2012 Trust, Security & Passwords Survey

June 2012

Contents page

Executive Summary

Cyber-Ark's 2012 Trust, Security & Passwords survey is the sixth in a series of annual surveys focused on identifying key security trends amongst IT workers. The survey assesses the extent to which privileged accounts and passwords are being protected in organizations today, and also provides insight into the core threats that exist and the measures being taken to defend systems.

The survey report is the result of interviews with 820 IT managers and C-level professionals across North America and EMEA, primarily from enterprise companies.

The security landscape continues to evolve – businesses can no longer simply focus on securing the network perimeter in hopes of keeping attackers out. As the enterprise perimeter dissolves, and reports of internal and external threats increase, privileged access points have emerged as the primary target for enterprise attacks. Privileged access points consist of privileged and administrative accounts, default and hardcoded passwords, application backdoors, and more. These accounts act as a gateway to an organization's most sensitive data accessible across systems, applications and servers.

The research reveals that while insiders continue to be perceived as the biggest risk organizations face in securing against data breaches, a majority of respondents agree that all recent security breaches – internal and external – involved the exploitation of privileged accounts. The continued exploitation of these accounts in some of the industry's most notorious data breaches is a significant factor in the growing recognition of the "privileged connection." Businesses need to continue to be vigilant in securing and managing these high value targets.

Key Report Findings

Insiders Considered Greatest Organizational Security Threat
71 percent of respondents believe that the insider threat is the priority security concern for their organization. Whether through accidental or malicious breach, internal employees have the access and system knowledge to perpetrate potentially devastating attacks.

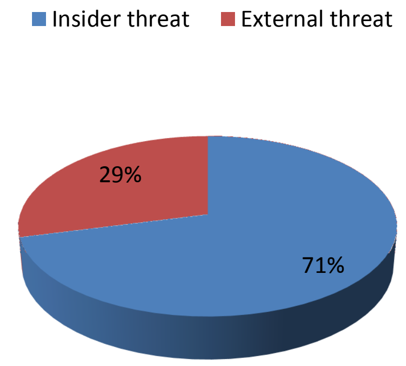


Figure 1: What do you consider to be the greatest security threat to your organisation at present?

The perception of the insider threat posing the most significant business risk is juxtaposed by last year's findings. When asked the question – 'In the next 1 – 3 years, do you see external threats becoming a greater security risk than insider threats?' – 57 percent of respondents believed that external attacks would surpass the insider threat in terms of security risk. The pathways for insider risk (accidental data loss, stolen devices, malicious hacks) may be a contributing factor to why it is still considered the highest security priority.

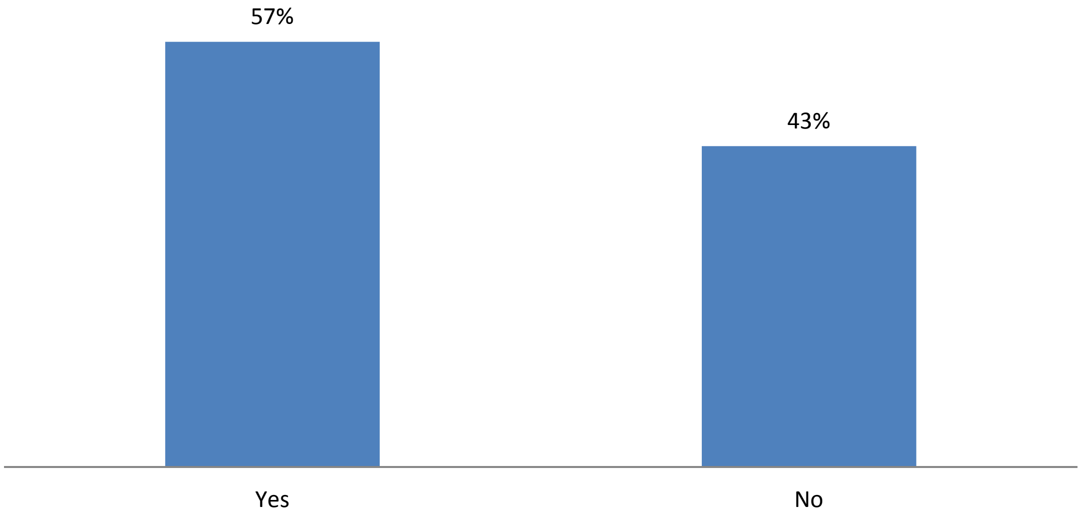


Figure 2: In the next 1-3 years, do you see external threats, such as cyber criminals, becoming a greater security risk than insider threats? (2011)

