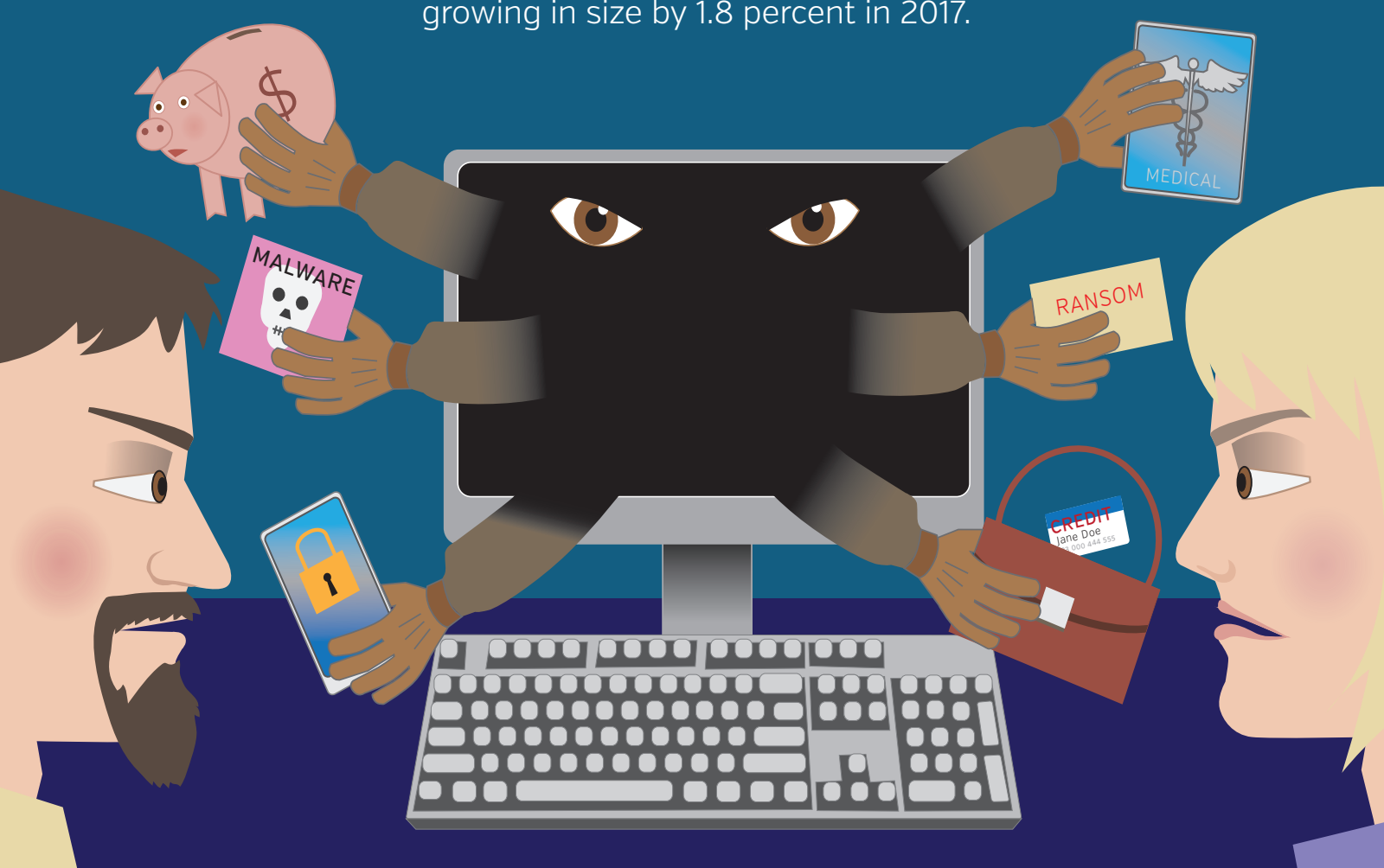
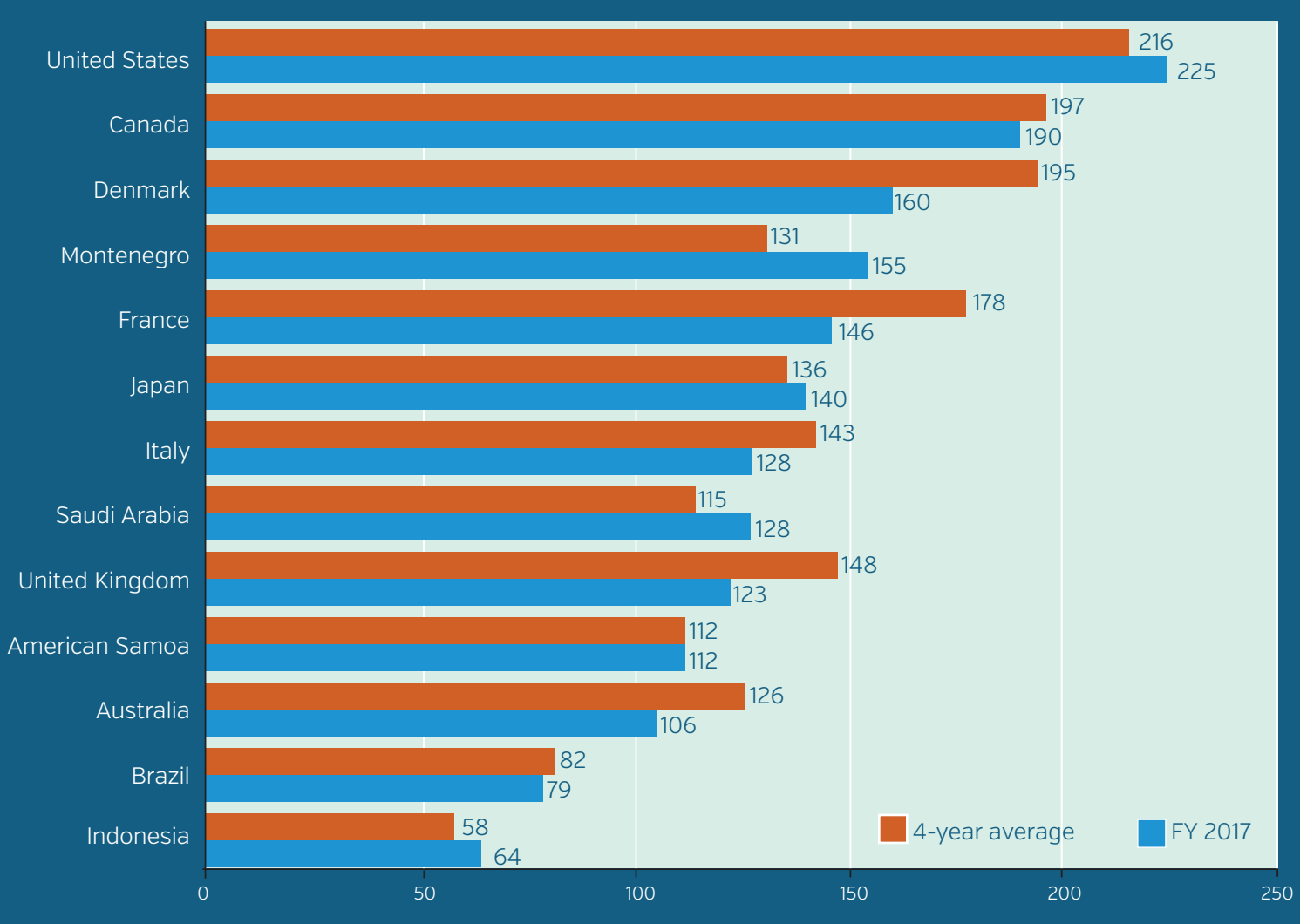
Data breach costs down, but breaches themselves grow

