Password Management receives vote of no confidence from IT Managers

Submitted by: Eskenzi PR Limited
Thursday, 9 June 2005

For Immediate Release 9th June 2005
PRESS RELEASE
Password Management receives vote of no confidence from IT Managers

Passwords are the most basic element of any IT security system, yet new research findings revealed today show that many organisations are still tripping up at this first security hurdle. According to new research into “password management” conducted by Cyber-Ark Software, specialists in Digital Vaulting, approximately half of IT managers employed in the largest organisations are not very confident that administrative passwords are stored securely. The research also found that not much has changed when it comes to securely storing user passwords with IT managers estimating that 19% of their colleagues still keep their passwords on post-it notes.

The research was carried out at Infosecurity Europe 2005 – Europe’s largest IT security event to find out how securely companies are storing and managing their administrative and user passwords. It was conducted amongst 175 IT professionals with a quarter coming from organisations employing over 5000 people.

Less than a third (32 percent) were storing passwords digitally. The remainder continued to use labour-intensive, manual processes, including paper copies stored everywhere from locked cabinets to physical safes which hinders efforts for regular and on-demand resetting of passwords.

Considering that administrative passwords are the “keys to the kingdom” and give access to the most confidential information on the network which is often seen as one of the major risk factors that can lead to internal fraud, it is alarming to note that nearly 10% of companies never change their mission critical administrative passwords and most shocking of all 5% don’t even change the manufacturer’s default password on their systems.

Other findings revealed:
- 14% still keep administrative passwords in an excel file – which is known to be insecure.
- 25% of IT staff can access administrative passwords without permission.
- 15% of large organisations never have their security practices audited.
- 62% of companies have now seen an increase in auditing of their security practices due to recent legislation.
- 14% have no password change management policy, which means they have no way of controlling who has access to systems

One IT security director who was interviewed for the survey admitted to keeping all the administrative passwords in his mobile phone explaining that he thought this was “a very safe place”. His IT security colleague standing within ear-shot replied “Wait till I tells the guys back in the office, you’ll never live this one down.”

“It would appear from this research that password management is still a major bugbear for many

organizations with two thirds who are still relying on the old-fashioned method of physically managing and storing passwords. Because this process can be so time-consuming and laborious IT staff often circumvent the security processes which can then open them up to potential security breaches." said Tom Crawford, president and CEO of Cyber-Ark. "However companies can now simplify the management of administrative passwords by using a digital vault which can securely automate administrative passwords in a cost-effective and efficient way."

Already, Cyber-Ark's Network Vault for Passwords has helped hundreds of organizations including Mohegan Sun and European direct debit processor Voca, which recently transitioned its password management, replacing the physical safes used to store over 800 administrative passwords and redeploying staff dedicated to administering passwords.

"Cyber-Ark has cracked the code for automating a potentially insecure and immensely time-consuming process of storing and managing administrative passwords," said Keith Reeve, Manager Certification Authority and Access Control, Voca. "We've replaced physical safes with virtual ones, using Network Vault for Passwords to securely automate administrative passwords critical to the systems that support our business."

Organizations interested in viewing how much they can save by migrating to automated, electronic Vaulting of administrative passwords should visit Cyber-Ark's Password Vault ROI calculator at www.cyber-ark.com.

About Cyber-Ark Software

Cyber-Ark Software is the leader in Vaulting solutions for securely connecting enterprises. The Company's Inter-Business Vault enables the creation of secure instant wide area networks (WANs) for connecting enterprises with partners, customers and sub-contractors over the Internet - enabling them to exchange information as if they have deployed a shared WAN, but without actually doing so. Cyber-Ark's leading Inter-Business Vault applications include solutions for Treasury Management files, PLM and CAD/CAM files, and Source Code. In addition to its business-to-business solutions, Cyber-Ark's Network Vault provides solutions for securely managing critical information, such as administrative passwords and critical documents, within the enterprise. Today Cyber-Ark enjoys strong customer relationships with more than 100 Global 1000 companies around the world.

Founded by a group of leading military security experts and computer engineers, Cyber-Ark Software is privately held and backed by some of the world's most successful venture capitalists, including Jerusalem Venture Partners, Seed Capital Partners (a SOFTBANK Affiliate), JP Morgan/Chase Partners and Vertex Management.

The Company is located in Dedham, Mass. and on the World Wide Web at www.cyber-ark.com.
# # #

For further information contact:
Yvonne Eskenzi
Eskenzi PR Limited
020 8449 8292
email yvonne@eskenzipr.com