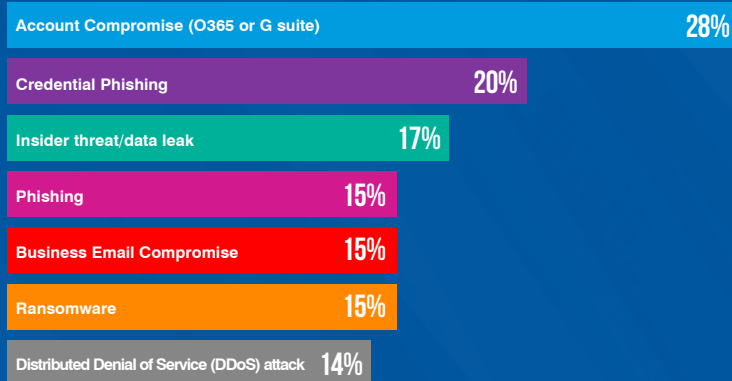


PEOPLE-CENTRIC CYBERSECURITY: A STUDY OF 150 IT SECURITY LEADERS IN THE UAE

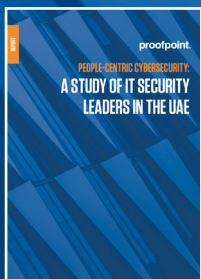
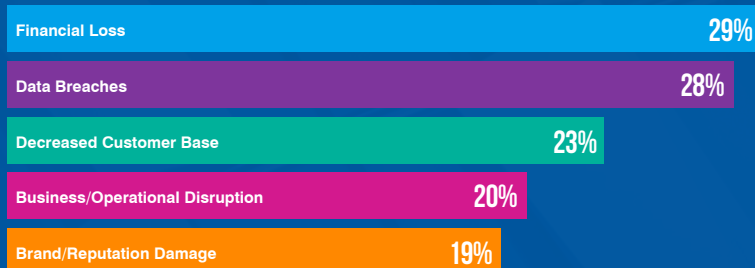
UAE: A DYNAMIC THREAT LANDSCAPE

82% of organizations in the UAE suffered at least one cyber attack in 2019. **51%** said that their business was targeted multiple times.

Targeted organizations in the UAE faced a diverse threat landscape in 2019:



And suffered the following consequences:



DOWNLOAD OUR FULL REPORT HERE

Contact us at info-middleeast@proofpoint.com to better protect your business.

MOST COMMON CYBER SECURITY CHALLENGES

55% of UAE IT security leaders believe that human error and lack of security awareness is a risk factor for their organization.

39% believe that their employees make their business vulnerable to a cyber attack.

23% Despite facing a fast-evolving threat landscape, only 23% train their employees more than three times a year.

CYBER RISK: PREPARING FOR THE FUTURE

21% of organizations in the UAE strongly feel that they are prepared for a cyber attack.

31% cite a lack of board-level buy-in as a major obstacle to implementing cybersecurity technology.

Senior IT security leaders in the UAE are optimistic that cyber security will become more of a business priority moving forward with...

50% reviewing their cybersecurity strategy twice a year or more

69% expecting their cybersecurity budget to rise by 11% or more over the next two years.