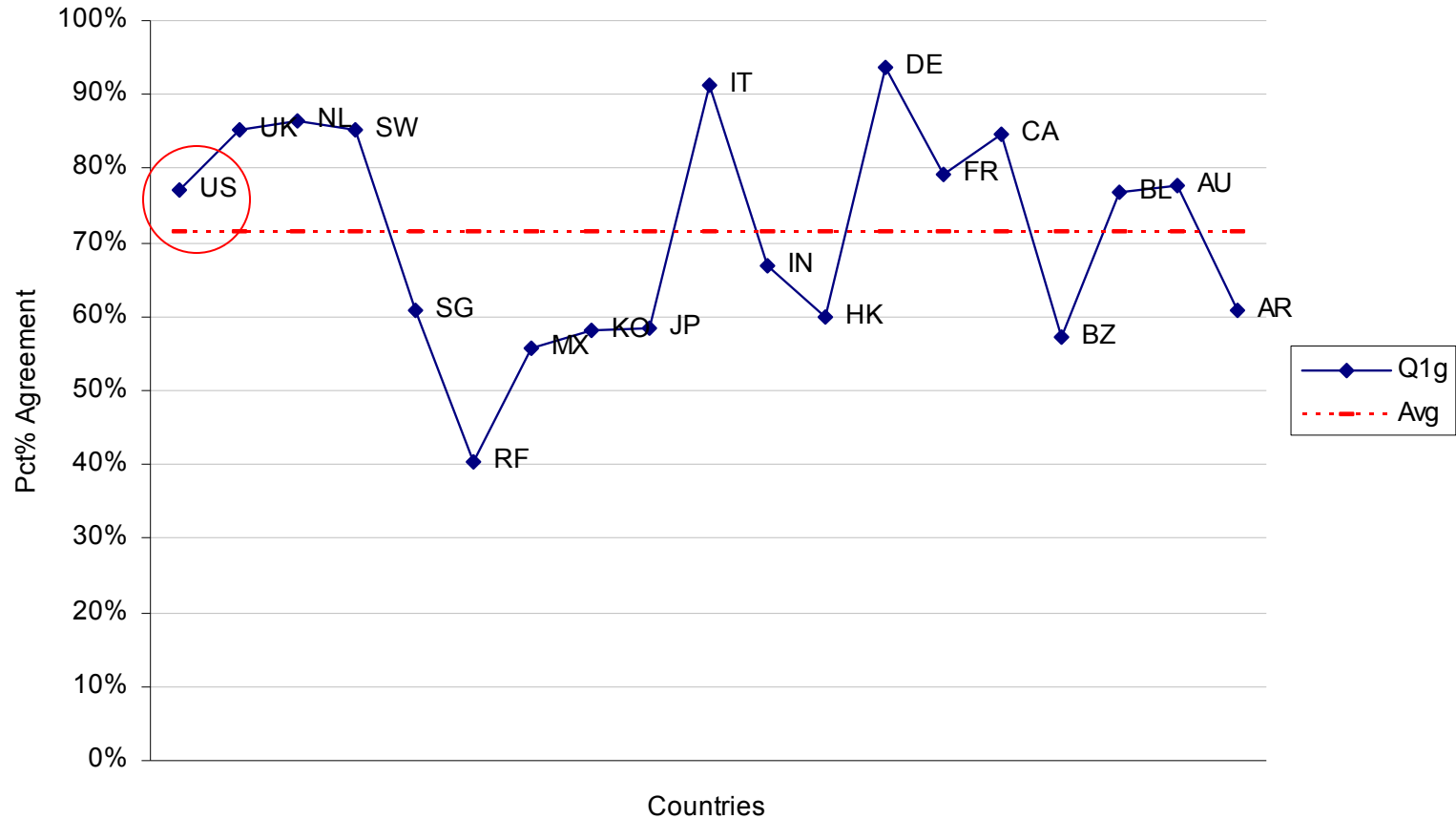
Q1f. Organizations have an obligation to control who has access to consumers' personal information.

Percentage = strongly agree and agree combined.



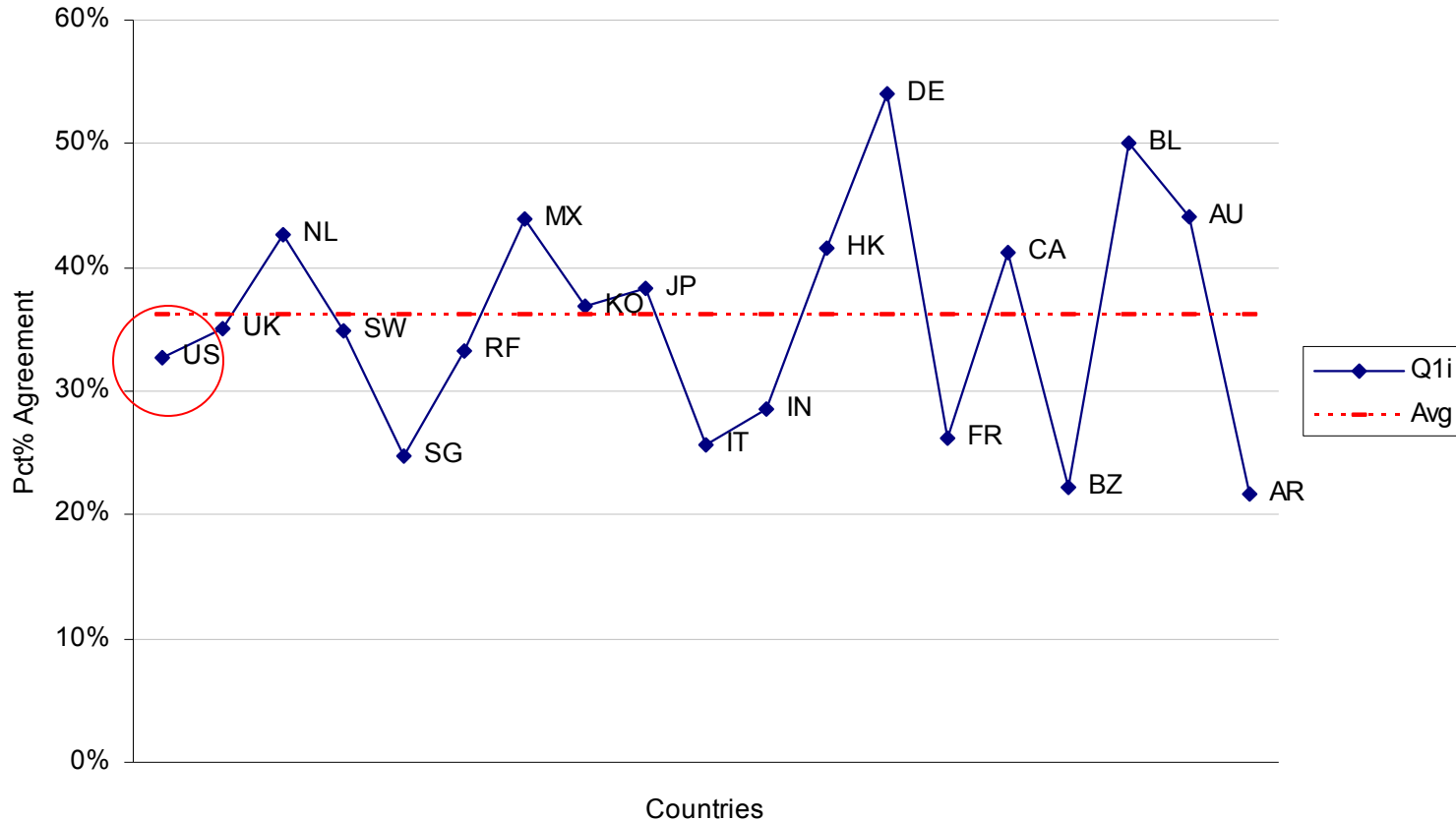
Q1g. Organizations have an obligation to disclose to consumers how their personal information is used.

Percentage = strongly agree and agree combined.



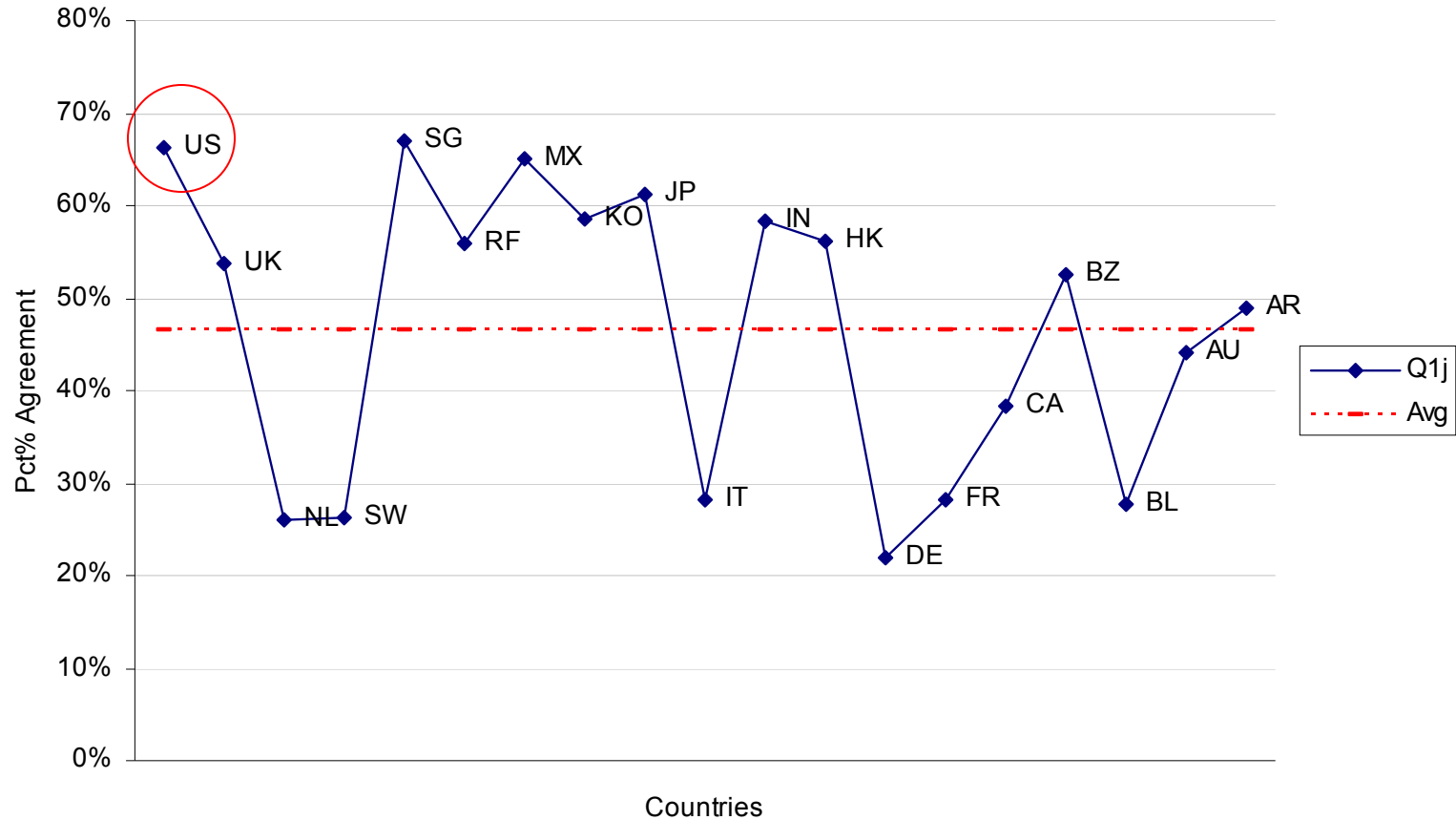
Q1i. Government regulations are necessary to protect consumers' personal information.

Percentage = strongly agree and agree combined.



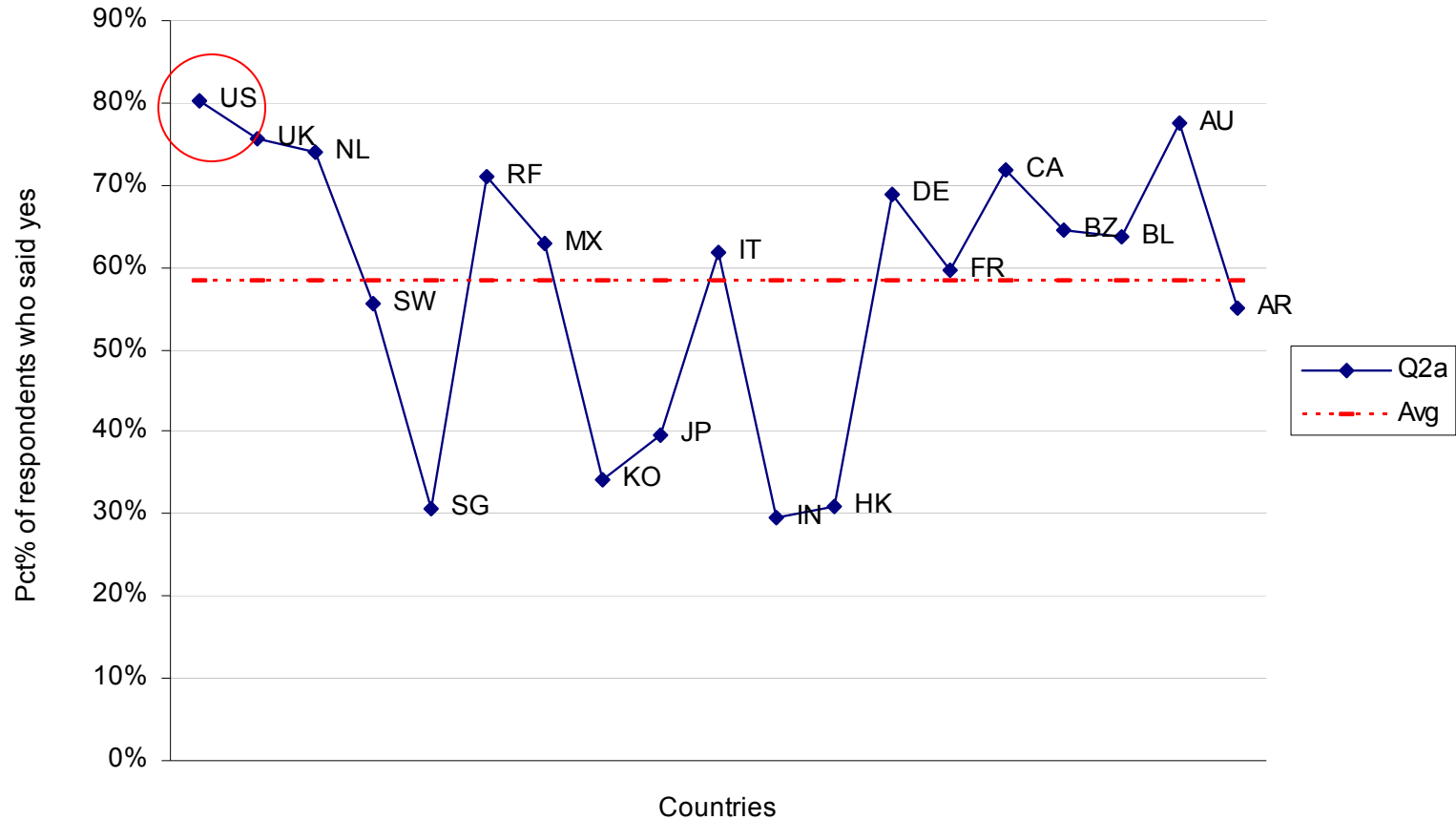
Q1j. The information consumers willingly share with business organizations is no longer owned by them.

Percentage = strongly agree and agree combined.



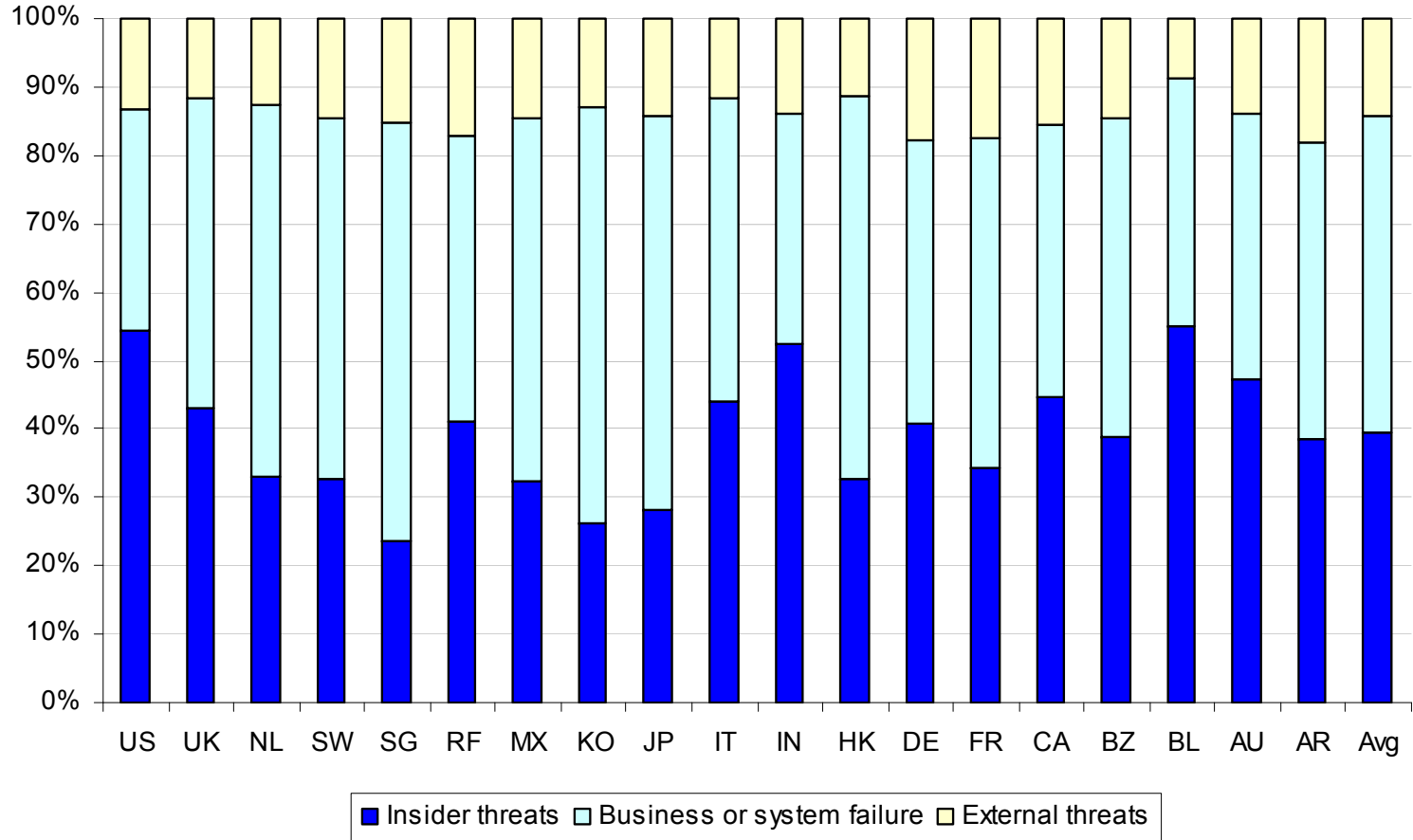
Q2a. Did your organization ever lose sensitive personal information – such as data about consumers, customers, employees or others?

