Global Advanced Threat Landscape Survey

June 2013

Cyber-Ark®

Table of Contents

Executive Summary

Cyber-Ark's 2013 Global Advanced Threat Landscape survey is the seventh in a series of annual surveys that focus on identifying global cyber-security trends. This year's survey has been updated to reflect the challenges that global organizations face in dealing with a significant increase in advanced targeted attacks.

The survey report is the result of interviews with 989 IT security and C-level executives (CEO, CIO, CSO) across North America, Europe, and Asia Pacific (APAC). The primary findings include:

Advanced Attacks Represent Grave Threats to National Security, Business and the Economy

Businesses are facing more sophisticated, advanced targeted attacks in recent years, especially companies and organizations that fall under the banner of critical infrastructure (this includes electricity generation, gas production, oil, water supply, telecommunications, financial services, etc…)[1]. Recent news reports on nation-based attacks out of Iran and China on US infrastructure, the DDoS attacks on South Korea's financial system, and more, have increased awareness of the growing threat of cyber-attacks. On a daily basis it seems, businesses are victims of IP theft and are faced with attacks that steal customer data, inflict reputational damage and cost large amounts of time and money to resolve. The survey reveals that these increasing attacks have had a significant impact on the global view of the threat cyber-attacks represent:

- **80 percent of respondents now believe that cyber-attacks pose a greater threat to their nation than physical attacks.**
- **In the face of this threat, 61 percent of respondents believe that government/legislative efforts can protect critical infrastructure against advanced threats.**

The Failure of Perimeter Security – Attackers are Already Inside

Advanced attacks are almost always precipitated by perimeter-oriented tactical aggressions (such as phishing). The increasing ease with which cyber-attackers breach perimeter security has generated considerable discussion of the on-going value of perimeter security. The survey results show:

- **57 percent of respondents believe their company puts too much faith in perimeter security.**
- **51 percent of respondents believe a cyber-attacker is currently on their network, or has been on their network in the past year.**

1 U.S. Department of Homeland Security, "Joint Security Awareness Report," May 2013

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. Privileged accounts can be found in any device with a microprocessor, including PCs, databases, networked devices like copiers, operating systems and more. These accounts have been used to perpetrate some of the most devastating business attacks, including RSA, Global Payments, Saudi Aramco, MasterCard/Visa, and the U.S. Chamber of Commerce, among others. Businesses have traditionally managed privileged accounts as an audit check box. The survey results demonstrate that privileged accounts have transitioned from primarily an audit concern to an advanced threat security concern, with more businesses viewing them as a critical part of their security strategy:

- **64 percent of respondents indicated that they now manage privileged accounts as an advanced threat security vulnerability.**
- **Despite this awareness, 39 percent of respondents either don't know how to identify where privileged accounts exist, or they are doing so manually.**
  - ***In a previous survey, Cyber-Ark discovered that 86 percent of large enterprises either do not know, or have grossly underestimated the magnitude of their privileged account security problem.[5]***

Companies Losing Privilege Controls in the Cloud

Despite growing awareness of the critical role unmanaged privileged accounts play in APTs, the majority of organizations are not applying this lesson across their entire infrastructure. As more organizations outsource infrastructure to cloud providers, it's critical they identify and understand how providers, partners, customers and anyone with access to their network manages their privileged accounts.

The survey results demonstrate that the majority of companies are unaware of whether their cloud service providers employ privileged account security:

- **56 percent of respondents do not know what their cloud service providers are doing to protect and monitor privileged accounts.**
- **25 percent of respondents felt they were better equipped to protect their company's confidential information than their cloud service provider – and yet they still entrust their information to the third party.**

Cyber-Ark's View:

The survey demonstrates that while the industry is acutely aware of the threat that today's cyber-attackers pose, there is still a lot of work to do to fully secure the enterprise from advanced threats. With more attackers assumed to have breached the perimeter, Cyber-Ark recommends taking a proactive approach to security, focused first on securing the critical data and assets that attackers covet, and only then moving outward towards the perimeter to the initial access point.

The survey shows that **motivated attackers will find a way into the network. A comprehensive privileged account security solution can deny the attacker the easy path to compromising a network**. For a full list of best practice, privileged account security recommendations please see page 11.