The average total cost of a data breach fell to $3.6 million from $4 million this year, according to a survey of more than 400 companies. The average cost for each lost or stolen record containing sensitive and confidential information also fell, from $158 in 2016 to $141. However, companies are seeing bigger breaches, with the average breach growing in size by 1.8 percent in 2017.



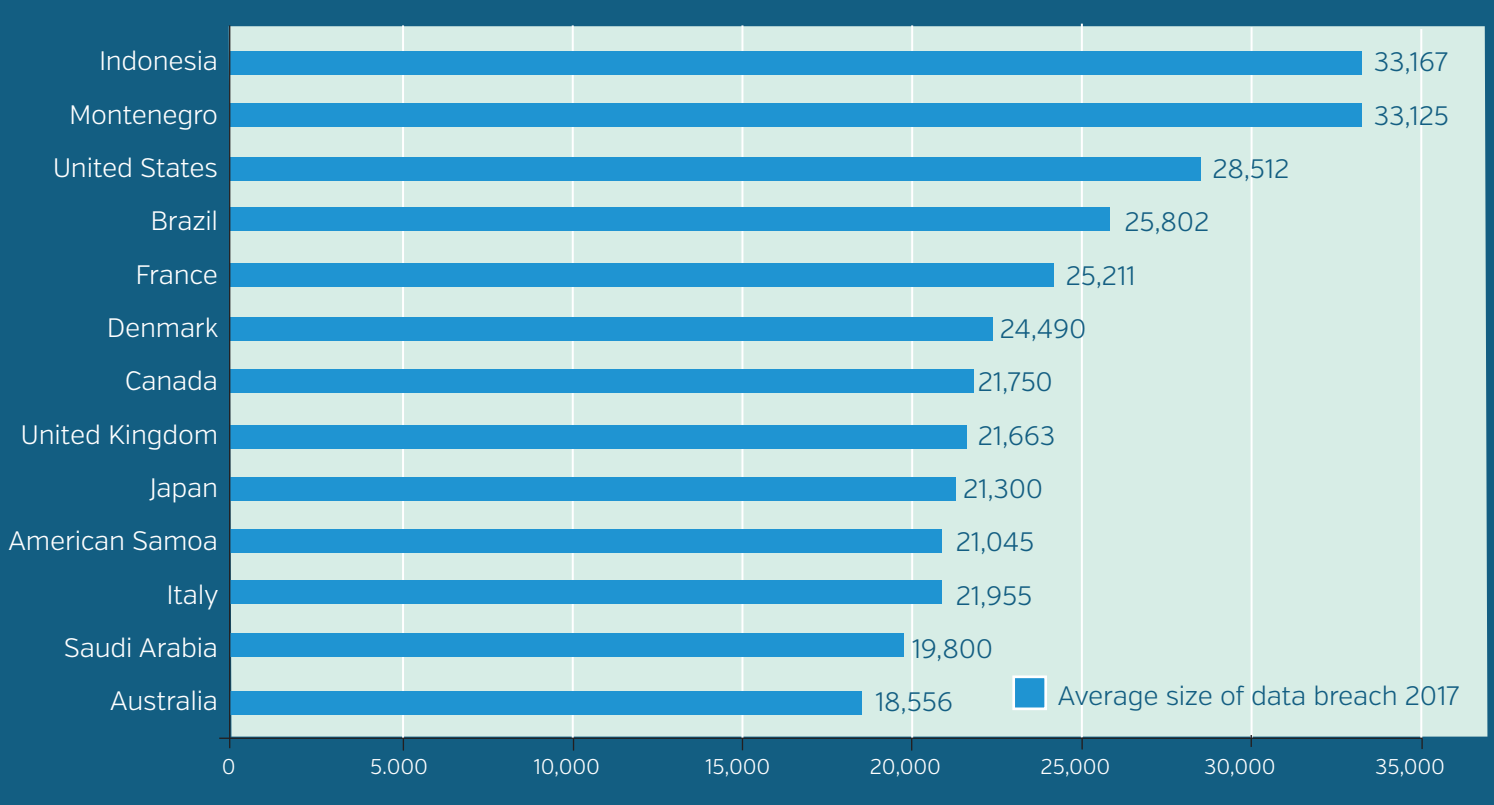
United States leads, and that's not good

The average per capita data breach cost over four years varied widely among nations, with companies in the United States seeing the highest costs.