Privileged Accounts Are Increasingly Targeted – Regardless of Attack Entry Point

More than two thirds (64 percent) of respondents believe that the majority of recent security attacks have involved the exploitation of privileged account access. Whether it's a malicious insider, or an external attacker looking to exploit privileged accounts to gain access to sensitive information, these privileged access points accounts have emerged as the priority target for cyber-assaults. Attackers have used the privileged pathway to penetrate some of the most spectacular breaches over the past couple of years, including RSA and Global Payments.

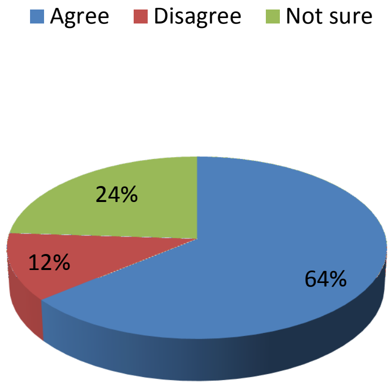


Figure 3: Do you agree that the majority of recent security attacks have involved the exploitation of privileged account access?

High Profile Security Incidents Impact Organizational Security Strategies

2011 was marked by some of the industry's most high profile and devastating attacks and security breaches, including attacks on NASDAQ Directors' Desk, RSA, and the U.S. Chamber of Commerce. The high profile nature of these attacks resulted in more than half of responding organizations to change or re-think their security strategies. Businesses realize that regardless of how the attackers were getting in (phishing, malware, infected applications, etc…) current security approaches were insufficient in stopping the infiltrations.

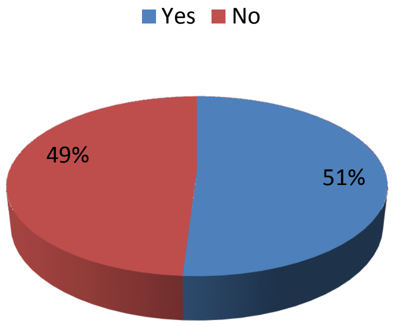
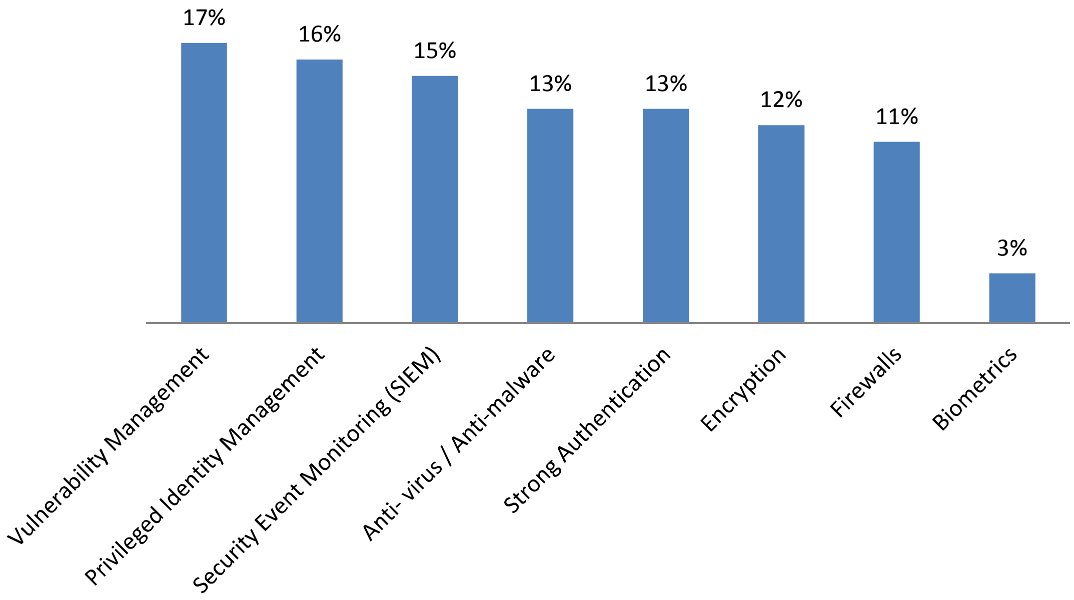