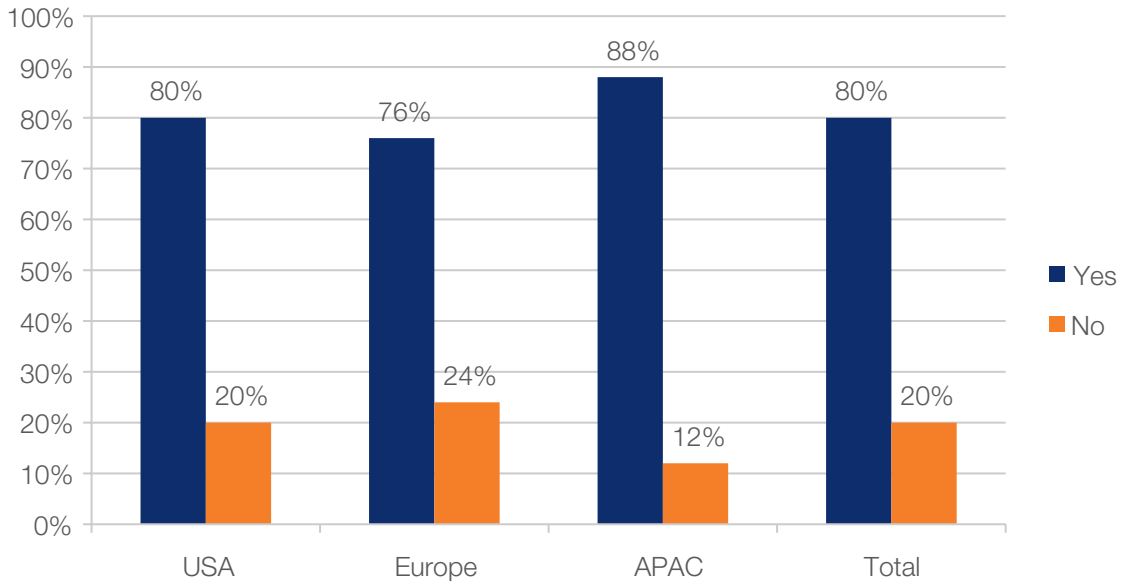
2 CyberSheath, "APT Privileged Account Exploitation," April 2013
3 Mandiant, "Exposing One of China's Cyber Espionage Units," Feb. 2013
4 Verizon, "2013 Data Breach Investigations Report," May 2013
5 Cyber-Ark, "Privileged Account Security & Compliance Survey," May 2013

Key Report Findings

The Future of National Security – Cyber-Attacks Represent Greater Threat than Physical Attacks

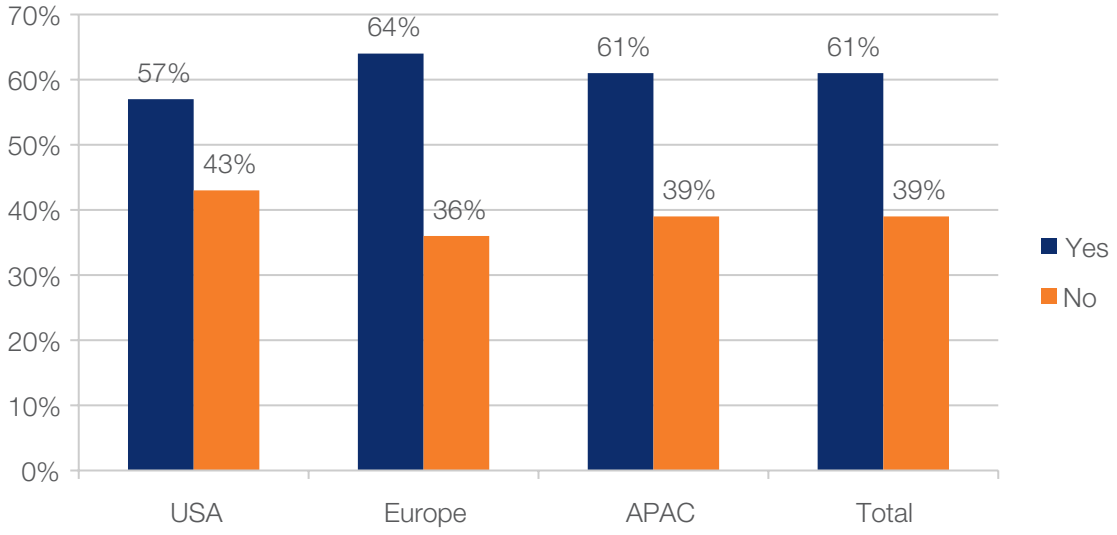
In the face of increasing attacks on businesses and critical infrastructure, 80 percent of respondents believe that cyber-attacks now pose a greater threat to their nation than physical terrorist attacks. The responses were similar, regardless of their global region.