Percentage = Yes response.



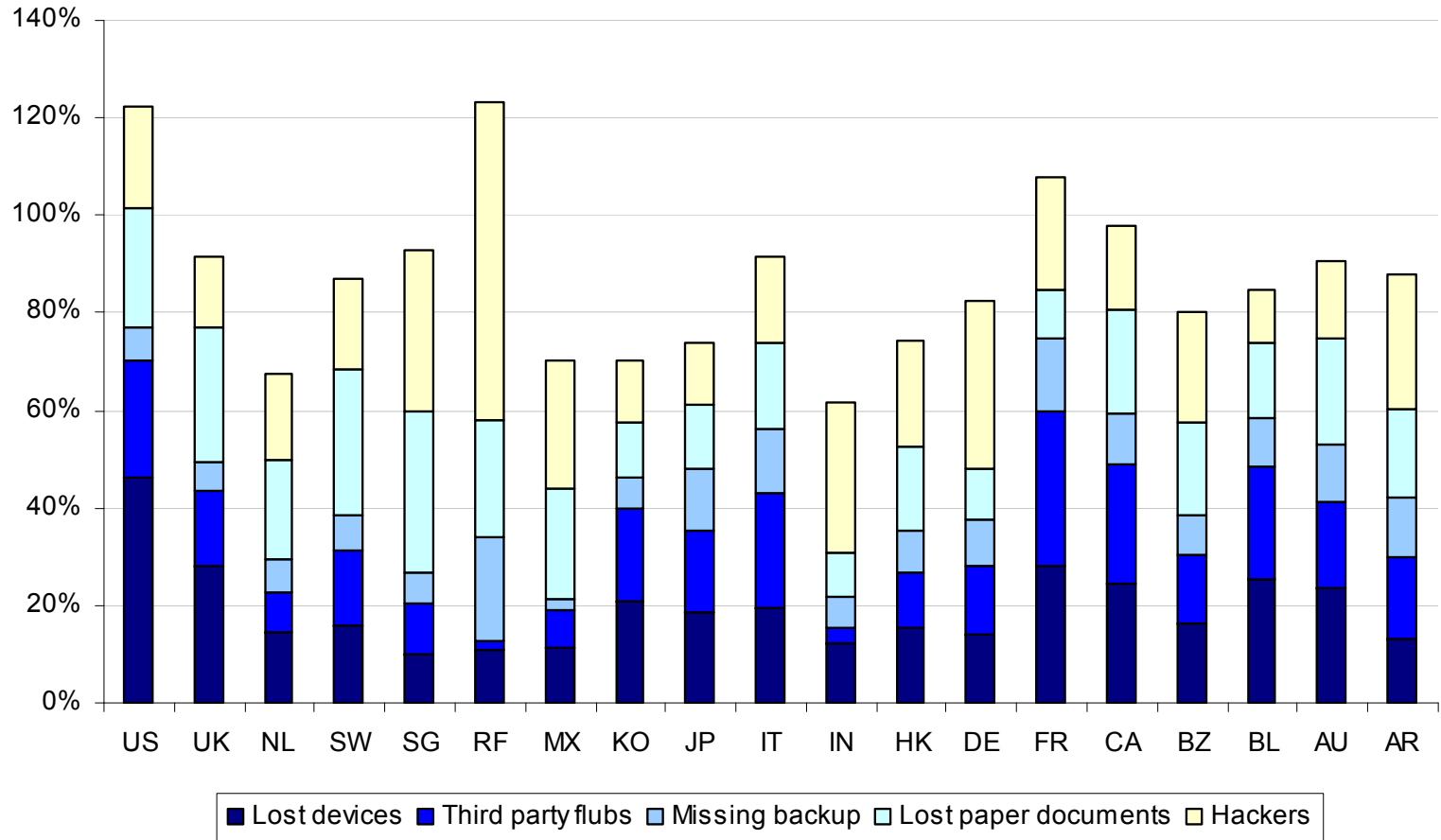
Q2c. If yes, why have these data breaches occurred in your company?

Three threat vectors = insider threats, business or system failures and external threats (percentage).



Q2d. If yes, how has your company lost personal information?

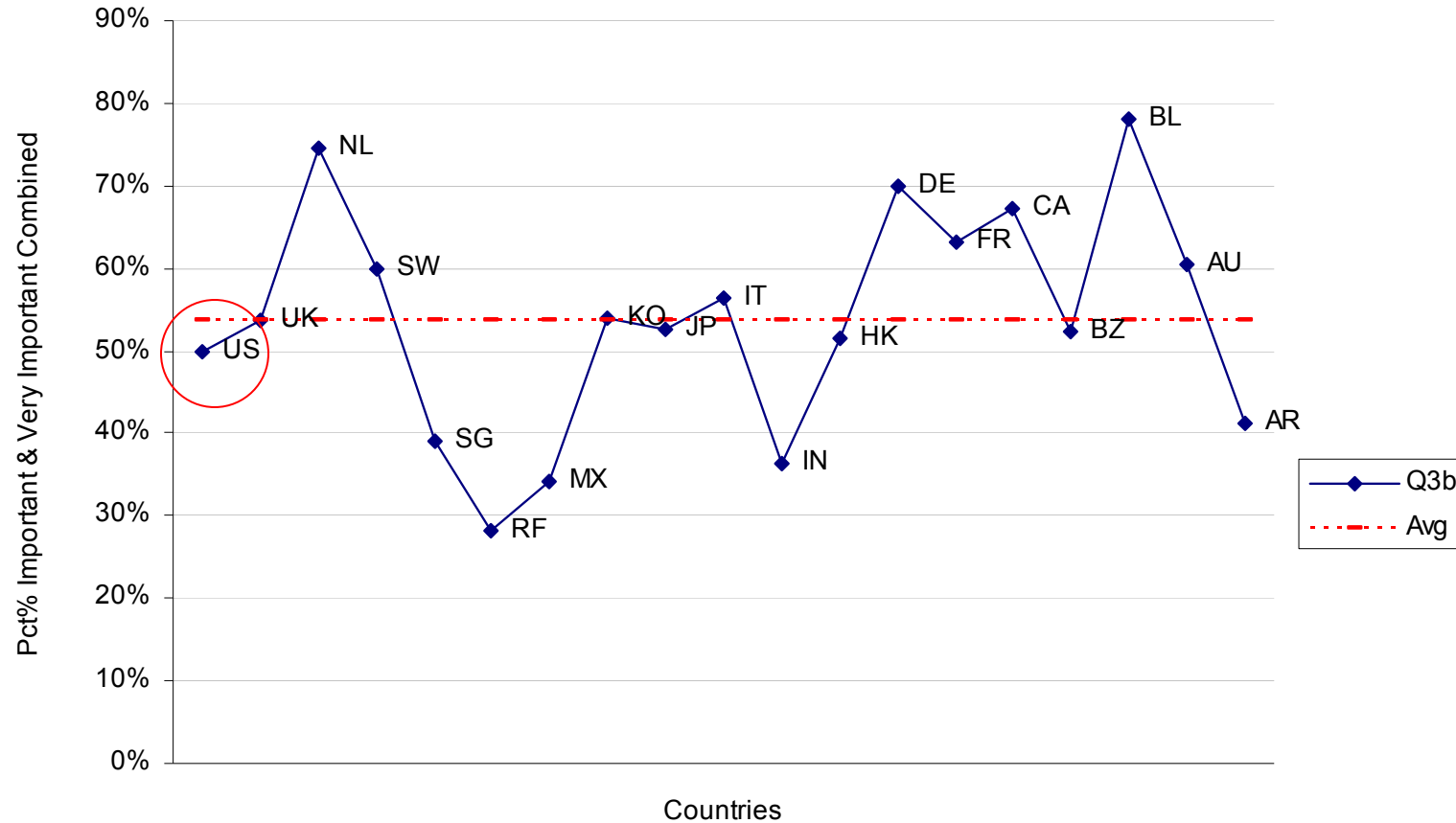
Five root causes = lost devices, third party flubs, missing backup, lost paper documents and hackers (percentage).



Key privacy goal for business

Q3b. Limiting the sharing of sensitive personal information.

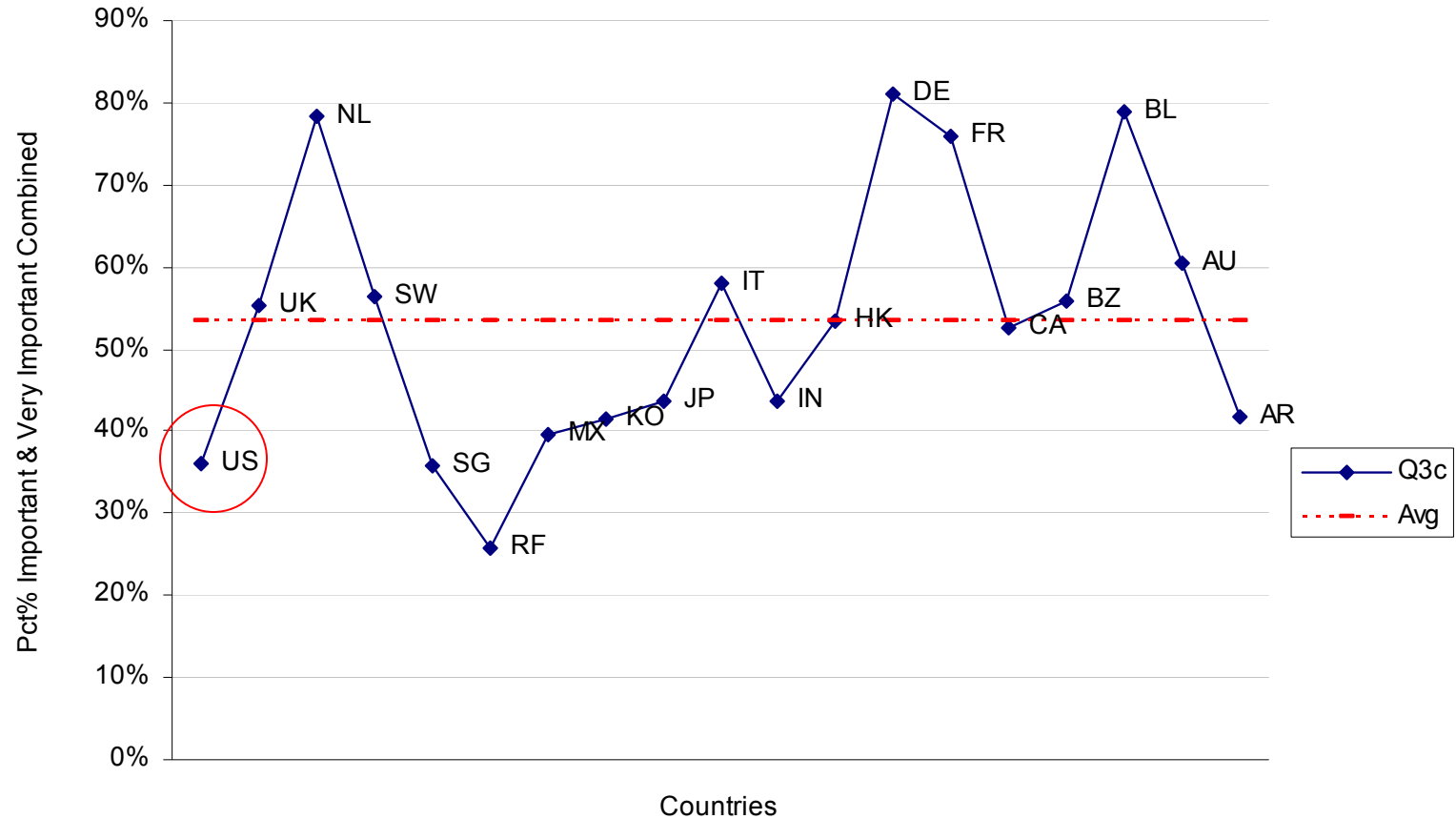
Percentage = very important and important combined.



Key privacy goal for business

Q3c. Protecting consumer privacy rights.

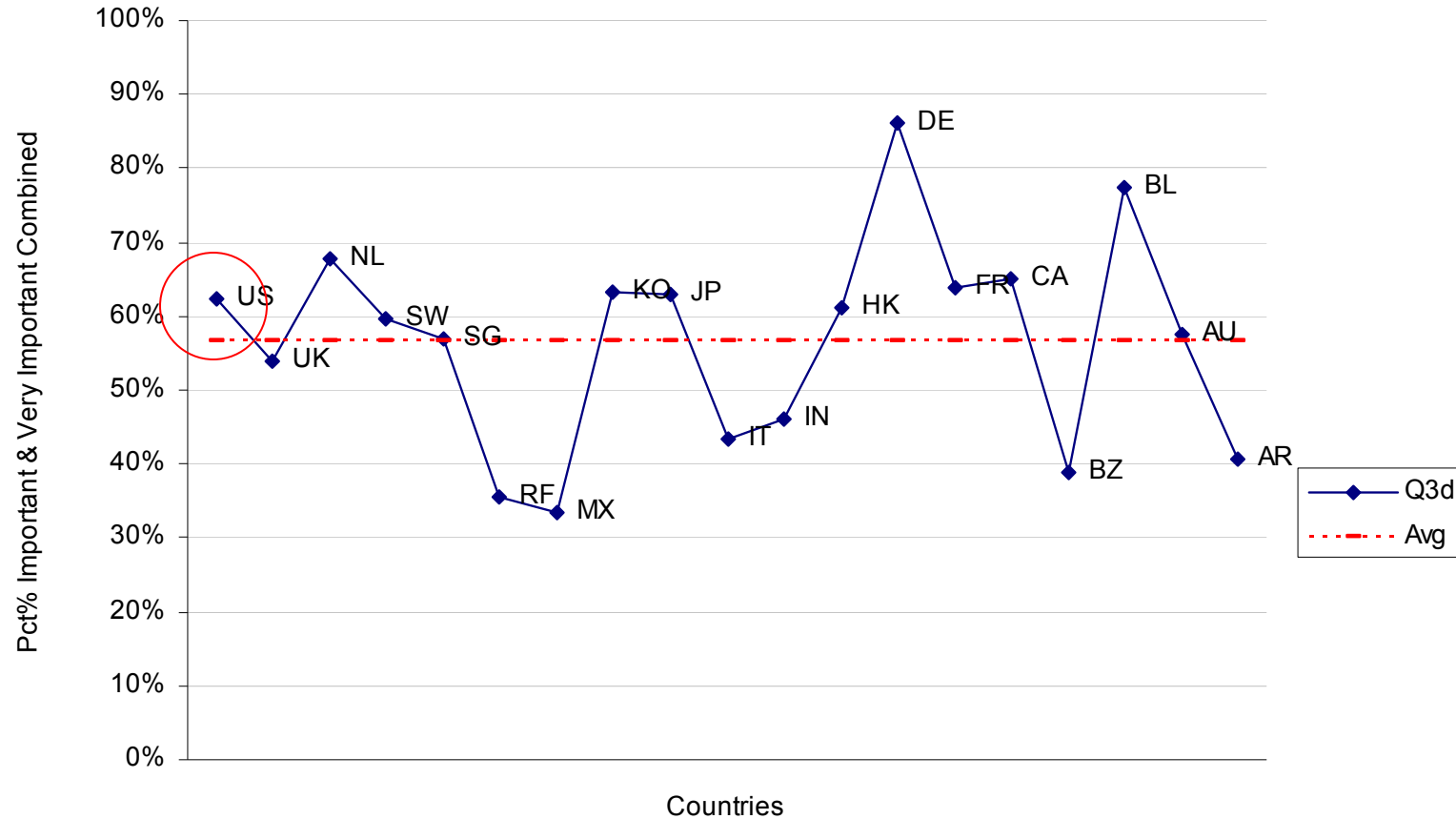
Percentage = very important and important combined.



Key privacy goal for business

Q3d. Avoiding regulatory and compliance violations.