Figure 4: Have high profile security incidents, such as the RSA hack, made you rethink your security strategy this year?

Organizations are taking a broad approach to security in 2012
The top three security priorities identified by respondents were Privileged Identity Management, Vulnerability Management and Security Event Monitoring. As breaches continue to demonstrate cyber-attackers' abilities to get inside an organization, businesses are putting a higher priority on securing internal assets before further investing in perimeter security.

Figure 5: What are your main IT security priorities for 2012?



Increasing Number of Organizations at Risk by Failing to Monitor Privileged Accounts
Despite growing awareness of the privileged connection to high profile security incidents, only 57 percent of respondents indicated they were currently monitoring the use of privileged accounts; 43 percent stated that either they did not monitor the accounts, or were simply unaware. These privileged accounts are often protected by weak or default passwords, which are seldom replaced. Businesses that are not securing and managing these high value targets are failing to uphold their responsibility for securing customer and similar sensitive information. As more businesses understand that almost every data breach has a privileged connection – we expect these numbers to continue to grow as businesses become more proactive about protecting their critical information assets.

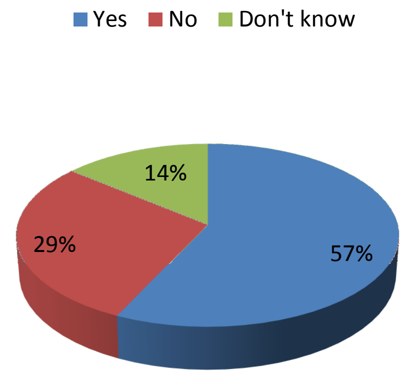


Figure 6: Is your use of privileged accounts monitored?

Insiders Get Around Current Controls

The report also reveals that a staggering 52 percent of respondents are able to get around controls put in place to monitor privileged access. From that, one could conclude that present methods of managing privilege accounts are failing.

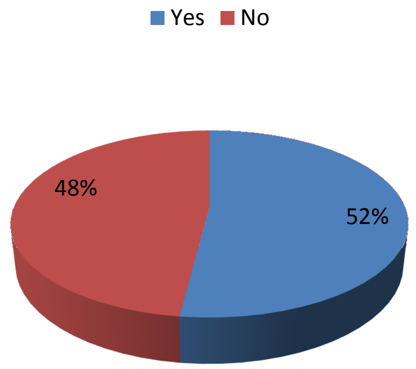


Figure 7: Can you get around any controls that have been put in place to monitor your privileged access?

Employees Accessing Unauthorized Information

Nearly half of all respondents indicated that they've accessed information on a system that was not relevant to their role. Whether curiosity or malicious intent is the driver, unauthorized access by insiders remains a significant threat to sensitive information.

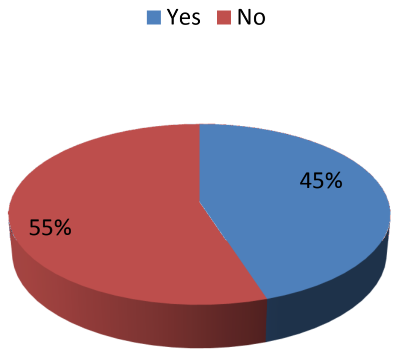


Figure 8: Have you ever accessed information on a system that was not relevant to your role?