Fig. 1: Do You Believe Cyber-Attacks Pose A Greater Threat To Our Nation Than Physical Attacks?



Despite facing this growing threat, nearly 2 out of 3 respondents believe that government legislation can help thwart critical infrastructure attacks. These numbers were somewhat surprising, given frequent industry discussion about how compliance and over-legislation can have a negative impact on business.

Fig. 2: Do You Believe Legislative Efforts Can Help Our Country Protect Business And Critical Infrastructure Against Advanced Threats?



External Attackers Already Inside – Erosion of Perimeter Security

Almost every advanced attack is precipitated by perimeter-oriented tactical attacks, many of which are not sophisticated, such as spear phishing attacks. The success of these perimeter intrusions has led to a decrease in confidence of perimeter security. **When asked whether their company puts too much faith in anti-virus and perimeter security, 57 percent responded yes. Amazingly, 51 percent of respondents believe that an attacker is currently in their network, or has breached their network in the past year**. This demonstrates the ease of which perimeter security is breached – and why organizations need to secure their organization from the inside out, protecting the actual targets of cyber-attackers. ***Cyber-Ark recommends isolating, monitoring and controlling every access point to all critical business systems – attackers may get past perimeter security, but they should find locked doors across the network, making movement extremely difficult.***

Fig. 3:

Do You Think Your Company Puts Too Much Faith In Anti-Virus And Perimeter Security?

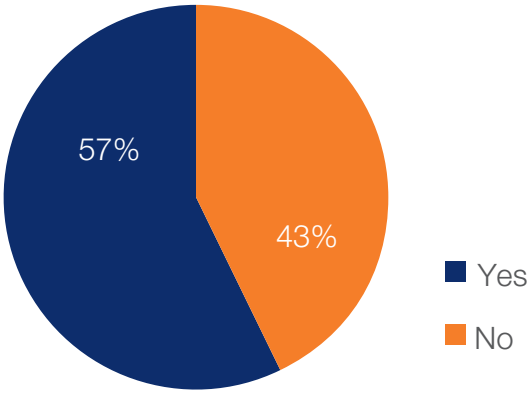
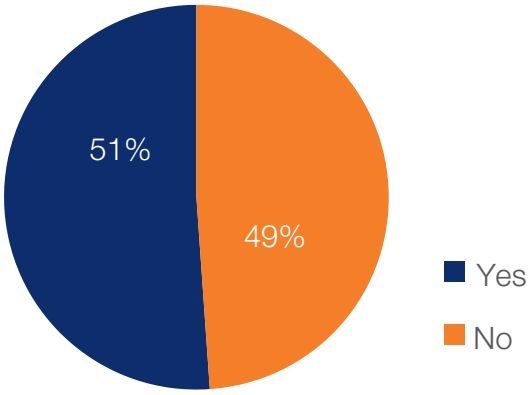


Fig. 4:

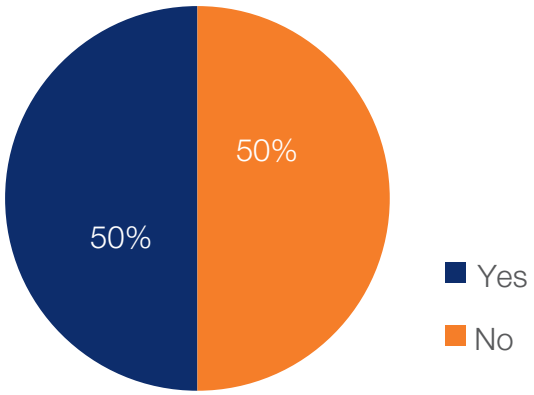
Do You Believe A Cyber-Attacker Is Currently In Your Network Or Has Breached Your Network In The Past Year?



Given the numerous attacks and intrusions organizations face, half of all respondents are deploying security strategies that assume the perimeter has already been breached. ***Cyber-Ark recommends a proactive approach to security – putting tight controls around what really matters: a business's high risk data.***

Fig. 5:

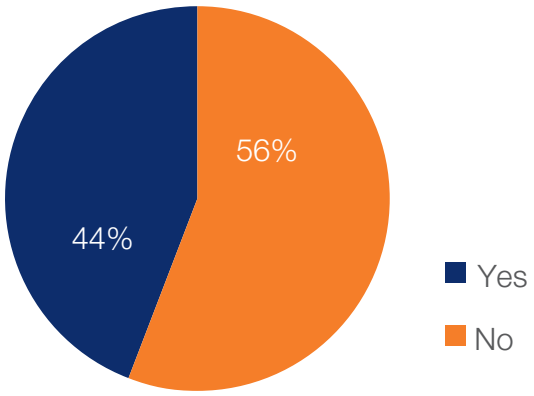
Does Your Security Strategy Assume That The Perimeter Has Already Been Breached?