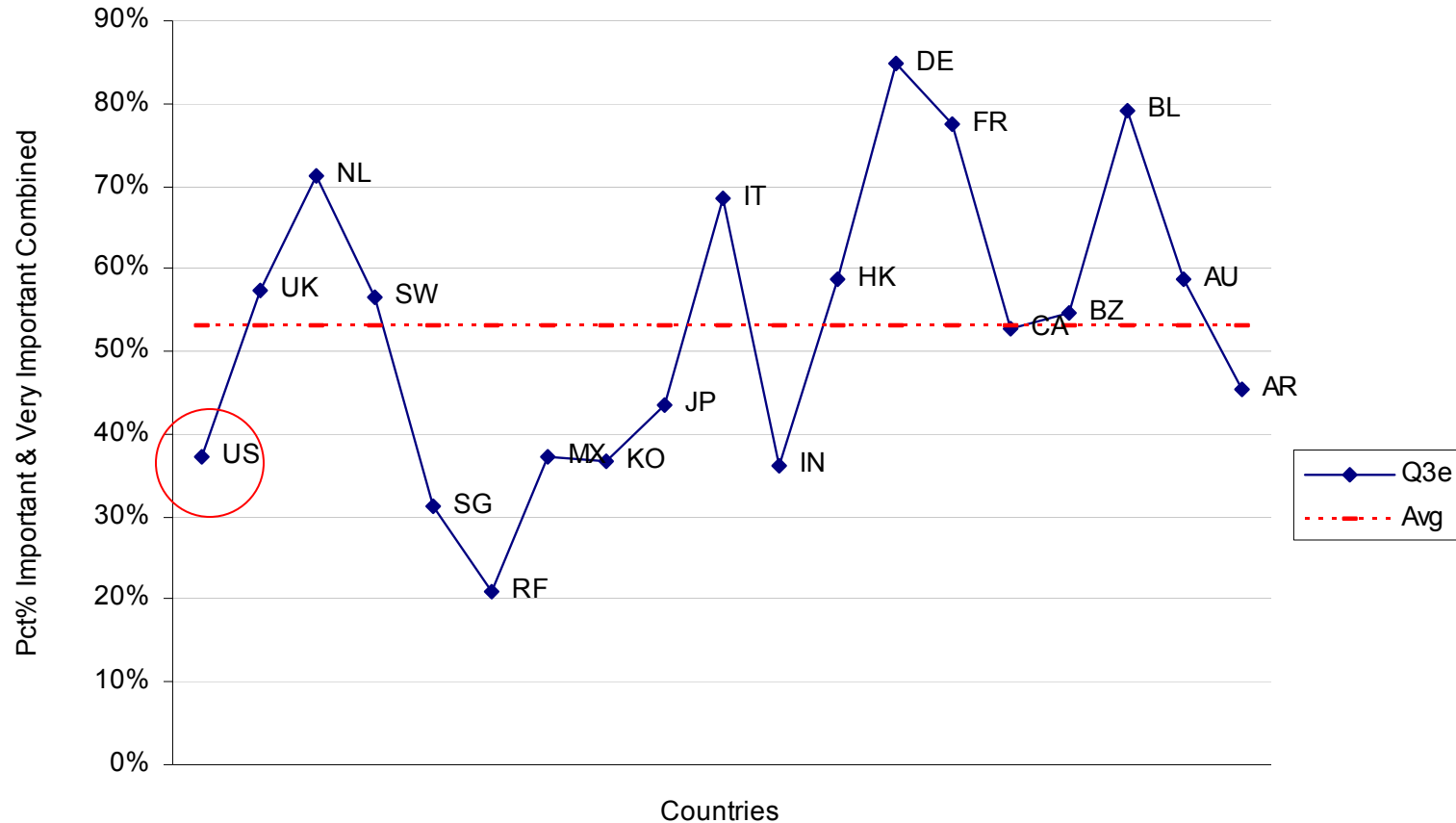
Percentage = very important and important combined.



Key privacy goal for business

Q3e. Preventing cross-border transfers of personal information to countries with insufficient privacy laws.

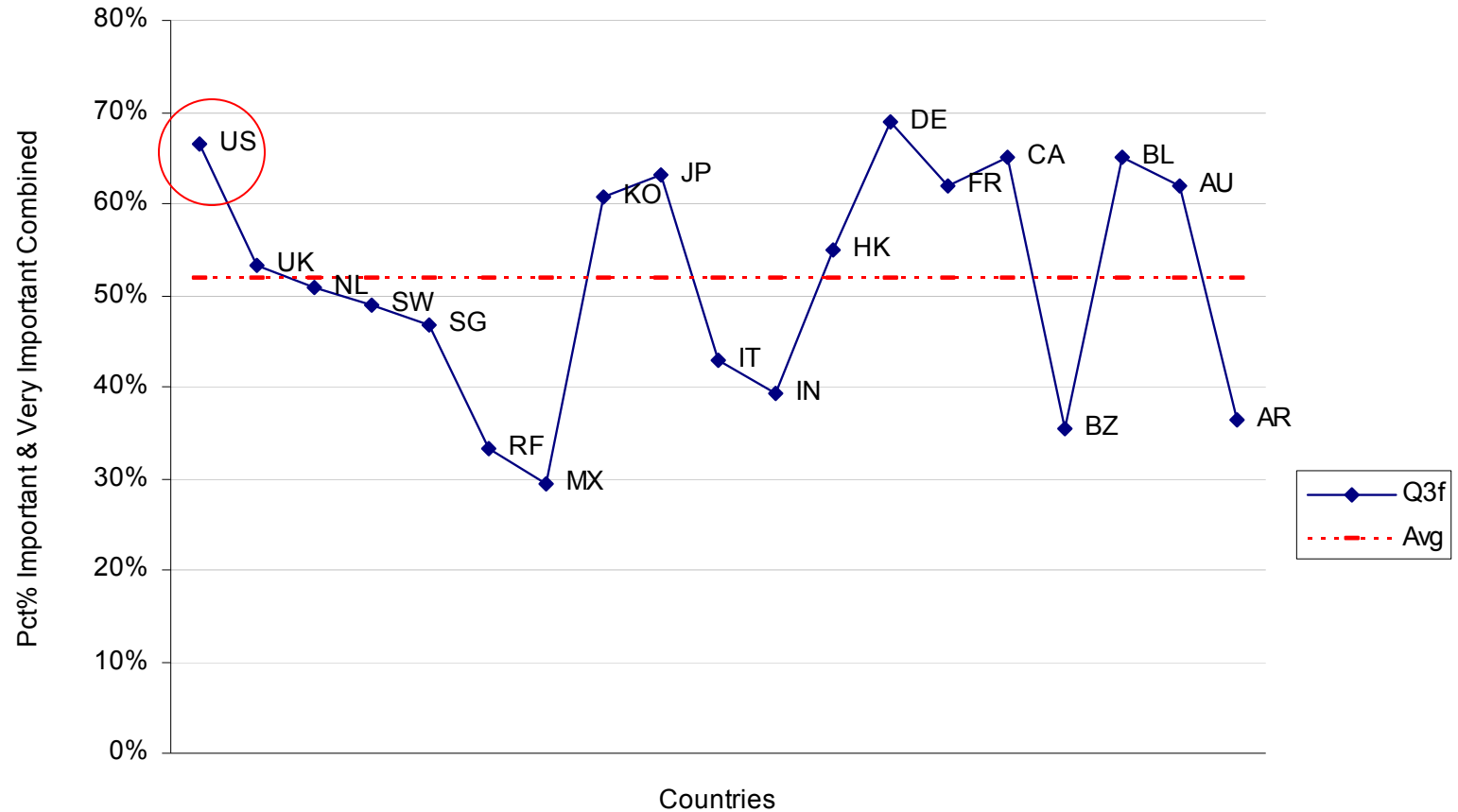
Percentage = very important and important combined.



Key privacy goal for business

Q3f. Preventing cyber crimes against consumers including identity theft.

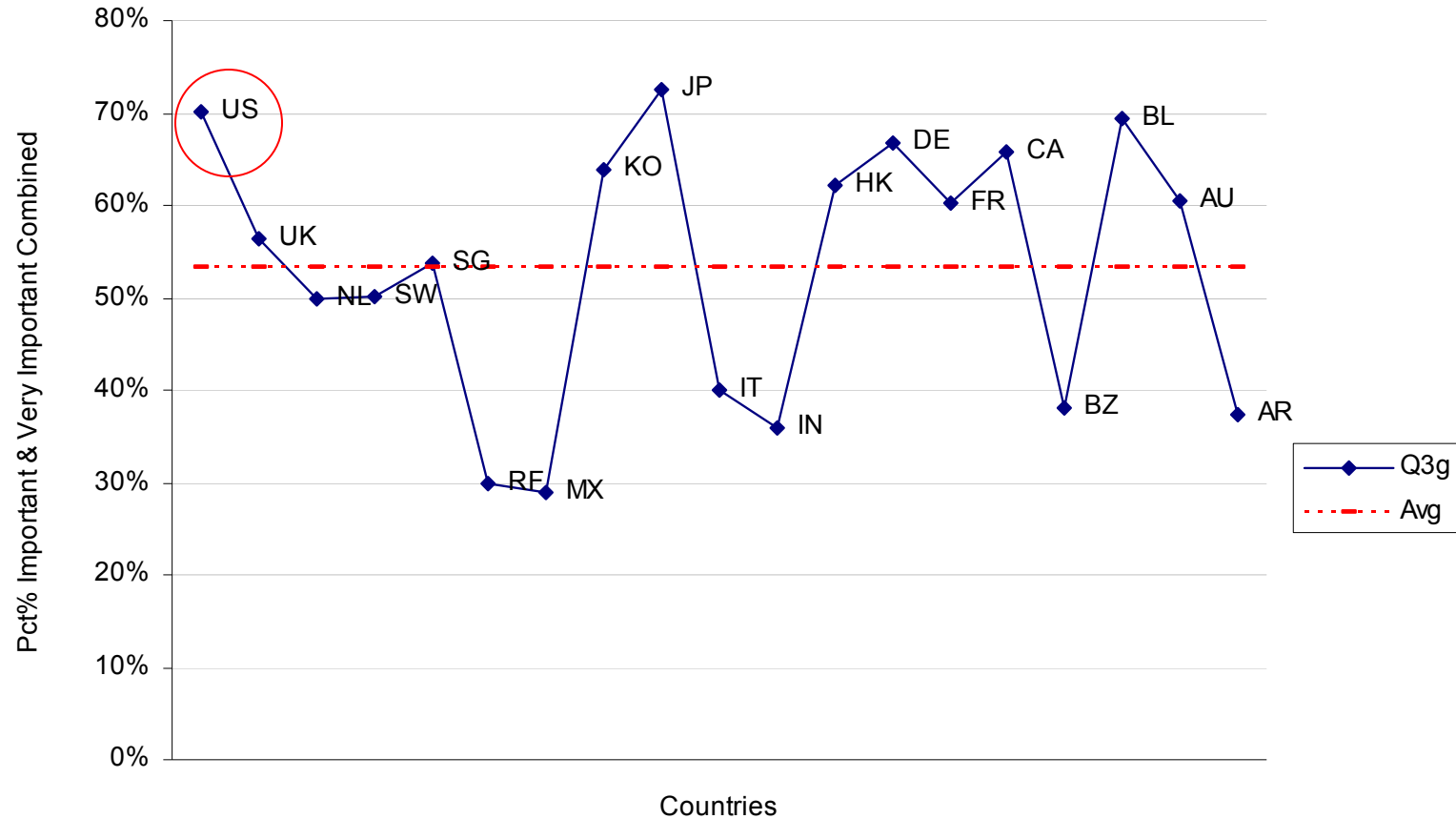
Percentage = very important and important combined.



Key privacy goal for business

Q3g. Preventing data loss or theft.

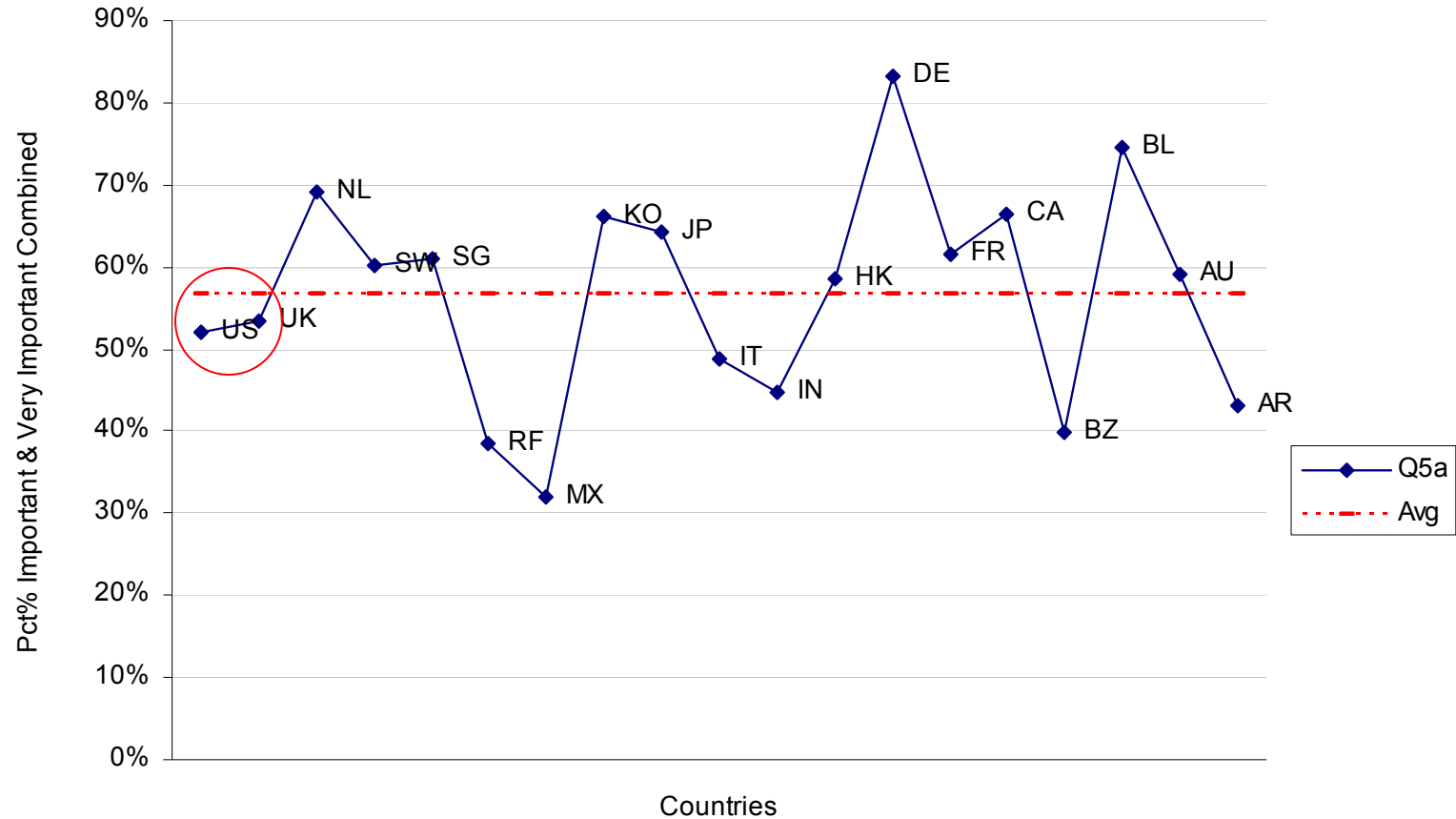
Percentage = very important and important combined.



Key privacy goal for business

Q5a. Disclosure – have a policy about its privacy practices.

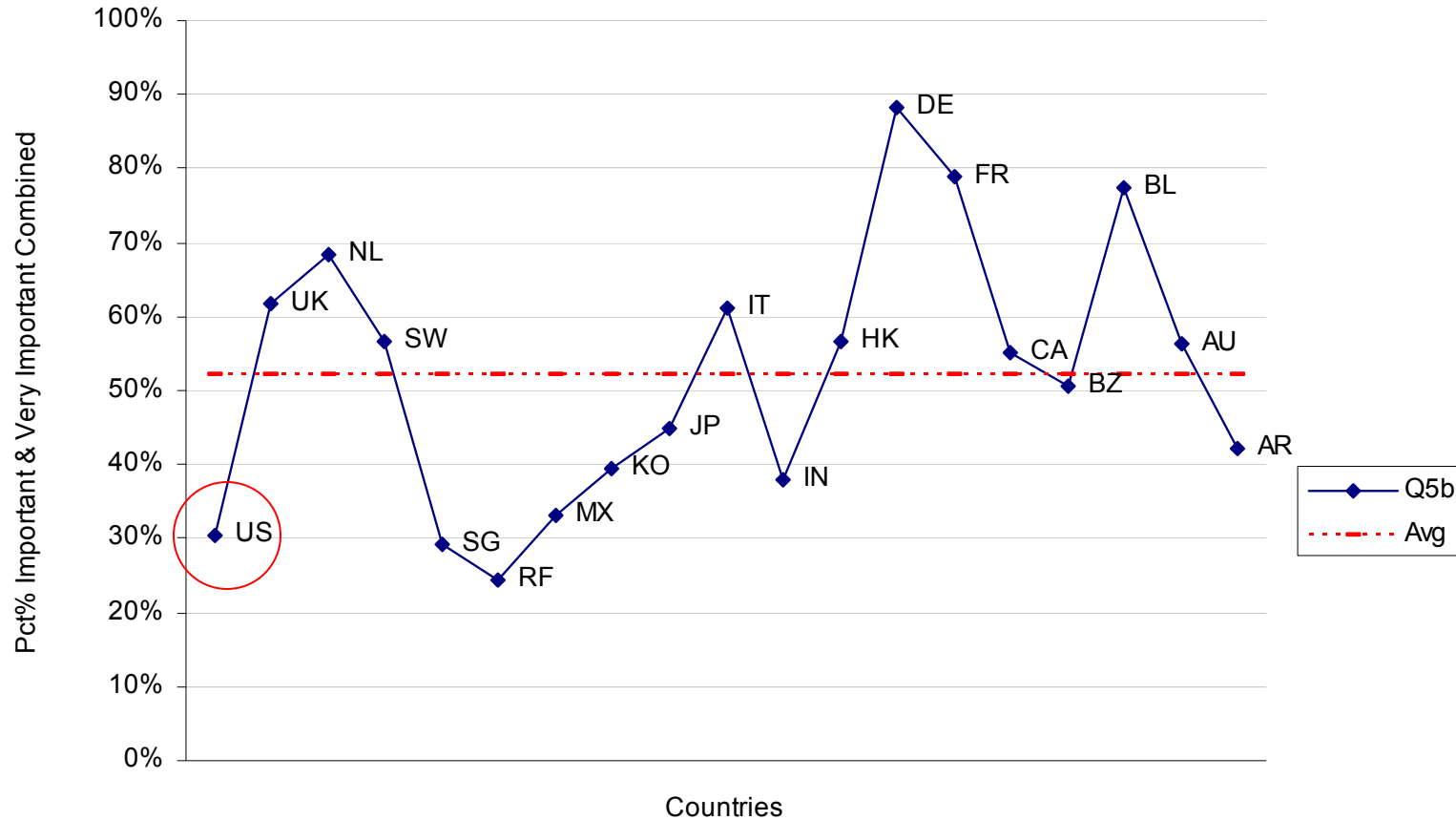
Percentage = very important and important combined.