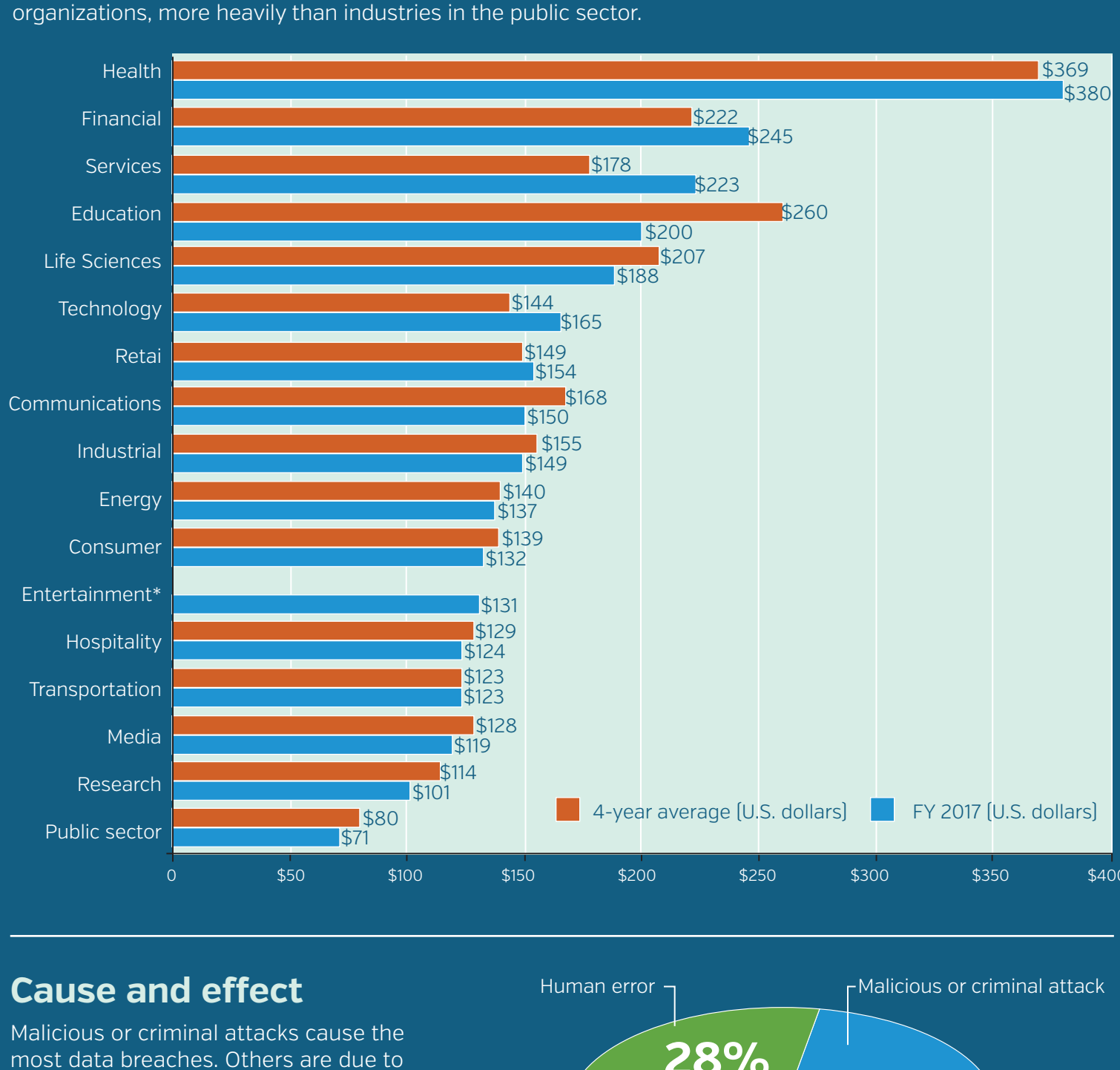
When more isn't better

Organizations in India, the Middle East and the United States had the largest average number of breached records.



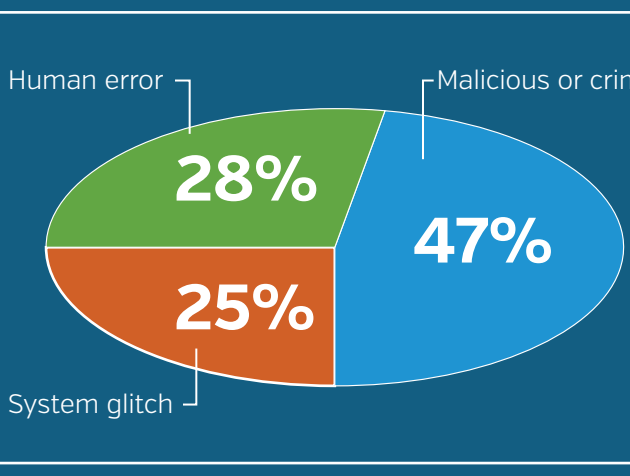
Accountability can lead to higher liability

The costs of a data breach hit highly regulated industries, such as health care, education and financial organizations, more heavily than industries in the public sector.