Of the organizations that have been breached in the past year, 44 percent believe that the breach resulted in sensitive data or intellectual property being stolen. Cyber-Ark believes this is a low number, but it's recognition of the fact that more companies are assuming their perimeter will be breached eventually and are trying to focus their security efforts on the internal targets of the attackers.

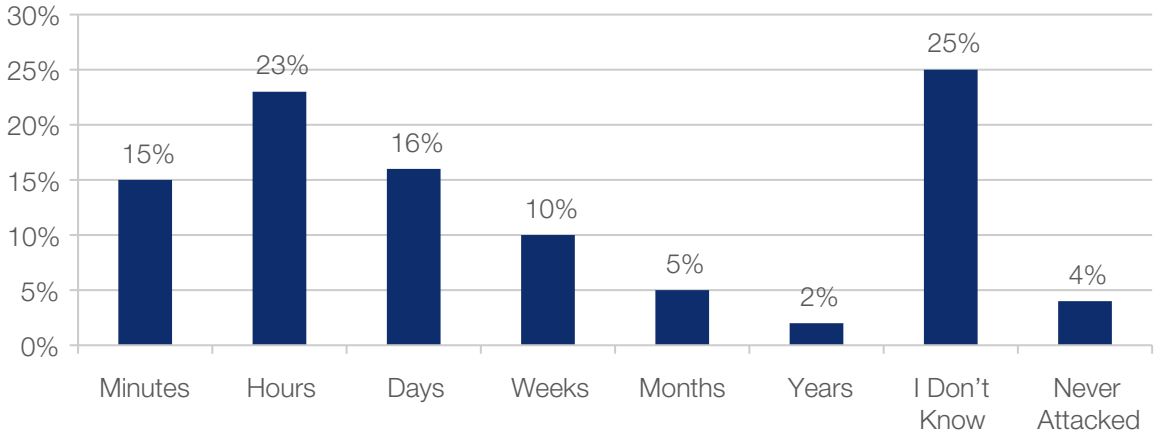
Fig. 6:

If Yes - Do You Believe Outsiders Could Have Received Highly Sensitive IP/Data From Your Organization via Unauthorized Access To Your Corporate Network?



Despite the recent Verizon data breach report stating that 62 percent of businesses take months or years to detect a breach, 38 percent of respondents to the Cyber-Ark survey indicated they can detect an attack in minutes or hours.[6] The results show the hit-or-miss nature of detection, which is why businesses should protect internal attack targets like privileged accounts and assume the attackers are inside. According to a recent report[7], once the attackers control privileged accounts, they can "delete logs to make forensic analytics difficult…and evade detection by opening more doors." ***Cyber-Ark recommends monitoring all privileged account activity to determine anomalous behavior immediately. Integrated privileged activity monitoring with SEIM provides a comprehensive view of all activity.***

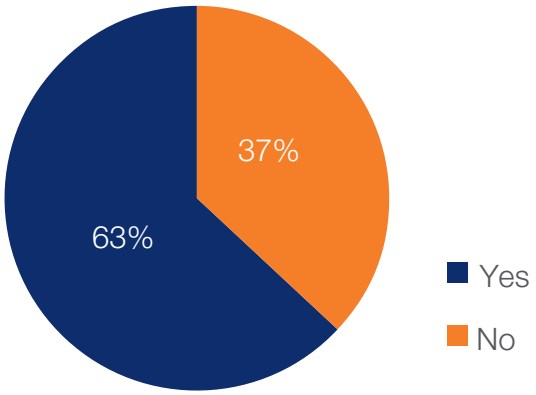
Fig. 7 How Long Does It Take You To Discover That You Have Been Attacked?



Privileged Accounts as an Advanced Threat Vulnerability

Businesses have traditionally viewed privileged accounts as an audit check box. The survey results demonstrate that privileged accounts have transitioned from primarily an audit concern to an advanced threat security concern. 63 percent of respondents now manage and secure privileged accounts as an advanced threat security vulnerability.

Fig. 8: Do You Manage And Secure Privileged Accounts As An Advanced Threat Security Vulnerability?