Key privacy goal for business

Q5b. Consent – obtain permission from consumers or customers before using or sharing personal information.

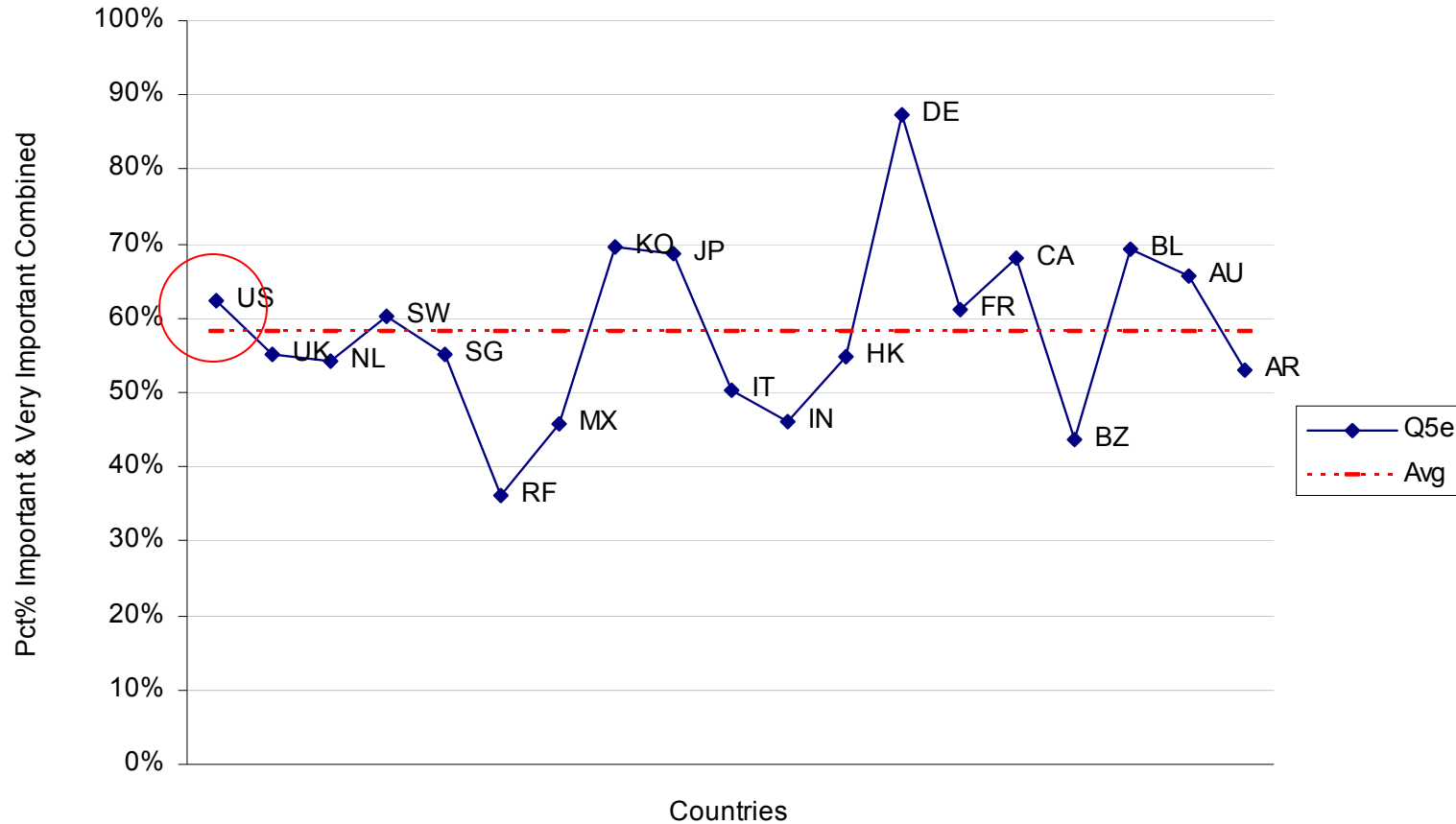
Percentage = very important and important combined.



Key privacy goal for business

Q5e. Security – adequately protect and secure consumer or customer’s personal information.

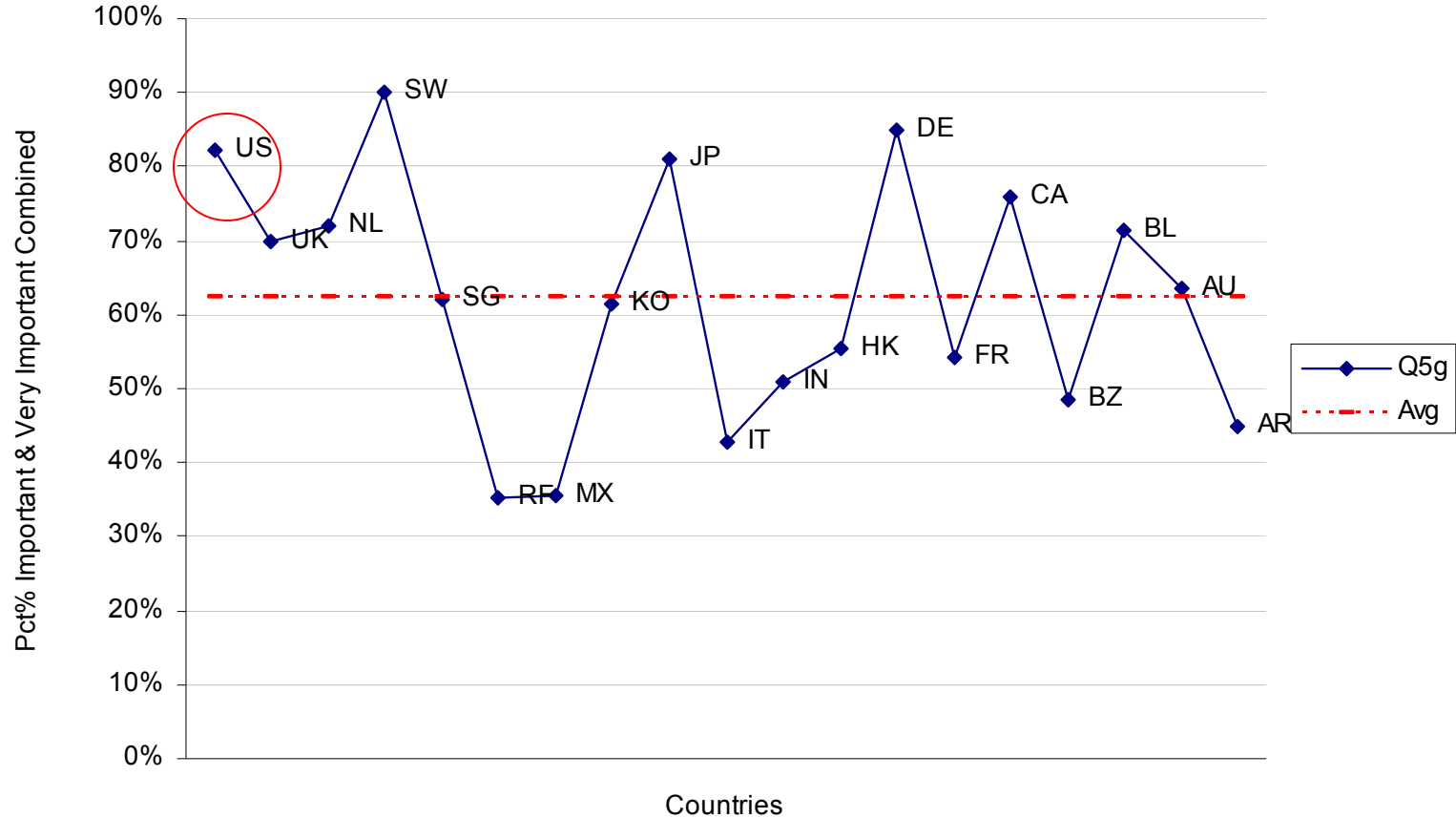
Percentage = very important and important combined.



Key privacy goal for business

Q5g. Accuracy – ensuring data collected and used is accurate (not false or misleading).

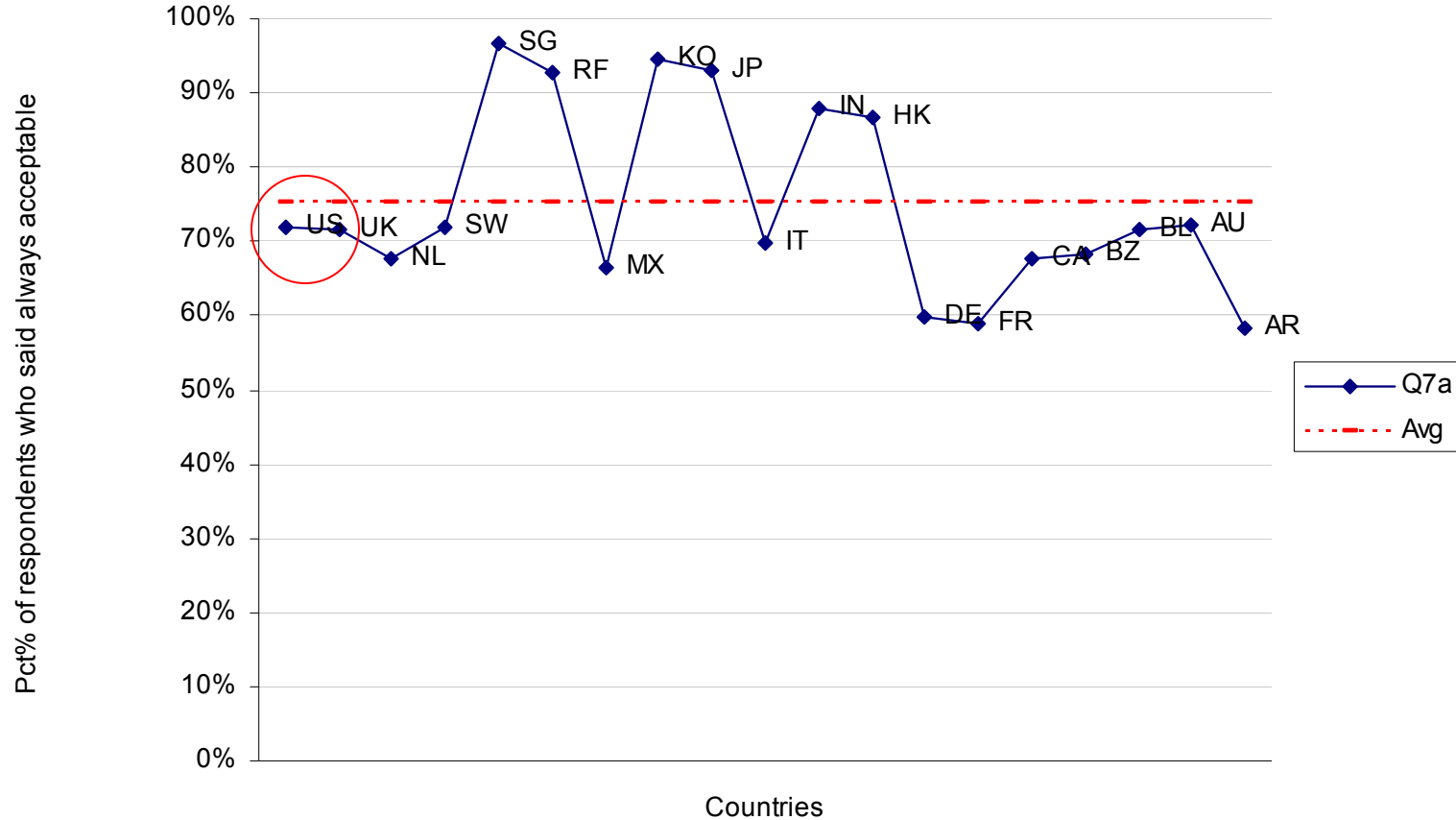
Percentage = very important and important combined.



Acceptable uses of personal information

Q7a. Using information to **identify and authenticate** customers.

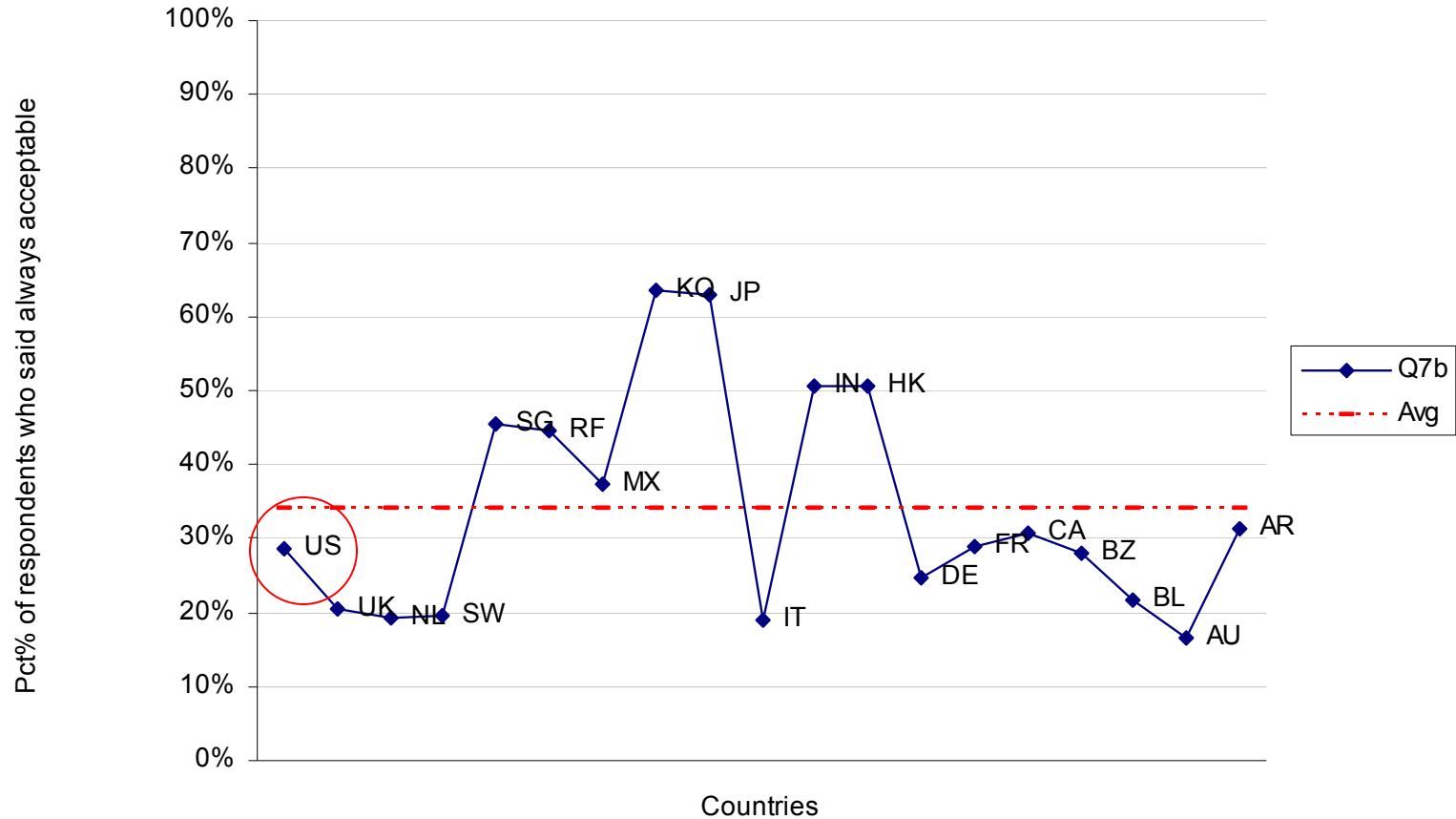
Percentage = respondents who said always acceptable.



Acceptable uses of personal information

Q7b. Using information for **targeted marketing** and promotions.