Administrative Passwords – Wide Ranging Access

The use of administrator passwords to access sensitive or confidential information should come as no surprise. Privileged accounts are an organizations most powerful access points and are the keys to unlocking a company's most valuable asset – its data. With 42 percent of respondents claiming that they, or their colleagues, have used their administrator passwords to access confidential information, the potential for damage is huge if these accounts are not used for legitimate purposes.

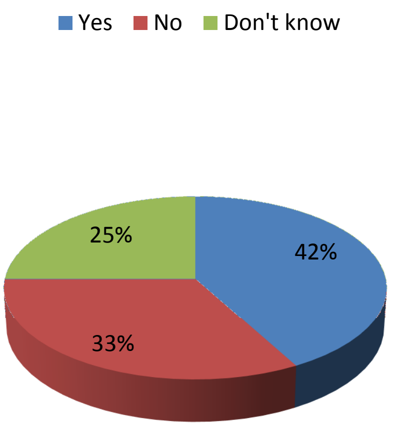


Figure 9: Have you or any of your colleagues used an administrator password to access information that was otherwise confidential or sensitive?

Employees Plan on Taking Privileged Passwords on Way Out
In response to the question, 'If you were told that you were going to be fired tomorrow, what, if anything would you take with you?' nearly half of respondents said they would take something. Of these, customer databases and privileged password lists topped respondents' named items.

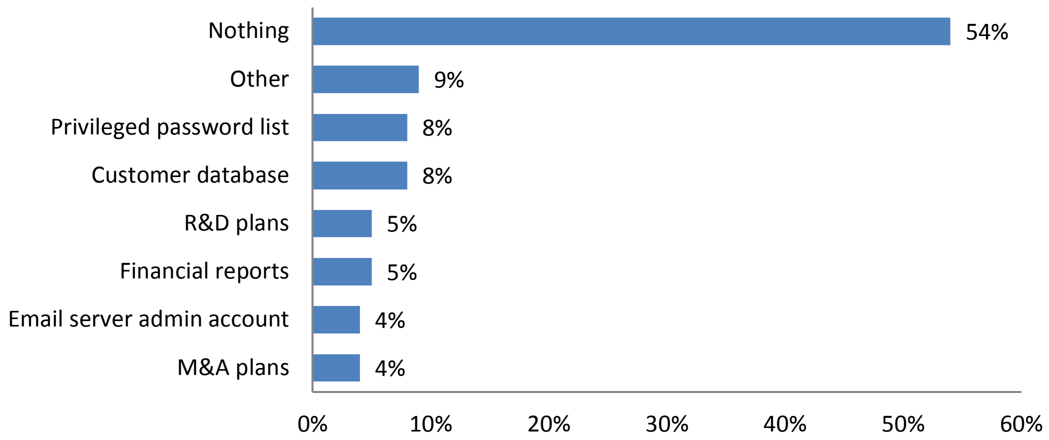


Figure 10: If you were told that you were going to be fired tomorrow, what, if anything would you take with you?

For those who would take information with them, customer databases have remained consistently top of the list, while privileged password lists have also been front of mind for respondents – stressing the value that they hold.