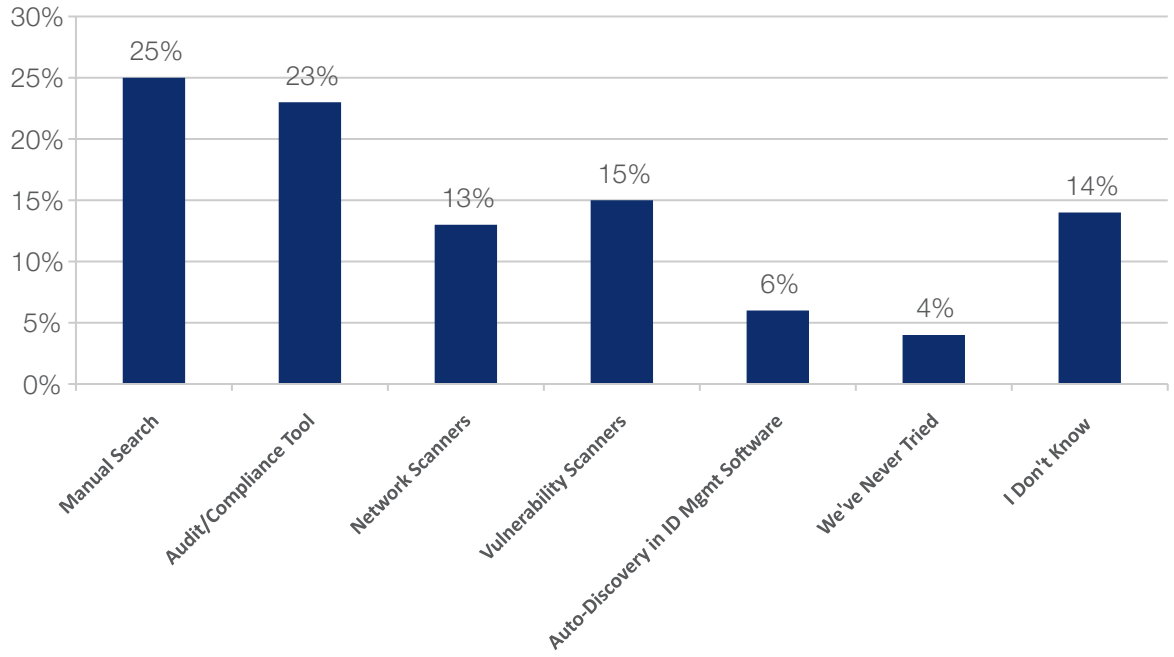


6 Verizon "2013 Data Breach Investigations Report," May 2013
7 CyberSheath: "APT Privileged Account Exploitation," May 2013

Despite nearly two thirds of companies recognizing and trying to secure privileged accounts as part of their APT security strategy, organizations are still struggling with how to identify where privileged accounts exist. When asked how they were identifying privileged accounts, 39 percent of respondents either don't know how to identify where privileged accounts exist, or are conducting manual searches, while 38 percent of respondents are using partial solutions that have limited capabilities.

This inability to discover privileged accounts could explain why a previous Cyber-Ark survey discovered that the majority of organizations fail to accurately scope the size of their privileged account security risk – with 86 percent of large enterprises either not knowing or grossly underestimating the magnitude of their privileged account security problem[8]. ***Cyber-Ark recommends using a privileged account security solution to automate the discovery process and find "hidden accounts," enforce controls, and provide a clear audit trail for accountability and security.***

Fig. 9: How Does Your Company Identify Where Privileged Accounts Exist?

