



2015 IT Risk/Reward Barometer Europe Results

October 2015

www.isaca.org/risk-reward-barometer

Number of respondents (n) = 1,554

Respondents are European business and IT professionals who are members of ISACA.

Media Inquiries:

Kristen Kessinger, ISACA, +1.847.660.5512, news@isaca.org

Sara Bosco, Ketchum, +1.646.935.4366, sara.bosco@ketchum.com

1. Do you think your IT department is aware of all of your organization's connected devices (e.g., connected thermostats, TVs, fire alarms, cars, etc.)? (n = 1,551)
 - a. Yes.....32%
 - b. **No**.....**51%**
 - c. Unsure.....17%

2. What do you think is the likelihood of a company being hacked through an Internet of Things (IoT) device?: (n = 1,554)
 - a. Low.....26%
 - b. **Medium**.....**42%**
 - c. High.....28%
 - d. Unsure.....5%

3. Do existing security standards in the industry sufficiently address IoT? (n = 1,552)
 - a. Yes.....9%
 - b. No, but updates and/or new standards are not needed.....5%
 - c. **No, and updates and/or new standards are needed**.....**74%**
 - d. Unsure.....13%

4. Which of the following best describes your opinion on the impact of the IoT on employee privacy in the workplace? Increasing use of IoT devices in the workplace has resulted in: (n = 1,550)
 - a. Increased employee privacy.....6%
 - b. No change to employee privacy.....16%
 - c. **Decreased employee privacy**.....**66%**
 - d. Unsure.....12%

5. Which of the following do you see as the most significant security concern for enterprises, related to the IoT? (n = 1,553)
- a. Vulnerabilities in the device themselves.....37%
 - b. **Data leakage**.....**39%**
 - c. Access control.....17%
 - d. Asset management.....4%
 - e. Other.....4%
6. What size enterprise, if any, do you think is most vulnerable to IoT-related risk? (n = 1,550)
- a. Small (1-49 employees).....8%
 - b. Medium (50-499 employees).....10%
 - c. Large (500 or more employees).....18%
 - d. **They are all equally vulnerable**.....**60%**
 - e. None of them are vulnerable.....0%
 - f. Unsure.....4%
7. Which of the following benefits, if any, has your organization experienced as the result of the IoT? (n = 1,512)
- a. Greater efficiency.....29%
 - b. Improved services.....33%
 - c. Improved supply chain.....11%
 - d. Lower costs.....17%
 - e. Improved data storage.....6%
 - f. **Greater accessibility to information**.....**38%**
 - g. Increased employee productivity.....21%
 - h. Increased customer satisfaction.....16%
 - i. No benefits have been achieved.....27%
 - j. Other.....3%
8. Does your organization's BYOD (bring your own device) policy address wearable tech (e.g., smart watches, etc.)? (n = 1,549)
- a. Yes.....15%
 - b. **No**.....**50%**
 - c. Unsure.....9%
 - d. We don't have a BYOD policy.....25%
9. When did your organization most recently update its BYOD policy? (n = 1,550)
- a. Within the past year.....29%
 - b. Within the past two years.....19%
 - c. More than two years ago.....6%
 - d. Unsure.....13%
 - e. **We don't have a policy that addresses BYOD**.....**33%**

10. Do you believe employees' use of wearable technology will have an impact on your organization? (n = 1,552)
- a. Yes, it will have a positive impact.....22%
 - b. It has already had a positive impact.....4%
 - c. Yes, it will have a negative impact.....15%
 - d. It has already had a negative impact.....2%
 - e. No.....20%
 - f. **Unsure**.....**36%**
11. Do you believe device manufacturers are implementing sufficient security measures in IoT devices? (n = 1,551)
- a. Yes.....4%
 - b. **No**.....**77%**
 - c. Unsure.....19%
12. Do you believe IoT device manufacturers make consumers sufficiently aware of the type of information the devices can collect? (n = 1,553)
- a. Yes.....5%
 - b. **No**.....**89%**
 - c. Unsure.....6%
13. Do you expect a cyberattack to strike your organization in the next 12 months? (n = 1,549)
- a. **Yes**.....**52%**
 - b. No.....24%
 - c. Unsure.....24%
14. Is your organization prepared for a sophisticated cyberattack? (n = 1,549)
- a. **Yes**.....**40%**
 - b. No.....32%
 - c. Unsure.....28%
15. Are you confident that you can control who has access to your information collected by IoT devices in your home? (n = 1,547)
- a. Yes.....24%
 - b. **No**.....**61%**
 - c. Unsure.....15%
16. Which of the following is most important for consumers to do to keep information secure on IoT devices they own? (n = 1,549)
- a. Change passwords.....10%
 - b. Change privacy settings.....15%
 - c. Turn off Internet-enabled functions when not actively in use.....15%
 - d. **Avoid storing sensitive or classified data on the device(s)**.....**50%**
 - e. Avoid using or logging into public Wi-Fi access points.....6%
 - f. Other (please specify).....4%