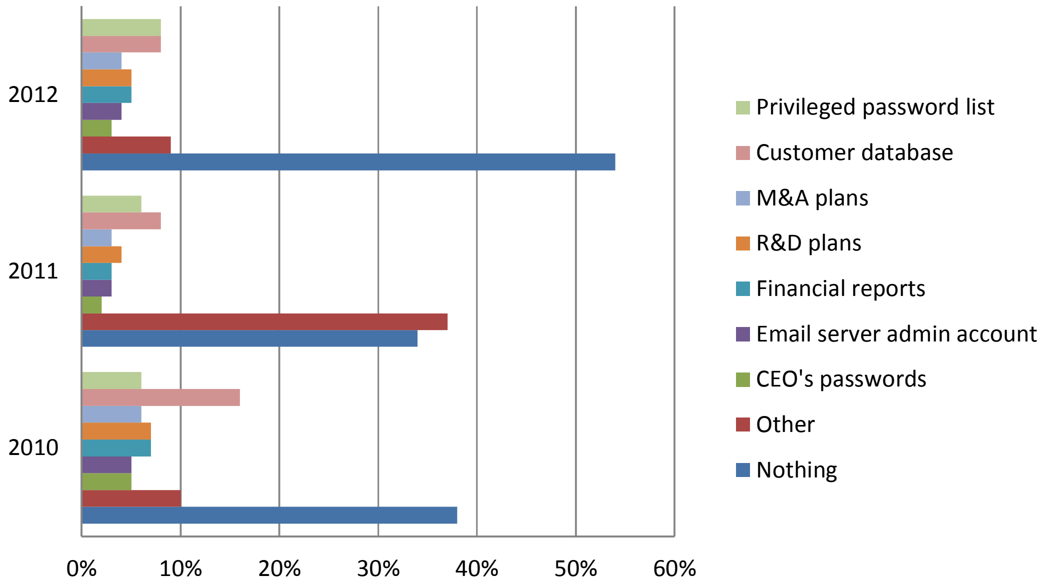


Figure 11: If you were told that you were going to be fired tomorrow, what, if anything would you take with you? (2010 – 2012 data)

When asked if they believed that they had a right to this information, 86 percent of respondents admitted that they knew they had no right to take this data.

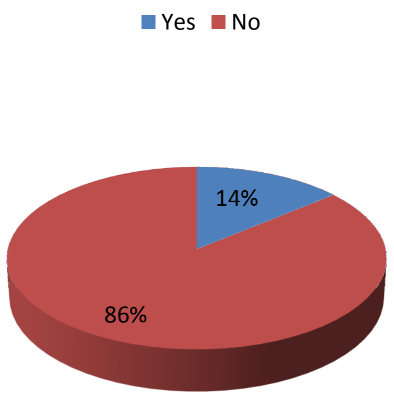


Figure 12: Do you think you have the right to take any information with you when you leave a company and are no longer employed by an organization

Intellectual Property – Competitive Theft

In a concerning trend, 55 percent of respondents revealed that they suspect that their competitors have received some of their company's highly sensitive information.

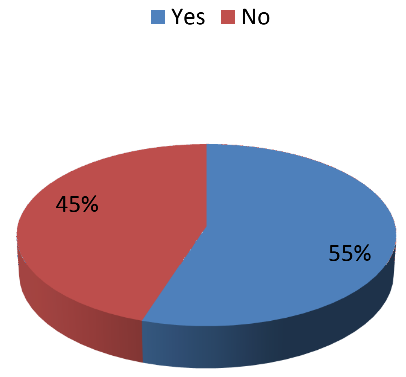


Figure 13: Do you suspect that your competitors have ever received any of your company's highly sensitive information or intellectual property?

These figures mark a significant increase over 2010 and 2011 survey data – which may indicate a growing problem.

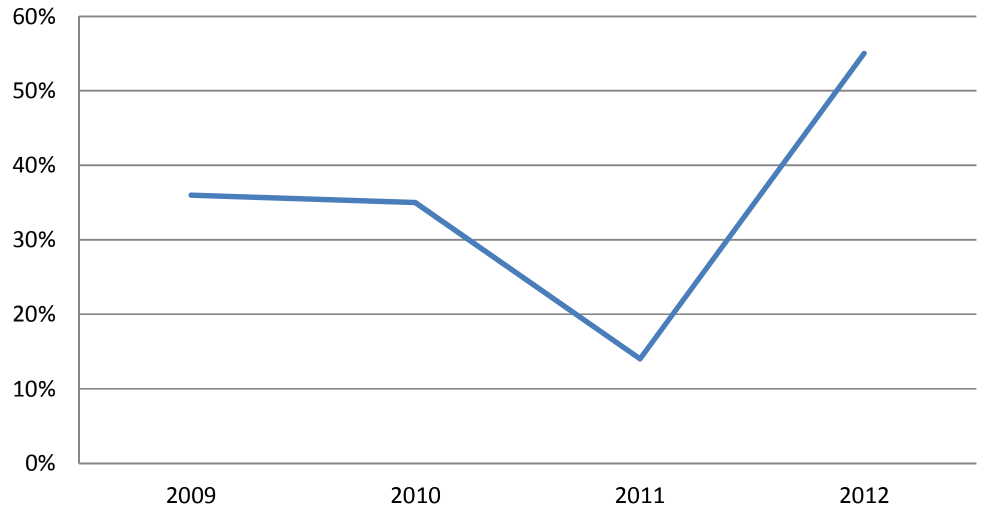


Figure 14: Do you suspect that your competitors have ever received any of your company's highly sensitive information or intellectual property? ('Yes' respondent 2010 – 2012)