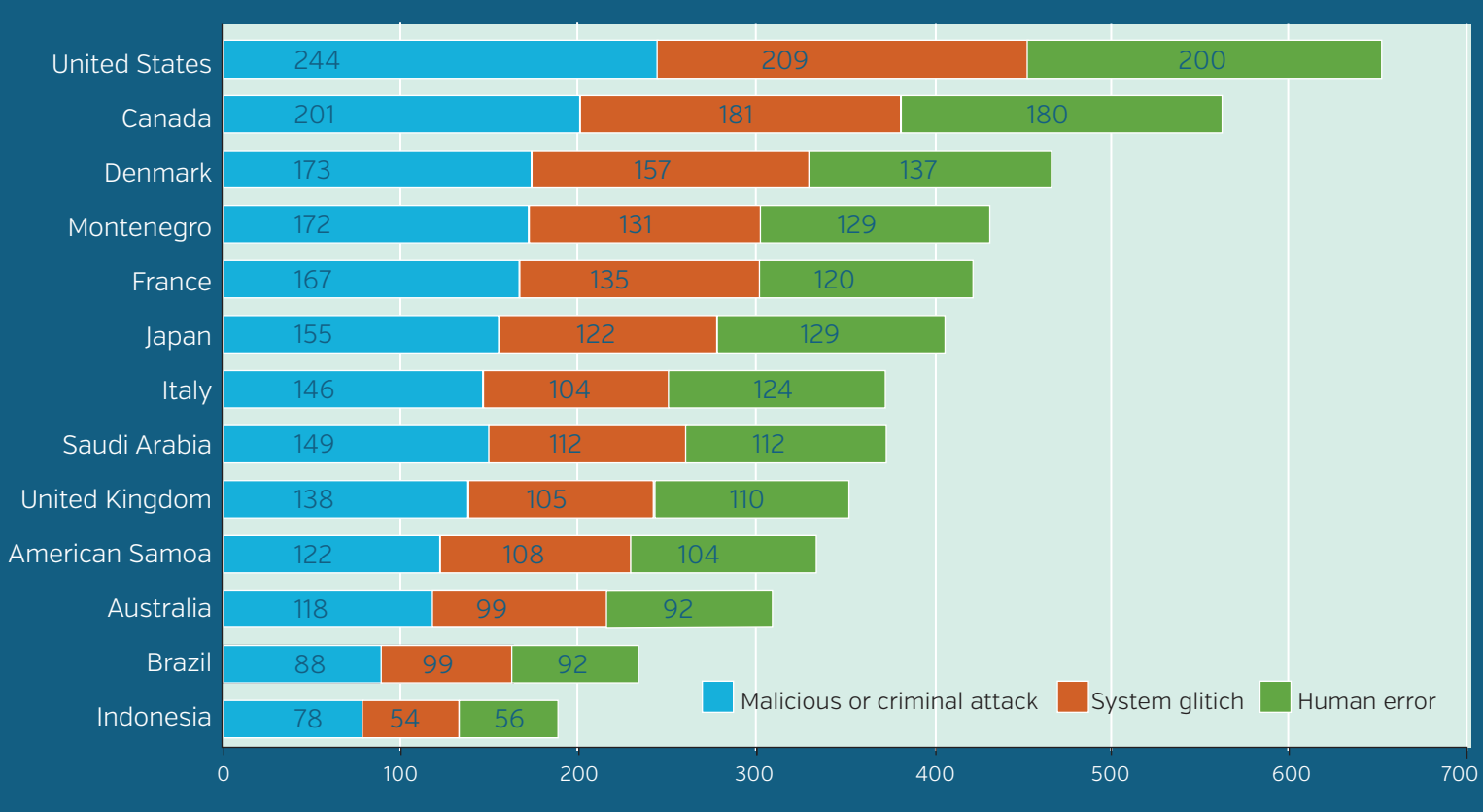
Cause and effect

Malicious or criminal attacks cause the most data breaches. Others are due to human error or negligence, and some are caused by technical or business process issues.



Malicious attacks cost companies the most

In the United States, the cost of a malicious or criminal data breach incident was $244 per compromised record.



Source: 2017 Cost of Data Breach Study: Global Overview, from IBM Security and the Ponemon Institute

For more information, call 888.682.5911 or visit us at www.IDT911.com.

third CERTAINTY

CYBERSCOUT