Global Survey Finds 80 Per Cent Believe Cyber-Attacks Pose a Greater National Threat than Physical Attacks

Cyber-Ark's 7th Annual Advanced Threat Survey Finds More than Half of All Businesses Believe Hackers are Already Inside Their Networks; 57 Per Cent Put 'Too Much Faith in Perimeter Security'

Singapore. June 27, 2013 – 80 per cent of C-level executives and IT security professionals believe that cyber-attacks pose a greater risk to their nation than physical attacks, while 51 per cent believe a cyber-attacker is currently in their corporate network, or has been in the past year. The findings are part of Cyber-Ark's 7th annual Global Advanced Threat Landscape survey – developed through interviews with 989 IT and C-level executives across North America, Europe, and Asia Pacific. The full survey can be downloaded for free here (attached). Analysis of this year's survey shows that continued reports of nation-based attacks on global critical infrastructure and businesses, combined with high-profile data breaches such as the NSA leak, have made the industry acutely aware of the threat that today's cyber-attackers pose. Despite this awareness, businesses still have a lot of work to do to secure the enterprise from advanced attacks. Cyber-attackers are continuing to breach perimeter security at an accelerated rate. As a result, businesses need to assume the attackers are already inside their network and focus on securing the access points to the critical data and assets that the attackers covet.

Key findings of the 2013 survey include:

- **Advanced Attacks Represent Grave Threats to National Security, Business and the Economy**
  - 80 per cent of respondents believe that cyber-attacks pose a greater threat to their nation than physical attacks.
    - § In last year's survey, 71 per cent of respondents indicated they were more fearful of insider attacks than outside cyber-attacks, but almost two thirds of respondents indicated that external cyber-attack threats would become a greater security risk in 1 to 3 years[1]. This year's survey validates that notion.
  - 61 per cent of respondents believe that government and legislative action can help protect critical infrastructure against advanced threats. This number was the lowest in the U.S., where only 57 per cent believe legislation will be an effective tool, as opposed to 64 per cent of respondents in Europe and 61 per cent in APAC.

- **The Perceived Failure of Perimeter Security – Attackers Already Inside**

- Advanced attacks are almost always precipitated by perimeter-oriented tactical aggressions, such as phishing attempts. The increasing ease with which attackers are breaching the enterprise perimeter is eroding confidence in perimeter security.
- 57 per cent of respondents believe their company puts too much faith in perimeter security.
- 51 per cent of respondents believe a cyber-attacker is currently on their network – or has been in the past year.

- **Privileged Accounts as an Advanced Threat Vulnerability**
  - It's been firmly established through multiple industry reports that privileged accounts have emerged as the primary target for advanced enterprise attacks[2][3][4]. Privileged accounts consist of privileged and administrative accounts, default and hardcoded passwords, application backdoors, and more.
  - 64 per cent of respondents indicate they are now managing privileged accounts as an advanced threat security vulnerability.
  - Despite this growing awareness, 39 per cent of respondents either don't know how to identify where privileged accounts exist or are doing so manually.
    - In a recent survey, Cyber-Ark discovered that 86 per cent of large enterprises either don't know or had grossly underestimated the magnitude of their privileged account security problem[5].

- **Companies Lose Control of Privileges in the Cloud**
  - 56 per cent of respondents do not know what their cloud service providers are doing to protect and monitor privileged accounts.
  - 25 per cent of respondents felt they were better equipped to protect their confidential information than their cloud provider – and yet they still entrust the third party with their data.

Supporting Quote

"People around the world are acutely aware of the global threat cyber-attacks represent. Cyber-attackers have repeatedly demonstrated the ability to disrupt national financial systems, cause harm to critical infrastructure and severely damage businesses and economies," said John Worrall, CMO of Cyber-Ark. "To achieve their goals, outside attackers must steal the privileged credentials of an authorised user to gain the access necessary to meet their objectives. This level of threat requires a proactive approach to security that protects and monitors the access points to the critical data and assets that attackers are targeting."

Full Research Brief:

http://www.cyber-ark.com/landing-pages/global-advanced-threat-survey/index.asp?utm_source=Release&utm_medium=PR&utm_campaign=GATL

Twitter: @CyberArk

Free Privileged Account Security Risk Assessment: http://www.cyber-ark.com/discover-dna

About Cyber-Ark

Cyber-Ark® Software is a global information security company that specialises in protecting and managing privileged users, sessions, applications and sensitive information to improve compliance, productivity and protect organisations against insider threats and advanced external threats. With its award-winning Privileged Identity Management, Privileged Session Management and Sensitive Information Management Suites, organisations can more effectively manage and govern data centre access and activities, whether on-premise, off-premise or in the cloud, while demonstrating returns on security investments. Cyber-Ark works with more than 1,200 customers, including more than 40 per cent of the Fortune 100. Headquartered in Newton, Mass., Cyber-Ark has offices and authorised partners in North America, Europe and Asia Pacific. For more information, please visit www.cyber-ark.com.