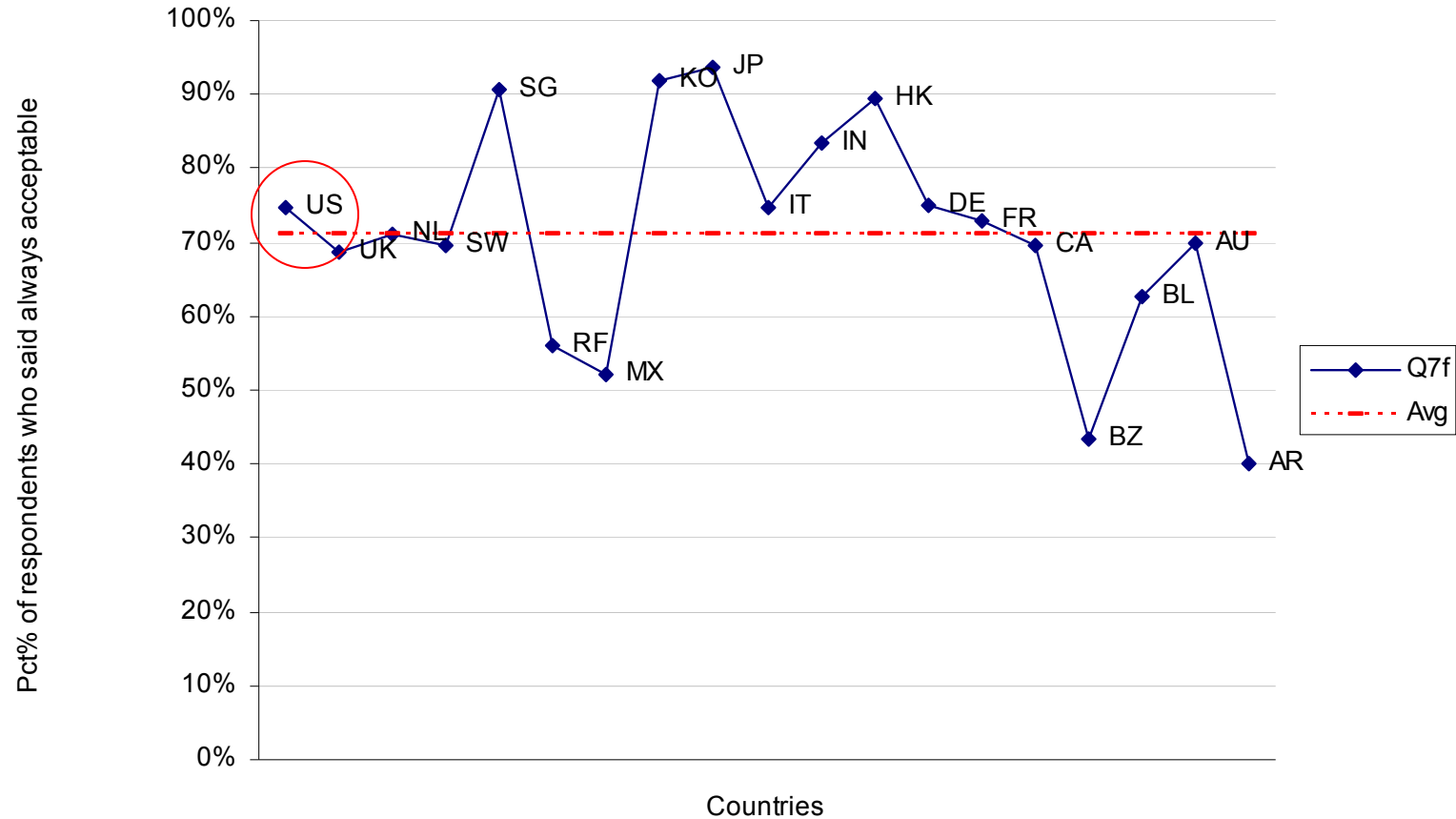
Percentage = respondents who said always acceptable.



Acceptable uses of personal information

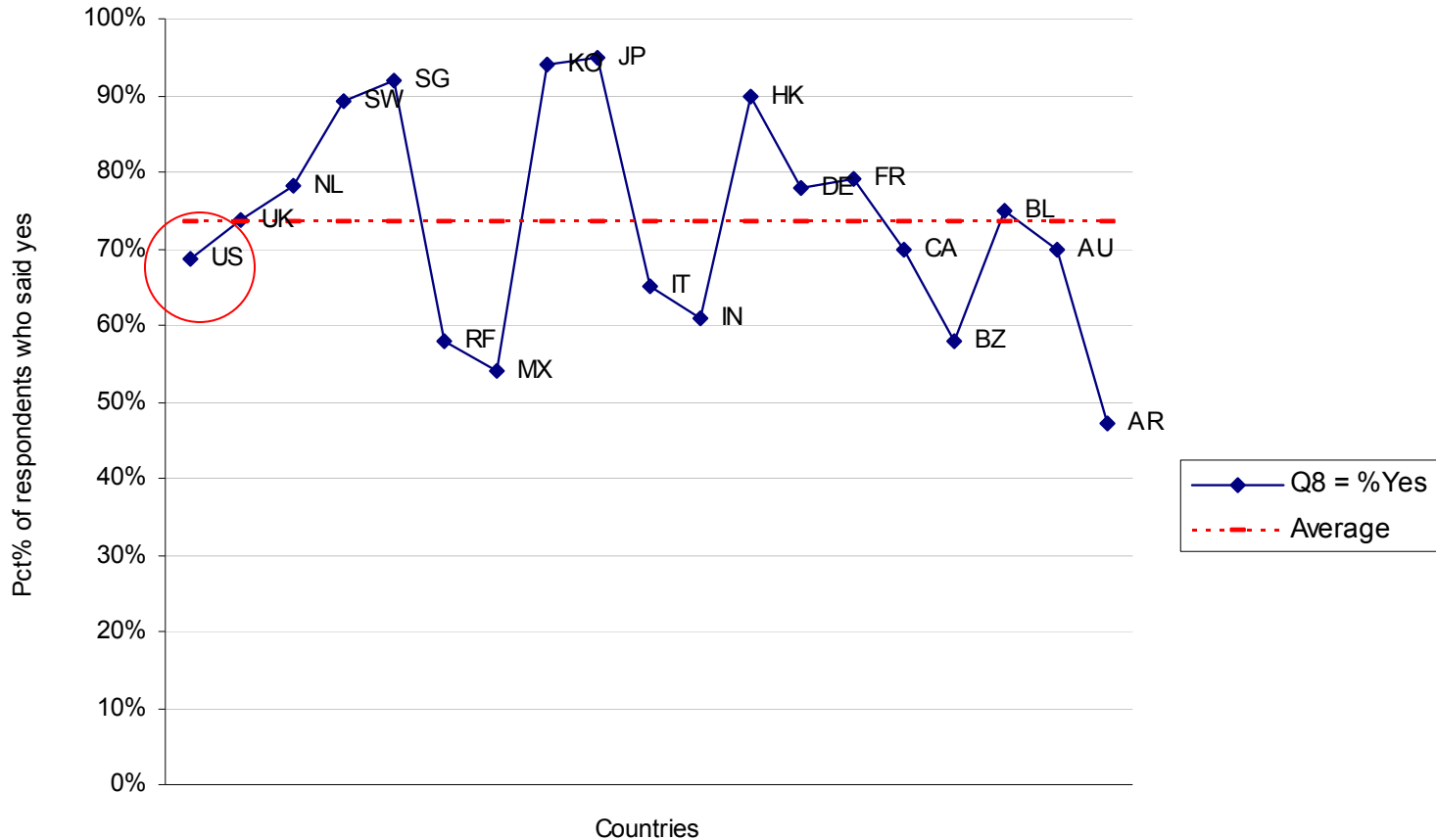
Q7f. Sharing information **with government** for national security purposes.

Percentage = respondents who said always acceptable.



Q8. Do you believe your organization has adequate policies to protect the personally identifiable information it maintains?

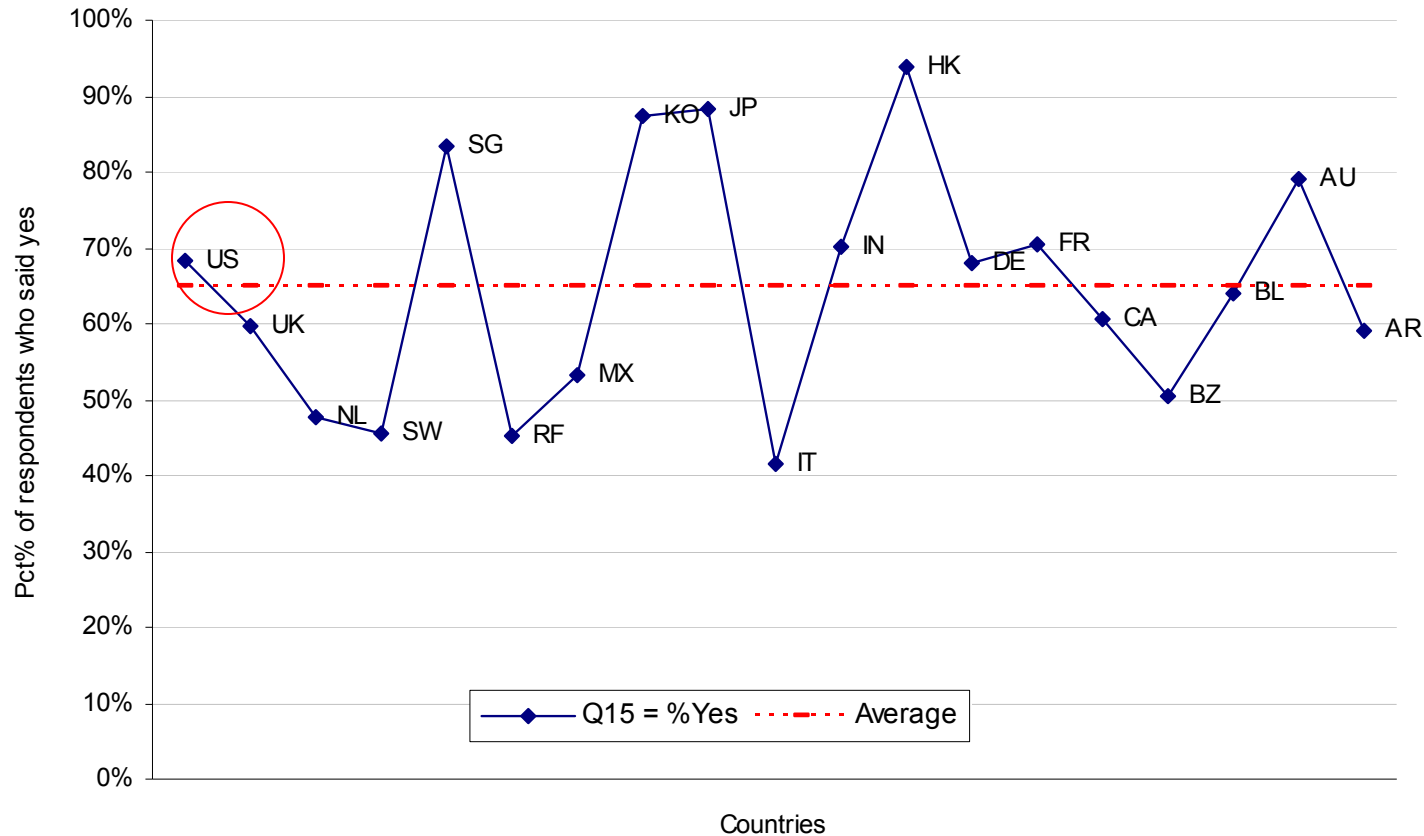
Percentage = Yes response.



Questions about Identity

Q15a. Would you prefer your customers or employees to have one private and secure verification credential that will be accepted by other organizations to verify who they are before providing access to secure records or locations?

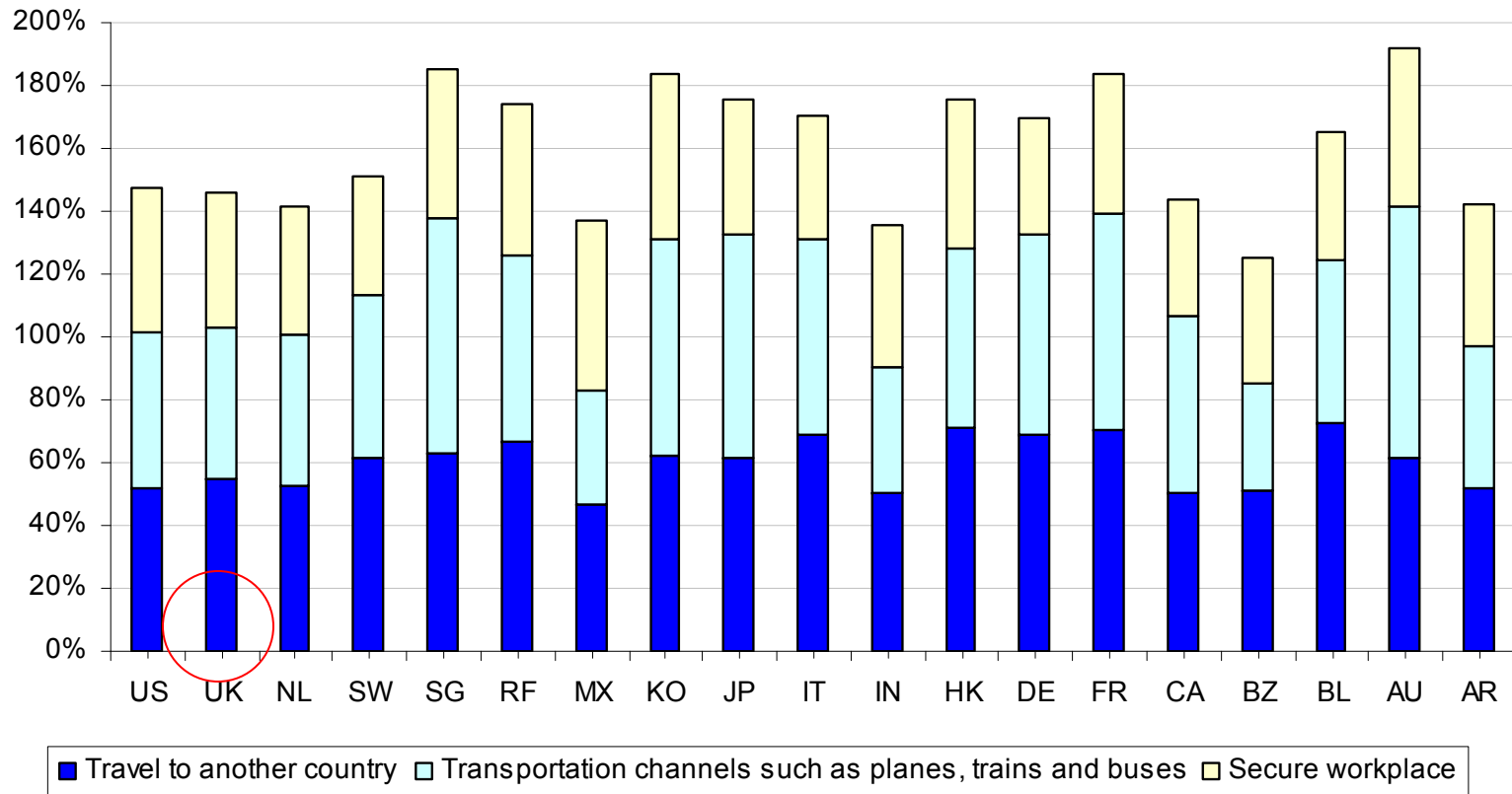
Percentage = Yes response.



Q15b. Please check all functions that you would like a multipurpose ID credential to provide access to.

Percentage of top three functional uses.

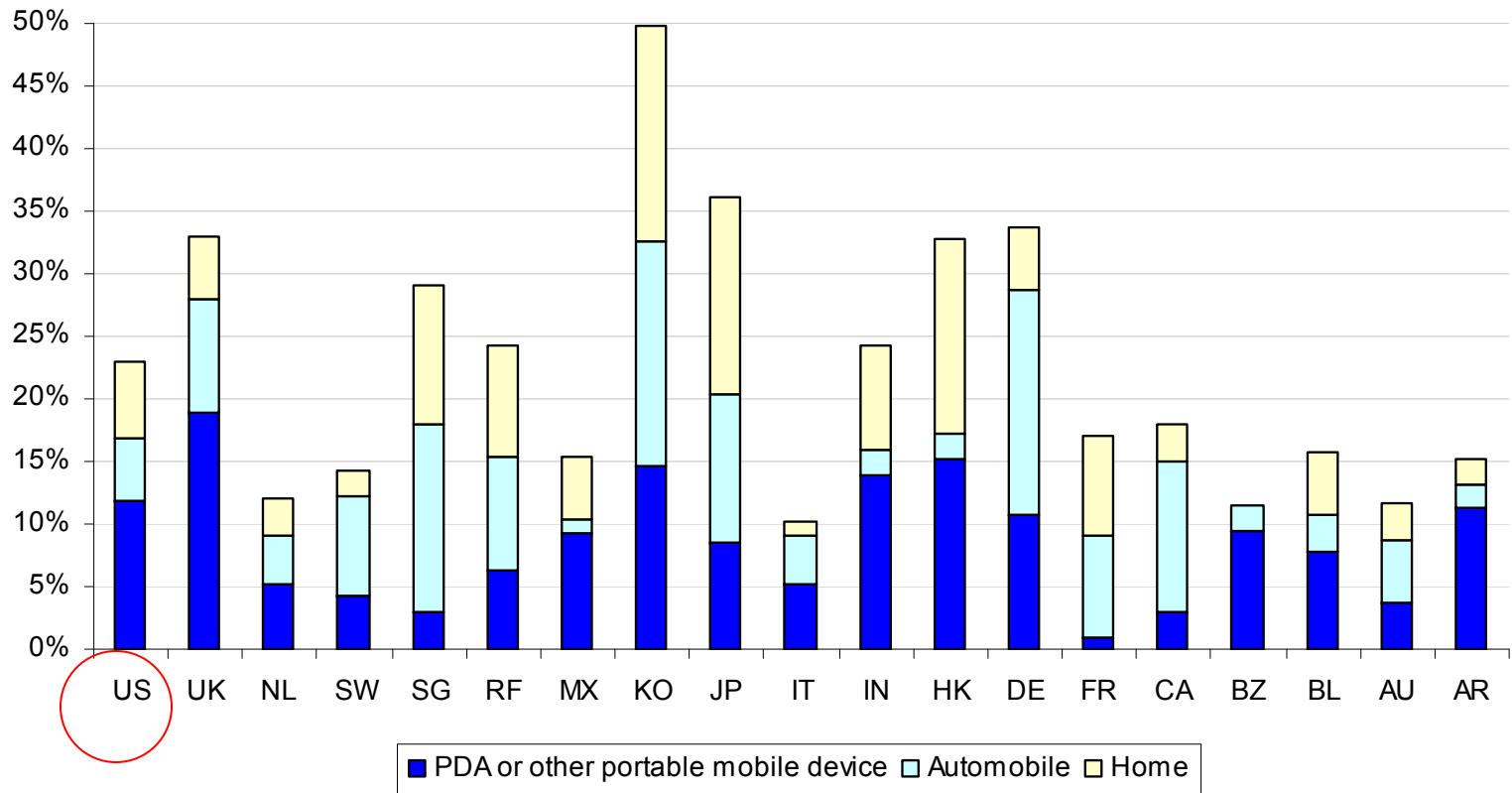
Multipurpose identity credential: Top three uses



