**CyberArk Survey Finds Executives Overly Reliant on Compliance Metrics to Measure Security Program Effectiveness**

December 9, 2015 8:30 AM ET

*Seventy-Nine Percent of IT Security Professionals Report to Executive Management on Compliance, Yet 59 Percent Say Threat Detection Metrics Are Most Critical*

NEWTON, Mass.--(BUSINESS WIRE)--Dec. 9, 2015-- New industry research sponsored by CyberArk (NASDAQ: CYBR) finds that one-third of CEOs and 43 percent of management teams are not regularly briefed on cyber security issues. Additionally, while 79 percent of IT security professionals are reporting on compliance metrics to demonstrate security program effectiveness, 59 percent state that threat detection metrics are most important.

An independent survey of global IT security professionals, "The Gap Between Executive Awareness and Enterprise Security," drills into the types of metrics used to measure security program effectiveness, frequency of reporting, and other factors such as budget and skills.

**The Cyber Security Gap: Executive Awareness and Responsibility**
The survey shows that 60 percent of respondents believe their organization can be breached. As cyber attacks grow in aggression and impact, CEOs and boards are being held accountable for the security posture of their organization. A closer look at the perceptions of IT security practitioners regarding executive cyber security leadership provides some clues into what's driving a lack of alignment:

- 61 percent believe that CEOs do not know enough about cyber security;
- 69 percent say cyber security is too technical for their CEO;
- 53 percent think that CEOs make business decisions without regard to security;
- 44 percent believe CEOs simply do not grasp the severity of today's risks.

**IT Security Professionals Need to Properly Educate Executives**
While IT security professionals are relying on executive-level leadership on security issues, CEOs are increasingly relying on their IT security teams to provide them with the security information that matters. The survey shows that the cyber security awareness gap may be driven in part by the need for security teams to properly educate CEOs on what's business critical when it comes to security:

- One-third of CEOs are still not regularly briefed on cyber security issues and related business risks;
- Forty-three percent of management teams do not regularly receive security status reports;
- Fifty-nine percent of respondents emphasized threat detection metrics as the most effective for measuring security program effectiveness, yet 79 percent still provide compliance and audit findings to their CEOs and executive teams;
- Executive visibility into security program effectiveness varies by industry with the highest percentage of respondents in financial services (72 percent) and healthcare (70 percent) saying they regularly provide executives with reports and metrics;
    - 50 percent or less of respondents in manufacturing, hospitality, transportation and non-profit industries said that they regularly provide reports and metrics to their executive teams;

"Compliance does not equal security. It can lull a CEO into a state of complacency because all it demonstrates is a simple checking of a box without context for responsible levels of information protection," said John Worrall, chief marketing officer, CyberArk. "Security professionals are briefing executives on the wrong information. They need to arm their CEOs and executive teams with information that matters such threat detection and risk metrics versus compliance and system availability."

**Is Budget a Barrier to Effective Cyber Security?**
Improving IT security fundamentals is a critical step in improving an organization's overall security posture. The survey

identified areas for improving organizational security:

- Seventy-five percent of respondents cited budgeting issues as the primary barrier to improving cyber security;
- In the face of a growing cyber security skills gap, 53 percent cited the lack of expertise as a primary barrier;
- Endpoint security and privileged account security were cited as the top two organizational security priorities over the coming year.

“Increasingly it’s CEOs who own the security agenda – whether they want to or not. One of our goals with this survey was to identify specific gaps between IT security and executive teams and help drive productive conversations that prioritize enterprise security,” continued Worrall. “By providing greater visibility into how cyber security programs are performing, and regularly communicating needs around budget and skills, IT security professionals will gain the support of the executive team and in turn help their organization become more proactive in protecting against advanced threats.”

To help support the need for greater executive guidance and dialogue around critical cyber security decisions, CyberArk recently launched a new industry initiative, the CISO View. The CISO View provides a forum for the CISO community to share best practices and tangible guidance for building effective cyber security programs. A new report, “The Balancing Act: The CISO View on Improving Privileged Access Controls,” features advice from a panel of CISOs from global 1000 enterprises about how to lead a comprehensive privileged account security program including recommendations for getting executive buy-in, delivering metrics that matter, and measuring effectiveness of the controls. The report is available for free at http://www.cyberark.com/cisoview.

“The Gap Between Executive Awareness and Enterprise Security” survey was conducted by Dimensional Research. The study, commissioned by CyberArk, surveyed 304 global IT security professionals. The primary research goal was to capture hard data on visibility and support of security programs at the executive level. In addition, researchers sought to determine which metrics are used to define security effectiveness.

**About CyberArk**
CyberArk is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the world’s leading companies – including 40 percent of the Fortune 100 and 17 of the world’s top 20 banks – to protect their highest value information assets, infrastructure and applications. A global company, CyberArk is headquartered in Petach Tikvah, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com, read the company blog, http://www.cyberark.com/blog/, follow on Twitter @CyberArk or Facebook at https://www.facebook.com/CyberArk.



View source version on businesswire.com: http://www.businesswire.com/news/home/20151209005201/en/

Source: CyberArk

**Media Relations Contacts:**
fama PR
Brian Merrill, +1-617-986-5005
cyberark@famapr.com
or
CyberArk
Liz Campbell, +1-617-558-2191

press@cyberark.com
or
**Investor Relations Contact:**
CyberArk
Erica Smith, +1 617-630-6426
ir@cyberark.com