Survey Findings Show Increased Education Will Help Organizations Better Prevent Cyberattacks

December 3, 2015

One in Seven European Managers Knowingly Expose Their Business to Risk Despite Spending Billions on Cybersecurity

LONDON – December 3, 2015 – Palo Alto Networks® (NYSE: PANW), the next-generation security company, today announced the findings of a new survey into management and executive attitudes towards cybersecurity across Europe. This noted that an alarming number of senior employees consciously expose their organizations to cybersecurity threats, largely due to frustration with workplace policies and a poor understanding of cybersecurity threats, according to new research released today.

Commissioned by Palo Alto Networks, the research findings show the actions of decision-makers undermine the $35.53 billion [1] European organizations are predicted to spend on cybersecurity by 2019. The survey found that 27 percent of respondents admit to exposing their company to a potential cybersecurity threat with 14 percent saying they knew they were doing so at the time.

Balancing security with functionality

While some actions could be tracked back to one in four claiming not to understand fully what defines an online cybersecurity risk, almost every respondent (96%) acknowledged cybersecurity should be a priority for their business.

The prevailing reason employees circumvent their companies' policies is to use a more efficient tool or service than that used by the organisation, or that such tools were considered the best in the market. These actions reflect 17 percent saying their company's cybersecurity policy is frustrating and prevents access to tools and sites that would enable better job performance. Employee education is essential in ensuring that the rationale behind the policy is clear.

Senior staff circumventing security

Survey results indicate that neither department nor seniority precludes employees from carrying out questionable actions or having misinformed views. One in ten respondents caught executives ignoring company guidelines; and when asked directly, one in four C-level respondents admitted to knowingly exposing their company to a potential threat.

Responsibility and accountability

The research found one in five (18%) management-level employees don't feel they have a personal role to play in their company's cybersecurity efforts; and that, if a successful attack were carried out, only one in five (21%) believe the employee responsible for the breach would be held accountable – the majority (40%) believe IT would be held to blame.

QUOTES

- "The impact of employees' actions may not be immediately visible as attacks often happen later – meaning organisations may struggle to identify their source. With two-thirds of people not yet on board with the reality of everyone having a role to play in preventing cyberattacks, it is clear there is an opportunity for organisations to put cybersecurity education front and centre in 2016."

- "The findings suggest senior employees are over-confident and willing to take chances because of a belief that 'it won't happen to them.' With changing regulations, visibility of what is really happening in Europe will shift in the coming years, and risk-taking will fall. It also suggests that too many still see cybersecurity as something done for the business, not something that everyone must follow."

- Greg Day, vice president and regional chief security officer, EMEA, at Palo Alto Networks

Additional findings from the research

- At 35% of respondents, the U.K. has the highest percentage who say they don't fully understand what defines an online security risk. France has the lowest with 17% claiming same.
- Germany has the highest number of respondents claiming to have exposed their company to a potential cybersecurity risk at 38%. Belgium has the lowest with 12%.
- 28% of those in the Netherlands say their company's cybersecurity policy frustrates them – significantly higher than the average of 17%.
- Those in financial services, insurance, or professional services are most likely to circumvent their company's cybersecurity policy with 21% across the regions admitting to doing so.
- Those in the U.K. are least likely to feel they have a personal role in protecting their company against cybersecurity risks.

Recommendations for European organizations

Palo Alto Networks recommends that organizations take the following steps to bolster their computing environments against cyberattacks:

1. Build a cybersecurity strategy that is focused on preventing cyberattacks at every step in the attack lifecycle.
2. Use next-generation security technology to enable employees to access the tools they need without compromising the organisation's security.
3. Educate everyone in the business on the key roles they play in preventing successful cyberattacks on the organization.

Research methodology

The survey was conducted online among 765 business decision-makers in companies with 1,000+ employees in the U.K., Germany, France, the Netherlands and Belgium by Redshift Research in October 2015.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com.

Palo Alto Networks and the Palo Alto Networks logo are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners.

Media contacts

Katherine James
Senior Manager, EMEA Public Relations and Analyst Relations
Palo Alto Networks
+44 (0)7887 522919
kjames@paloaltonetworks.com

[1] Based on findings from MicroMarketMonitor.