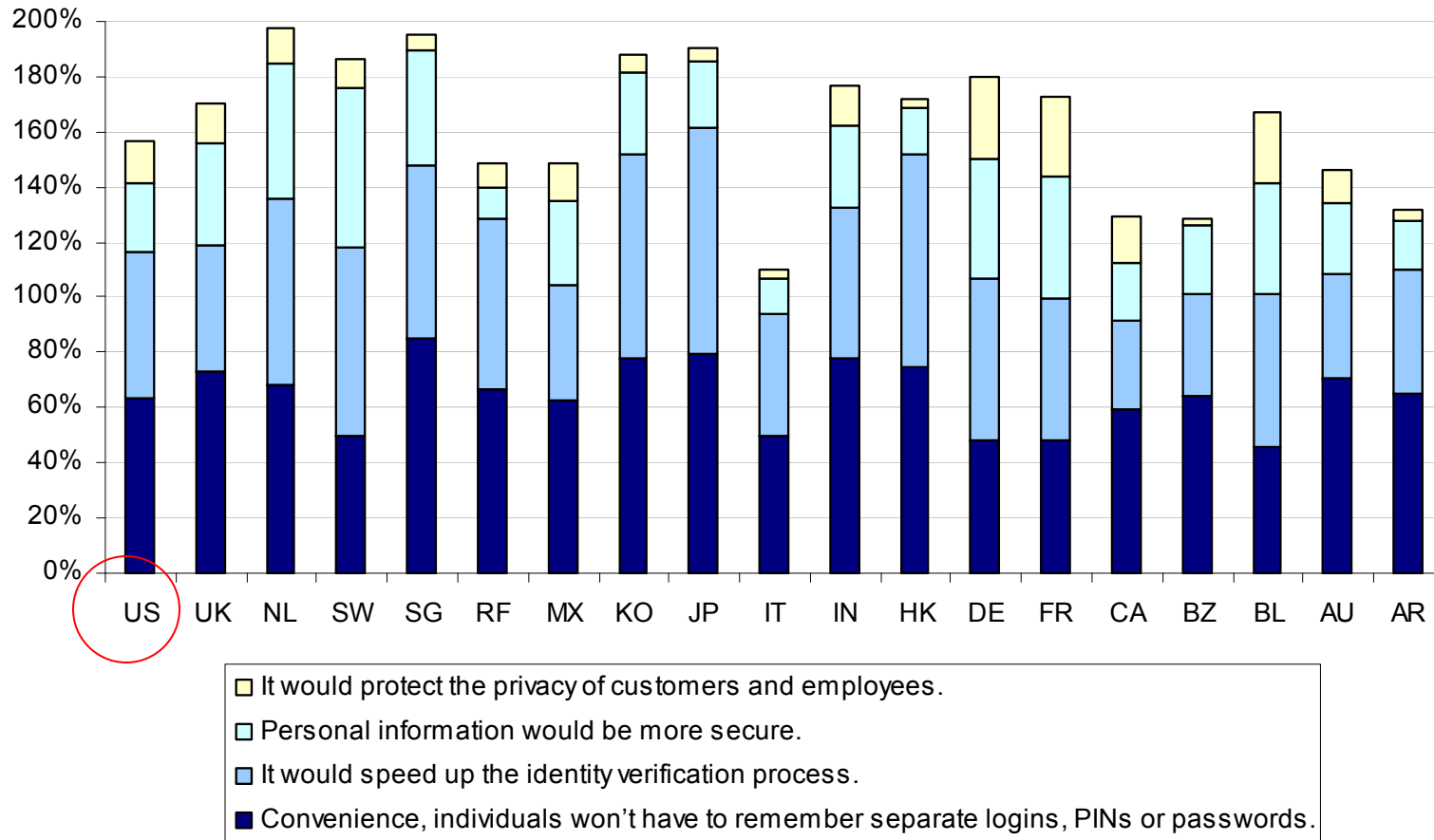
Q15b. Please check all functions that you would like this multipurpose ID credential to provide access to:

Percentage of bottom three functional uses.

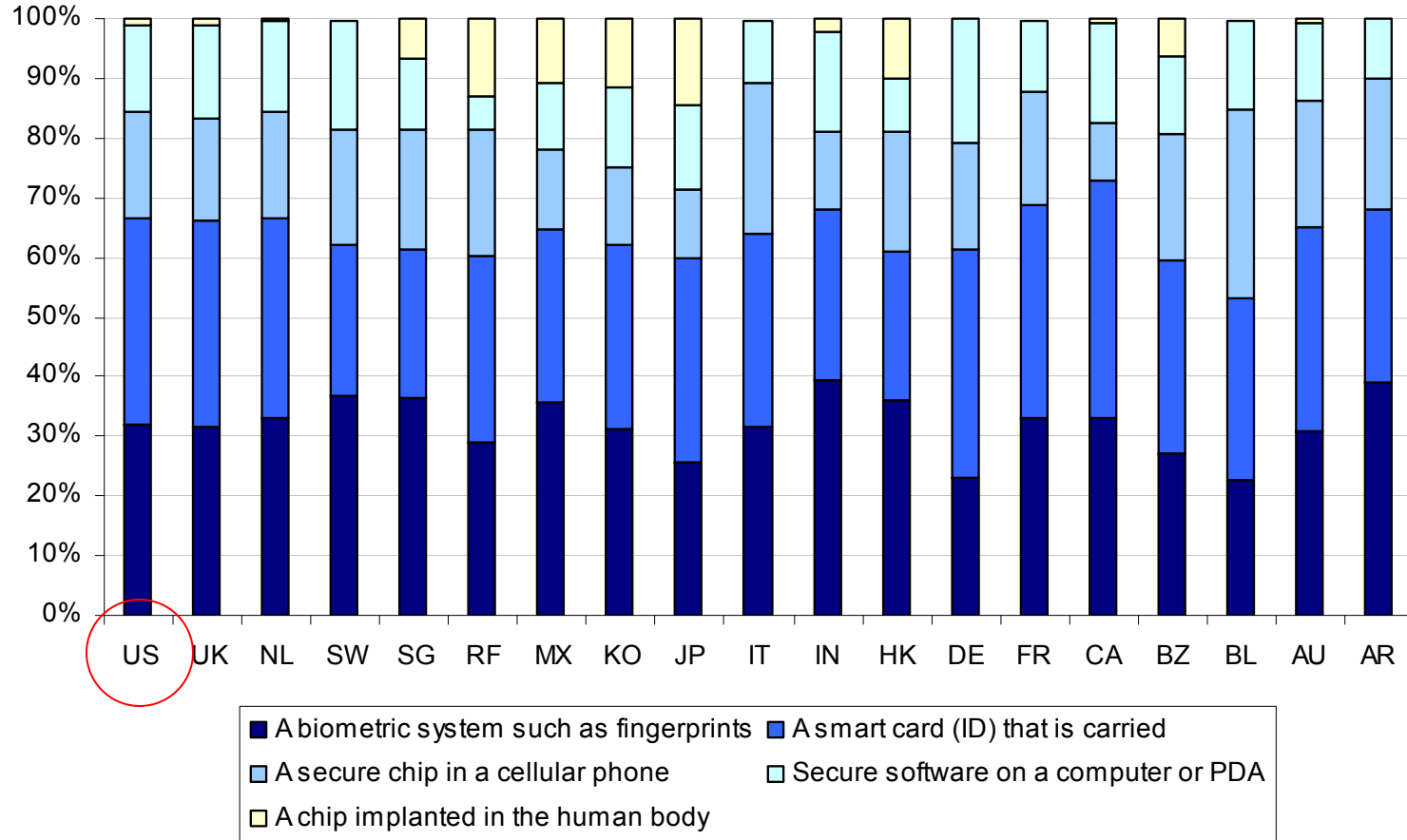
Multipurpose identity credential Bottom three uses



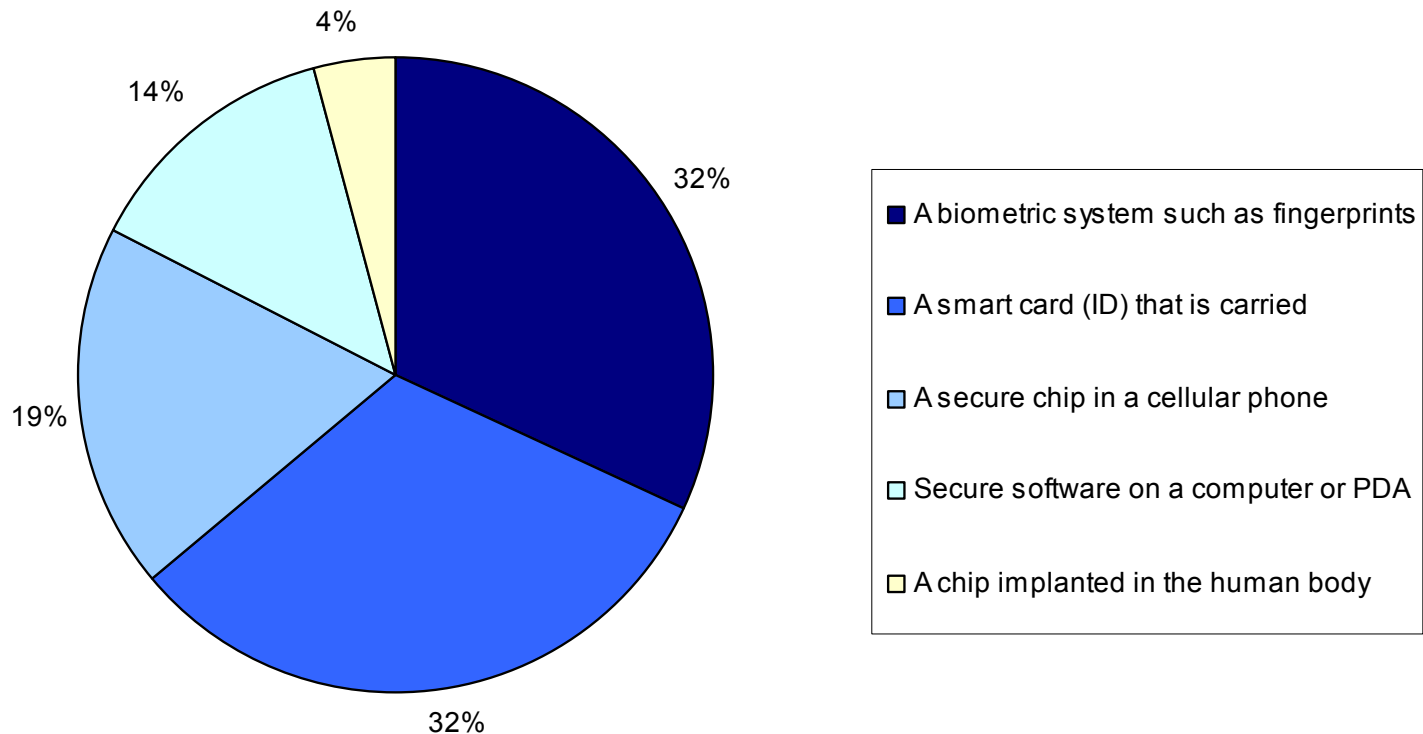
Q15c. What is the most important reasons for obtaining and using a multipurpose identity credential (primary reasons)?



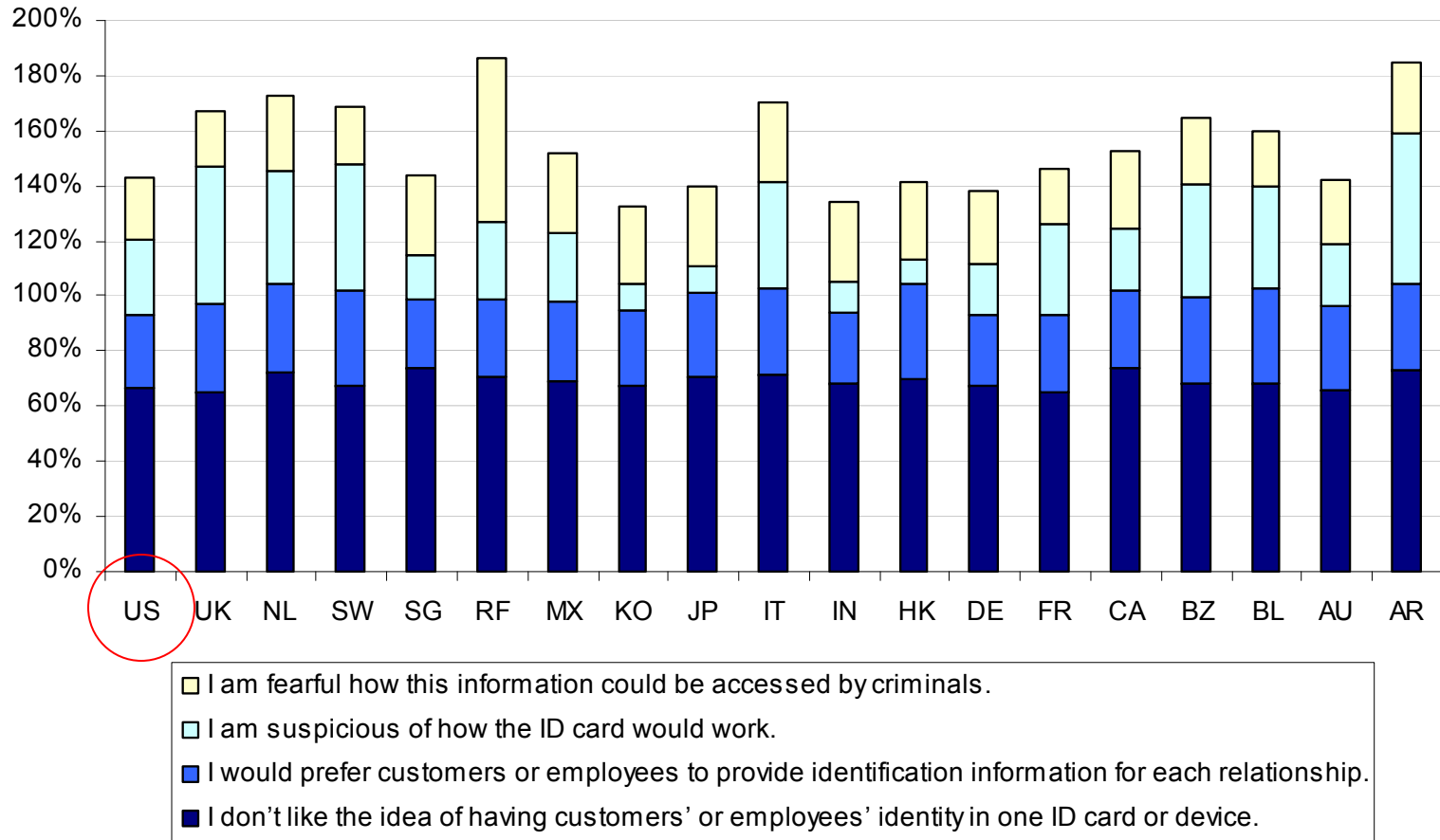
Q15d. Please select the one device from the list below that you would prefer customers or employees to use for managing their identity.



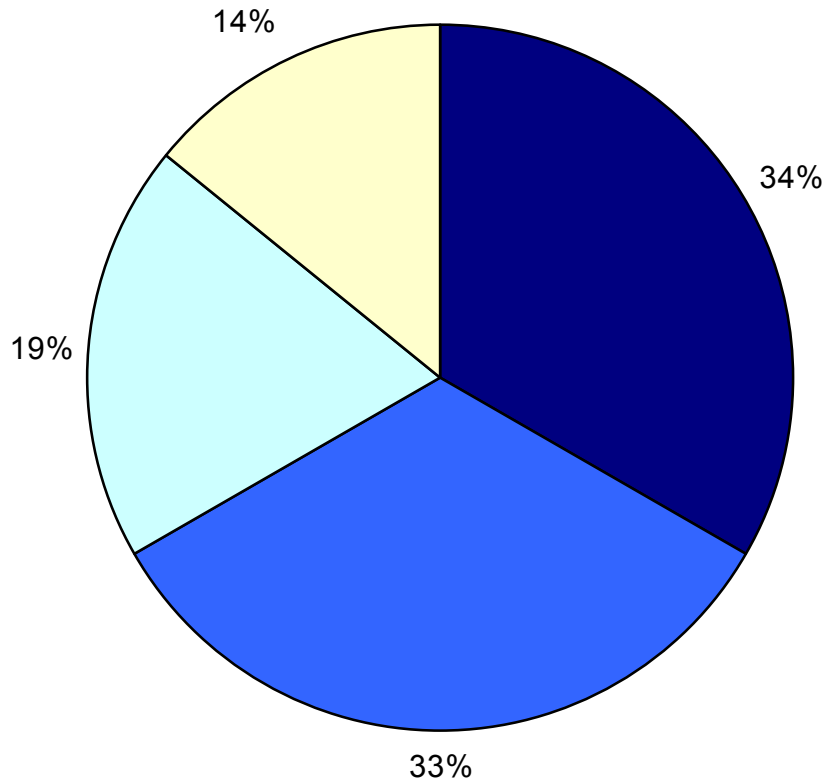
Q15d. Please select the one device from the list below that you would prefer customers or employees to use for managing their identity.