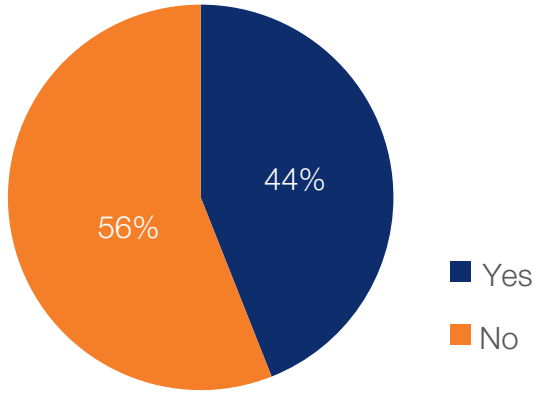


8 Cyber-Ark "Privileged Account Security & Compliance Survey," May 2013

Cloud Privileges – The Great Unknown

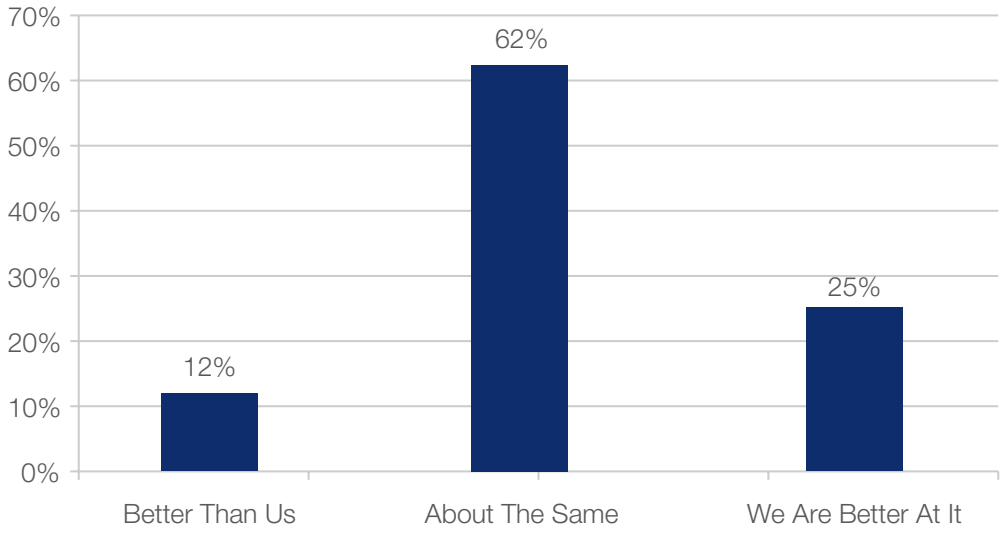
Despite growing awareness of the critical role privileged accounts play in APTs, the majority of organizations don't apply this lesson across their entire infrastructure. As more organizations outsource infrastructure to cloud providers, it's critical they identify and understand how providers, partners, customers and anyone with access to their network manages their privileged accounts. **56 percent of respondents stated that they did not know what their cloud provider was doing to protect and monitor privileged accounts.**

Fig. 10: Do You Know What Your Cloud Service Providers Are Doing To Protect And Monitor Privileged Accounts?



Cyber-attackers understand that third-party providers and partners can present a weak spot to get backdoor access into a target organization. When selecting providers and partners, security should be a priority. Despite this, only 12 percent of respondents use a cloud provider that protects confidential information better than their own organization. Amazingly, 25 percent of respondents partner with cloud providers that provide less security than the organization itself.

Fig. 11: Do You Feel Confident That Your Cloud Service Provider Can Protect Your Company's Confidential Information?



Cyber-Ark's Best Practice Recommendations for Preventing Privileged Account Compromise

- **Isolate, monitor and control every access point to all critical business systems**
- **Change default passwords on all servers, databases, applications and network devices**
- **Remove hard-coded passwords from scripts, configuration files and applications**
- **Employ technical means of automatically enforcing enterprise password policies**
- **Control access by enforcing least privilege**
- **Use multi-factor authentication for access to privileged accounts**
- **Increase password complexity**
- **Use a unique password for each local administrator account**
- **Remove local administrator rights from the majority of users**
- **Reduce the number of privileged domain-wide service accounts**
- **Automatically change passwords on a periodic basis and immediately upon suspicion of misuse**
- **Monitor and record all activities associated with administrative and privileged accounts**
- **Implement tamper-proof logging, auditing, and alerting on privileged access**

About Cyber-Ark

Cyber-Ark® Software is a global information security company that specializes in protecting and managing privileged users, sessions, applications and sensitive information to improve compliance, productivity and protect organizations against insider threats and advanced external threats. With its award-winning Privileged Identity Management, Privileged Session Management and Sensitive Information Management Suites, organizations can more effectively manage and govern data center access and activities, whether on-premise, off-premise or in the cloud, while demonstrating returns on security investments. Cyber-Ark works with more than 1,300 customers, including more than 40 percent of the Fortune 100. Headquartered in Newton, Mass., Cyber-Ark has offices and authorized partners in North America, Europe and Asia Pacific.

For more information, please visit www.cyber-ark.com.

Media inquiries:

Christy Lynch

Cyber-Ark Software, Inc.
Phone: +1 617-796-3210
Email: christy.lynch@cyber-ark.com

Brian Merrill

fama PR (US)
Phone: +1 617-986-5005
Email: cyber-ark@famapr.com