17. In the past year, there have been reports in the media of each of the following types of IoT hacks. For each item, please rate how likely you think it is to occur as an actual hack: (n = 1,549)

	Very Likely	Somewhat Likely	Somewhat Unlikely	Very unlikely
A car is taken over by hackers through its infotainment system while traveling along a highway.	23%	36%	26%	15%
Hacks to a Wi-Fi enabled sniper rifle make the rifle miss its target and disable the scope's computer or prevent the gun from firing.	10%	26%	36%	28%
Computerized drug-infusion pumps are hacked to access and alter hospital patients' dosages	10%	39%	35%	16%
Employees of an on-demand video streaming media company hacked into a wearable fitness tracker.	24%	46%	25%	6%
Researchers hacked into a popular home thermostat and were able to access the Wi-Fi password for the local network, data related to the presence of users at home, and security vulnerabilities in a baby monitor and older PC.	44%	39%	13%	3%

Demographics

In what industry do you work? (n = 1,553)

a. Financial/Banking.....	24%
b. Insurance.....	5%
c. Public accounting.....	3%
d. Transportation.....	1%
e. Aerospace.....	0%
f. Retail/Wholesale/Distribution.....	3%
g. Government/Military.....	8%
h. Technology Services/Consulting	29%
i. Manufacturing/Engineering.....	4%
j. Telecommunications/Communications.....	6%
k. Mining/Construction/Petroleum/Agriculture.....	2%
l. Utilities.....	1%
m. Legal/Law/Real Estate.....	0%
n. Healthcare/Medical.....	2%
o. Pharmaceutical.....	2%
p. Advertising/Marketing/Media.....	1%
q. Education/Student.....	1%
r. Other (please specify).....	8%

How many people are employed in your enterprise, including all branches, divisions and subsidiaries? (n = 1,551)

a. Fewer than 50.....	10%
b. 50-149.....	7%
c. 150-499.....	9%
d. 500-1,499.....	13%
e. 1,500-4,999.....	14%
f. 5,000-9,999.....	7%
g. 10,000-14,999.....	5%
h. 15,000 or more	34%

Which of the following is closest to your job title? (n = 1,550)

a. Student.....	0%
b. External consultant.....	12%
c. Professor/teacher.....	1%
d. Practitioner.....	10%
e. Supervisor.....	9%
f. Manager	33%
g. Director.....	8%
h. Vice president.....	1%
i. CIO/CISO/CAE.....	11%
j. President/CEO.....	2%
k. Other (please specify).....	13%

Please indicate your gender? (n = 1,533)

- a. Female.....14%
- b. **Male**.....**86%**

Please select your age group. (n = 1,549)

- a. 18 to 24 years.....0%
- b. 25 to 34 years.....18%
- c. **35 to 44 years**.....**39%**
- d. 45 to 54 years.....32%
- e. 55 to 64 years.....11%
- f. 65 to 74 years.....1%
- g. 75 years or above.....0%

About ISACA's 2015 IT Risk/Reward Barometer

The annual IT Risk/Reward Barometer is a global indicator of trust in information. Conducted by ISACA, the Barometer polls thousands of IT and cybersecurity professionals and consumers worldwide to uncover attitudes and behaviors about essential technologies and information, and the trade-offs people make to balance risk and reward. The study is based on online polling of 7,016 ISACA members in 140 countries from 27 August to 8 September 2015. Additional online surveys were fielded by M/A/R/C Research among 1,227 consumers in the US, 1,025 consumers in the UK, 1,060 consumers in Australia, 1,027 consumers in India and 1,057 consumers in Mexico. The US survey ran 17-20 August 2015, and the UK, Australia, India and Mexico surveys ran 21-30 August 2015. At a 95 percent confidence level, the margin of error for each individual country sample is +/- 3.1 percent. To see the full results, visit www.isaca.org/risk-reward-barometer.

Note: Due to rounding to the nearest whole number, responses may not add up to 100%.