Q16. What are your primary concerns about using multipurpose identity credential?



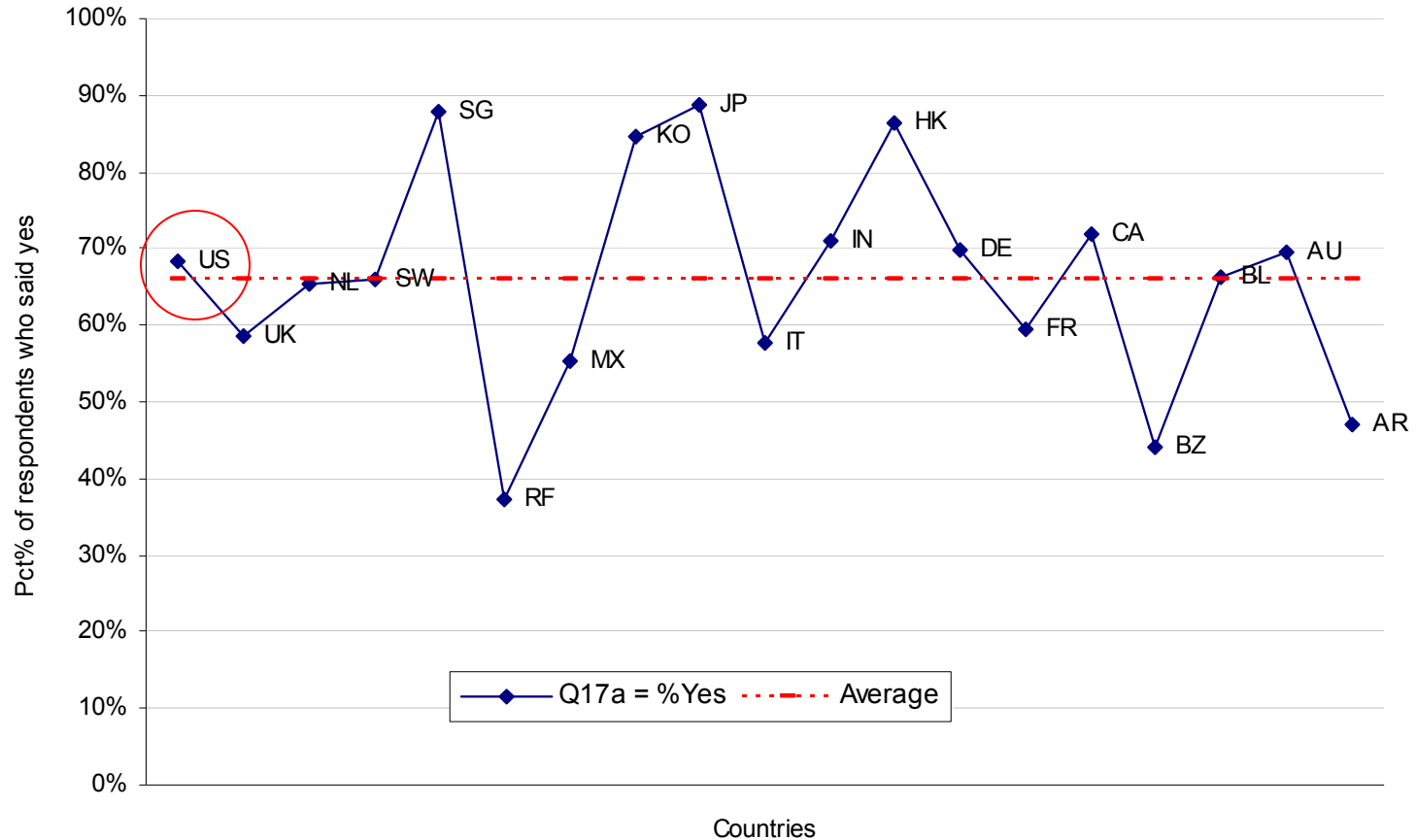
Q16. What are your primary concerns about using a multipurpose identity credential?



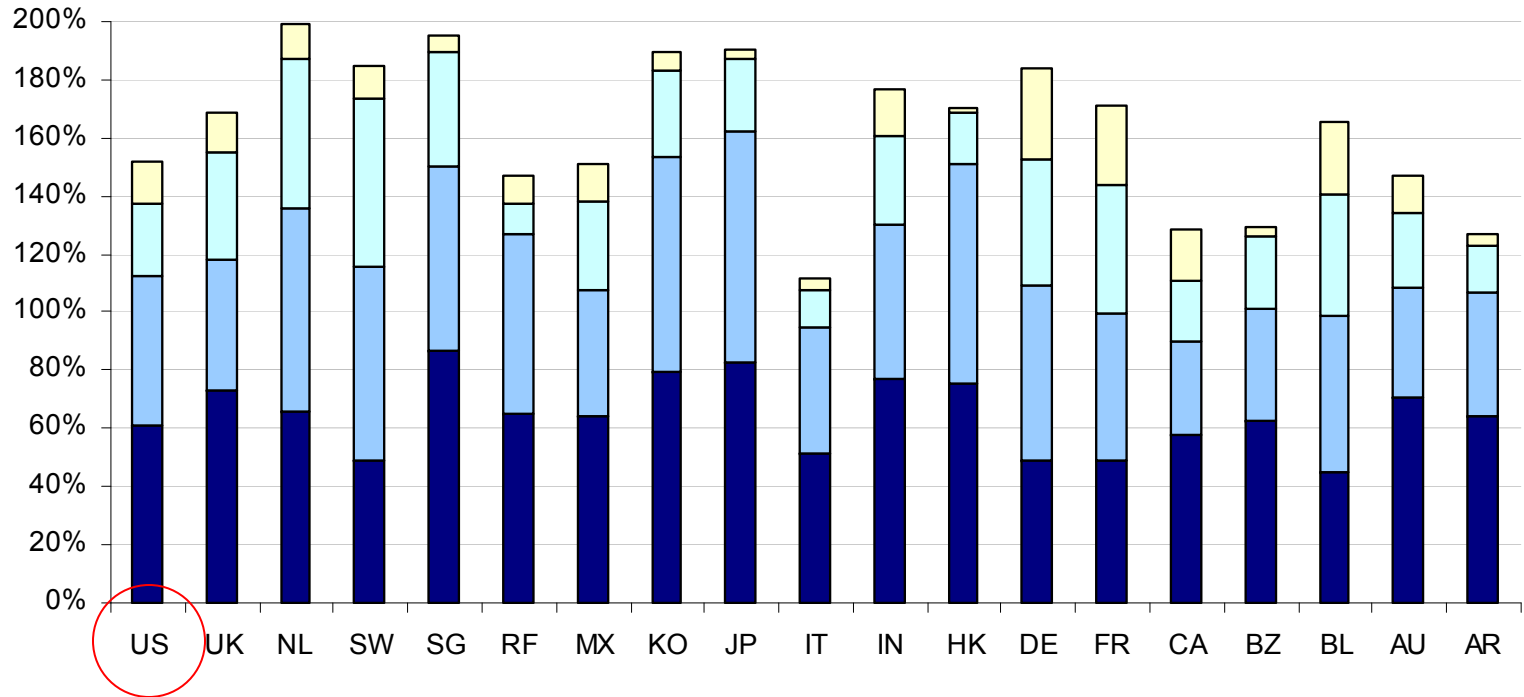
- I don't like the idea of having customers' or employees' identity in one ID card or device.
- I would prefer customers or employees to provide identification information for each relationship.
- I am suspicious of how the ID card would work.
- I am fearful how this information could be accessed by criminals.

Q17a. Is it acceptable for an organization to use biometrics such as voice or fingerprints to verify identity?

Percentage = Yes response.

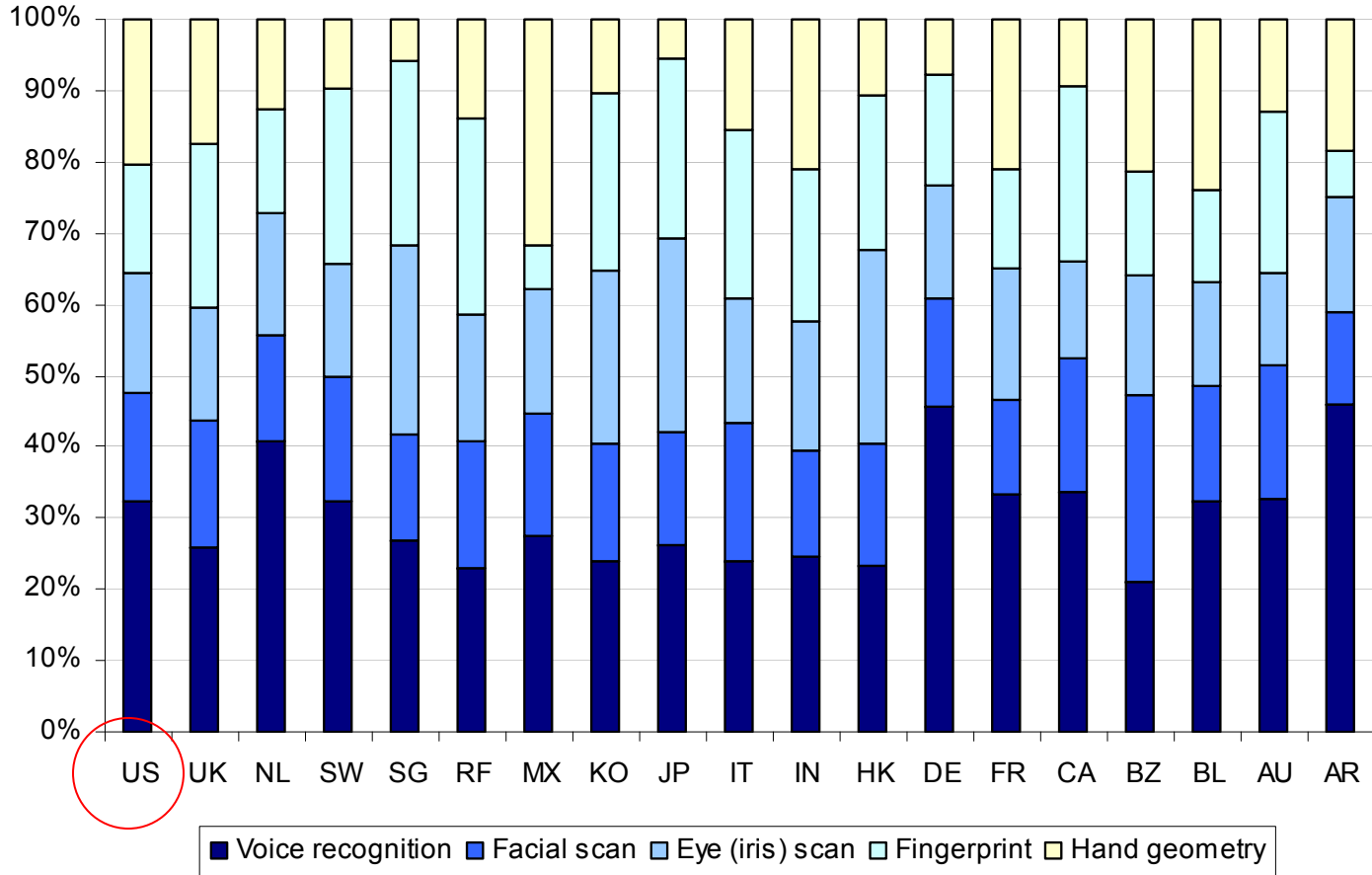


Q17b. What are your primary reasons why biometrics would improve your organization's state of identity management?

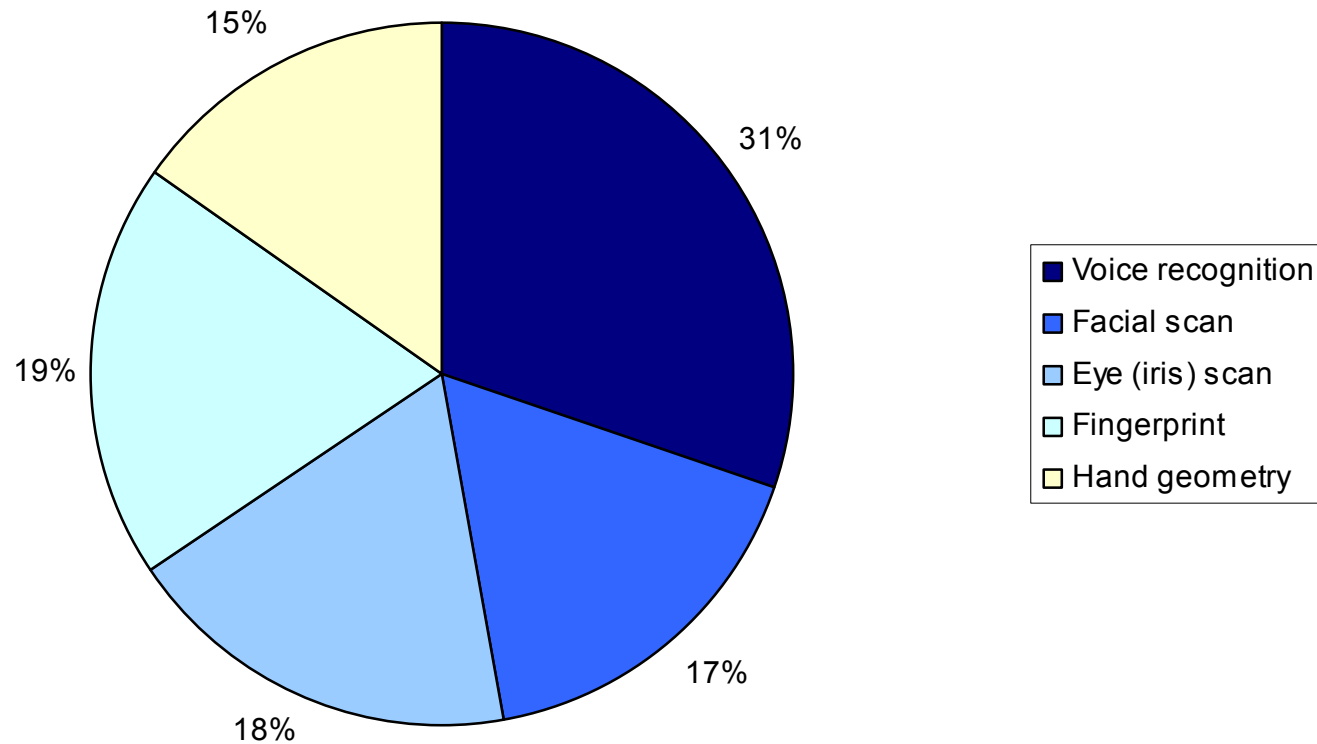


- It would protect the privacy of customers and employees.
- Information would be more secure.
- It would speed up the identity verification process.
- Convenience, because customers or employees won't have to remember separate logins, PINs or passwords.

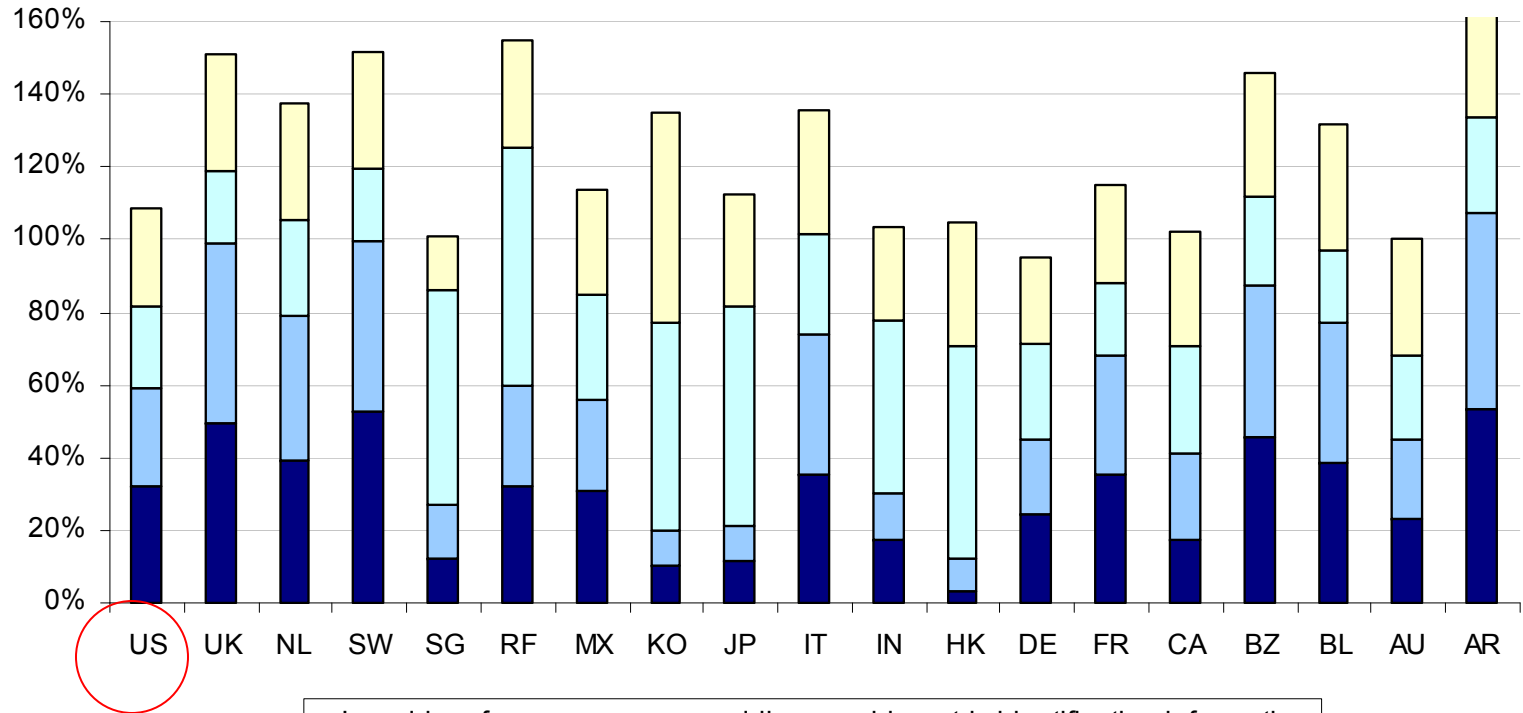
Q17c. What type of biometric authentication method would be most acceptable to you?



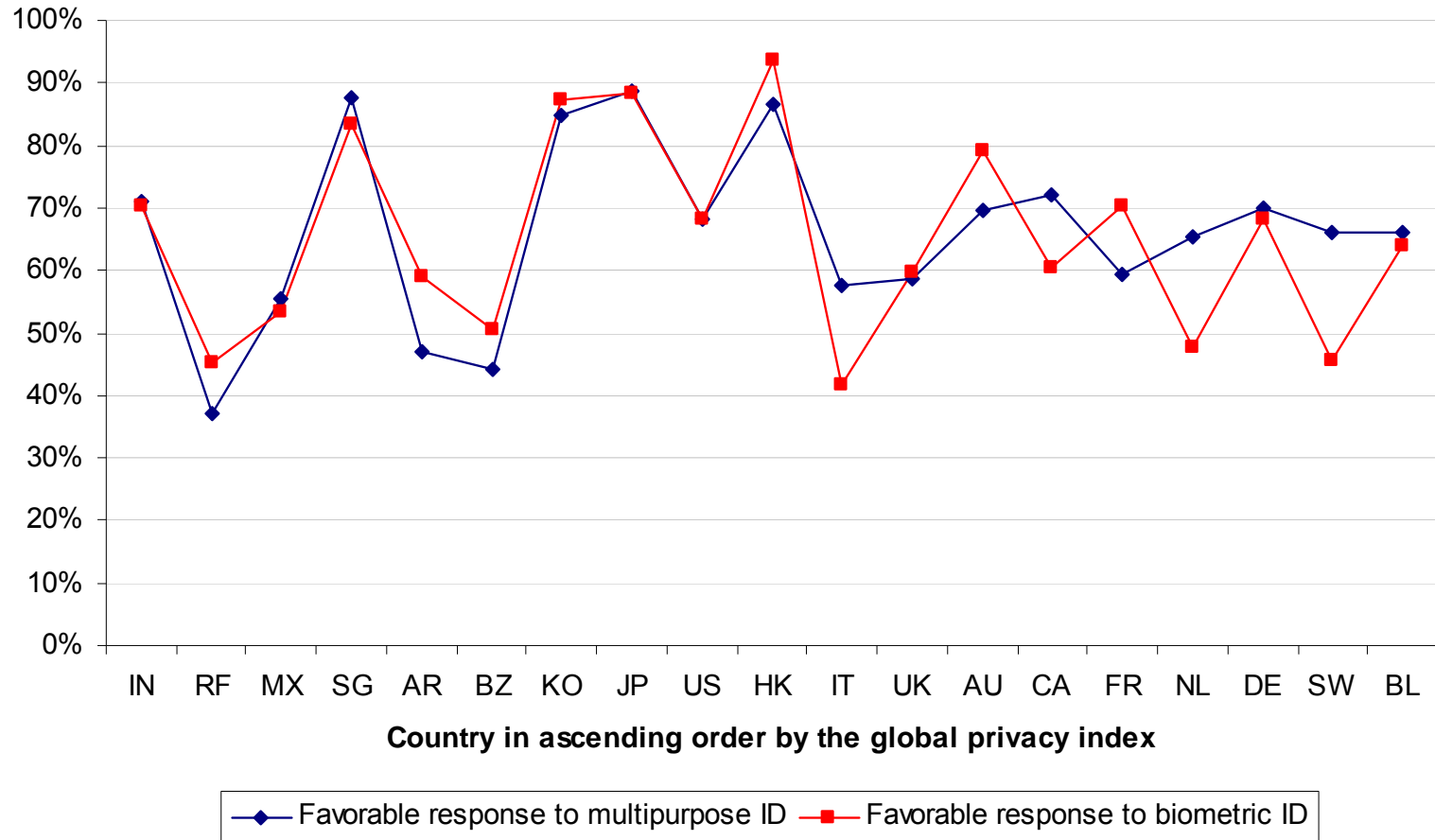
Q17c. What type of biometric authentication method would be most acceptable to you?



Q18. What are your primary concerns about using biometrics to identify and authenticate customers or employees?



Do individual attitudes about privacy affect perceptions about the use of multipurpose ID and biometric credentials?



About Device Fingerprinting & Privacy

Research Sponsor: ThreatMetrix

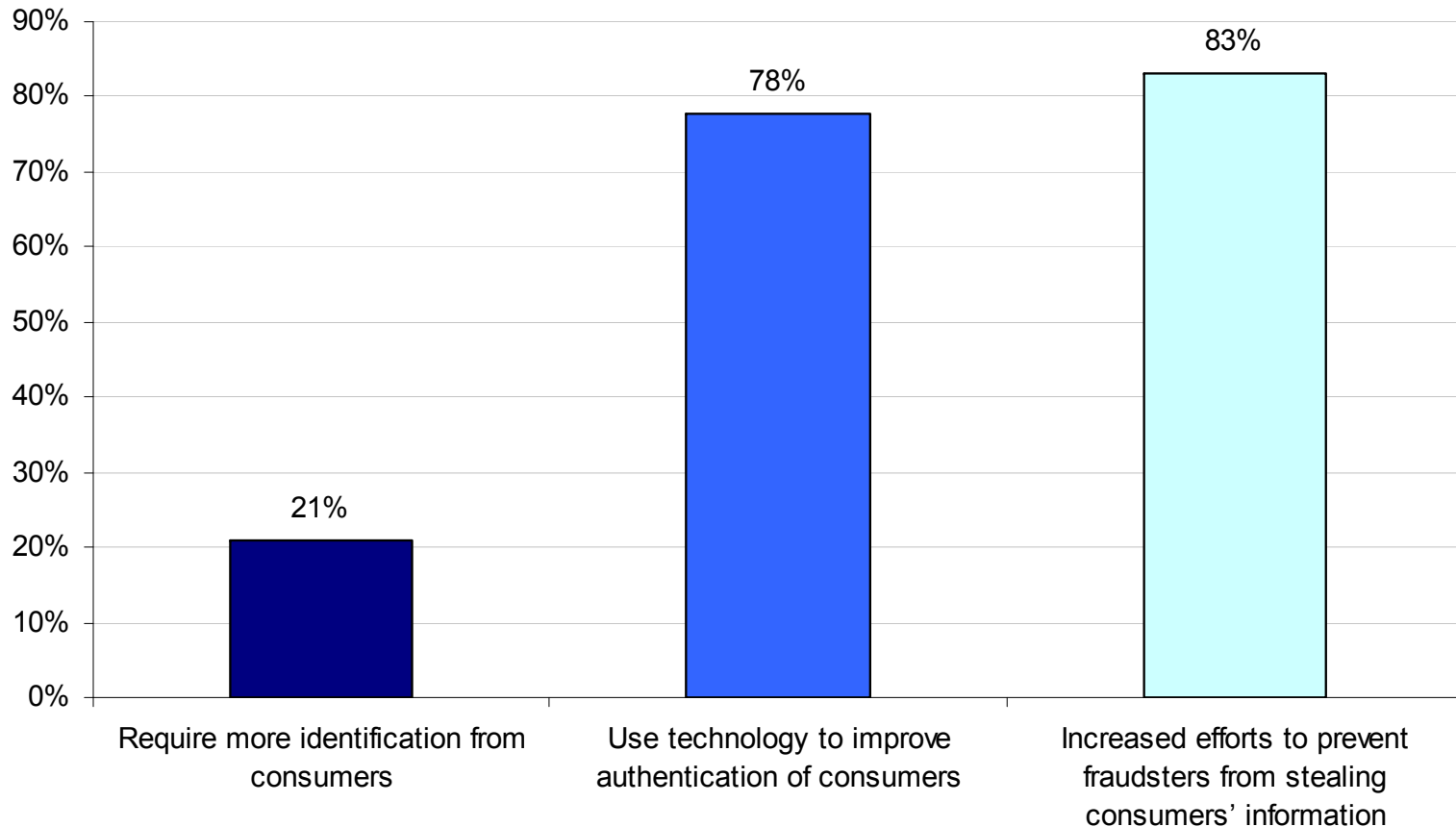
White paper available upon request

Sample & key findings

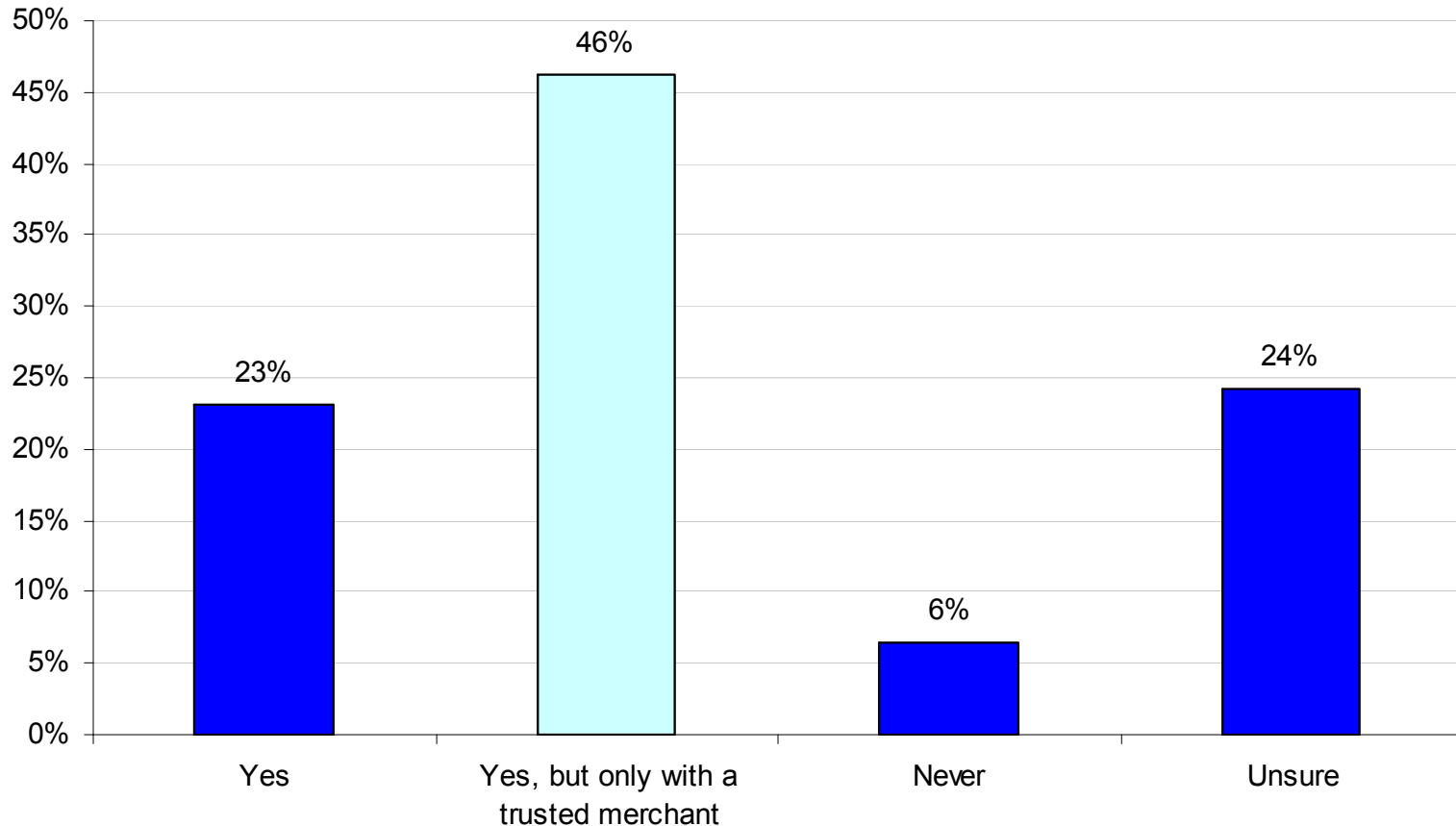
- Sample of adult-aged consumers located in the United States
- Survey focused on consumers' attitudes and beliefs about the use of device fingerprinting technology to combat online fraud and abuse.
- In general, most consumers do not appear to have privacy concerns about the use of a digital ID that defines their device – as long as this cannot be linked to natural identity or persona.
- In general, consumers expect organizations to use enabling technologies rather than demand more fact or memory-based methods in the identity and authentication process.

Sampling frame (adult-aged consumers)	14009
Bounce-back	2453
Total sample (before reliability)	632
Response rate (before reliability)	4.5%
Total sample (final)	551
Response rate (final)	3.9%

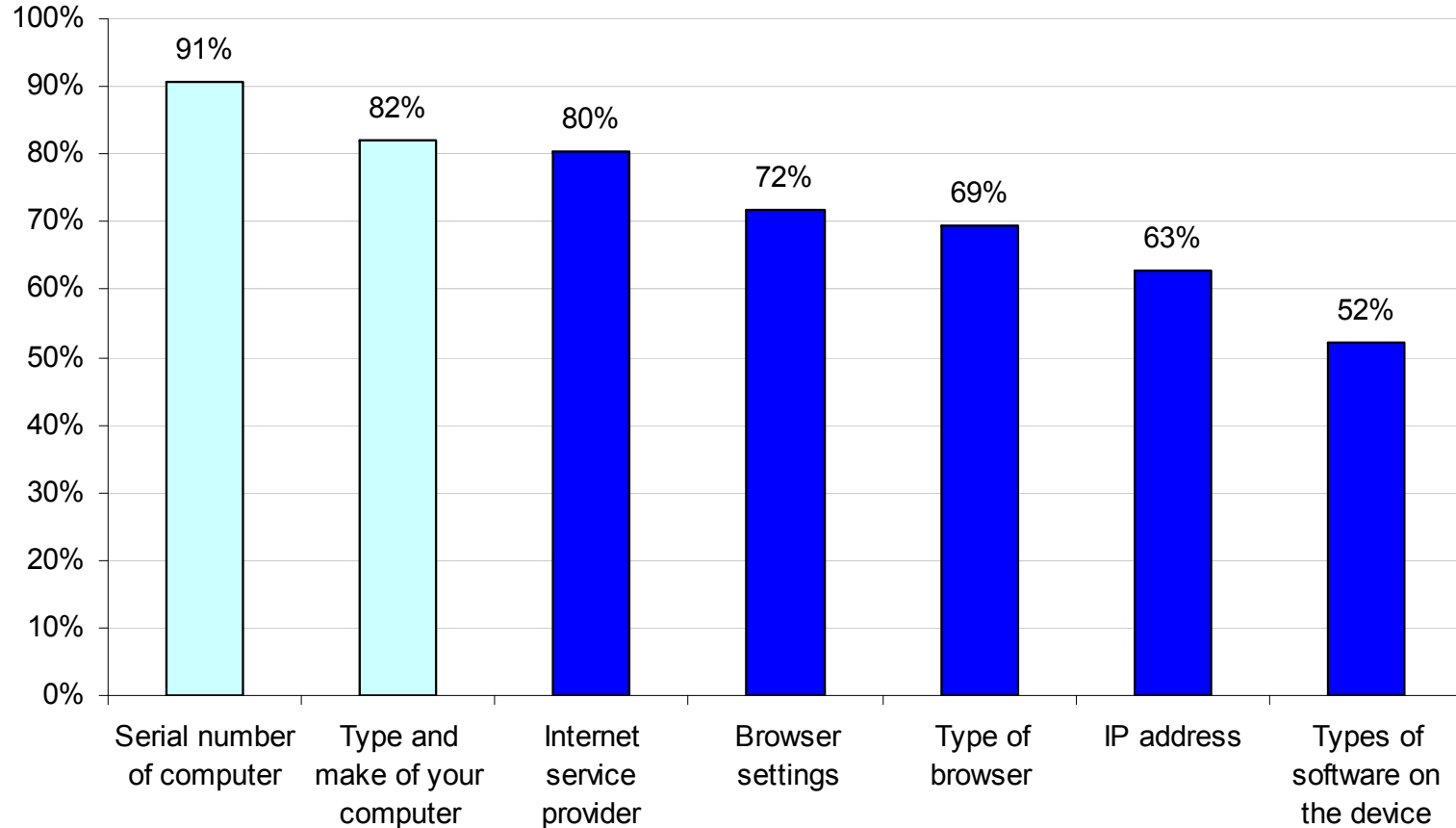
What steps should be taken by online merchants, banks and social networks to protect your personal information and identity



If you were assured that your personal information was not collected, would you be willing to have your computer authenticate your identity (device fingerprint) by an online merchant before when making a purchase?



What information you willing to share with a trusted online merchant to fingerprint your computer device?



Summary of key findings

- Understand the global view – there are significant differences in the perceptions and attitudes of individuals concerning privacy and the use of certain identify and authentication technologies.
- Perceptions about privacy may be inextricably linked to the public’s acceptance of technology-based identity and authentication methods such as biometrics, device fingerprinting, and others.
- Individuals want more control and expect more convenience when using technology-based identity and authentication methods.
- Opinion: Privacy concerns may not be a significant barrier to the adoption of technology-based identity and authentication methods as long as disclosure, consent and redress are made available to the user.

Questions from the audience

Dr. Larry Ponemon
Ponemon Institute LLC
2308 US 31 North
Traverse City, Michigan 49686 USA
231.938.9900
research@ponemon.org