Data Breach Notification Laws Fail to Curb Data Loss

In both Europe and the US, data breach notification laws have been enacted in varying degrees. 46 states in the US have enacted legislation requiring notification of security breaches involving personal information. Whereas in Europe, the EU's new data protection laws, which include an obligation for organizations to reveal the detail of a security breach within 24 hours, will be rolled out to all member states by 2014. In Europe, additional legislation, such as Germany's data breach notification laws, and the UK's Information Commissioner's Office (ICO), which has the power to fine organizations up to £500,000 for breaches of the current UK Data Protection Act, also play their part.

Despite these regulatory efforts, nearly 3 out of every 4 companies believe that data breach notification laws are ineffective in curbing data loss.

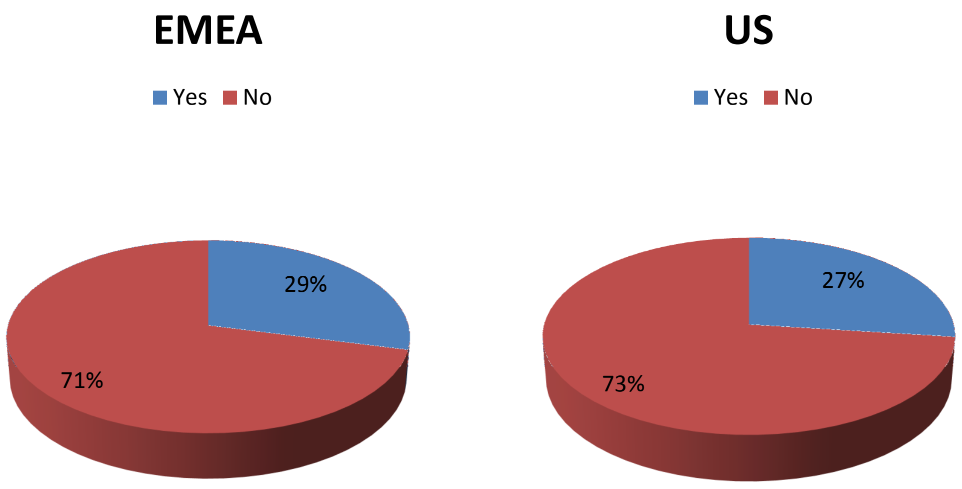


Figure 15: Do you believe that data breach notification laws are effective in curbing data loss?

Appendix 1 – Sample

This is Cyber-Ark's sixth report on this subject, and over the time the methodology and sample size has grown and changed, but the subject matter has remained constant.

This year, Cyber-Ark surveyed 408 respondents in EMEA and 412 in the US at a number of industry events. The respondents were from a variety of industry sectors and organization size ranged from small to medium sized companies, to large enterprises (10,000+ employees). All respondents worked in or had an association with the IT department. The full breakdown of respondents is as follows:

Job level	GLOBAL	EMEA	US
C-Level Executive	64	21	43
Director	124	40	84
Manager/Supervisor	242	127	115
Business/Admin/Technical Staff	226	122	104
Consultant	110	64	46
Other	53	34	19
Did not answer	**1**	**0**	**1**
TOTAL	**820**	**408**	**412**

Company- No. of Employees	GLOBAL	EMEA	US
1-500	284	153	131
501-1,000	70	22	48
1,001-5,000	90	78	12
5,001-10,000	120	30	90
10,001 +	256	125	131
TOTAL	**820**	**408**	**412**

Industry	GLOBAL	EMEA TOTAL	US TOTAL
Automotive & Transport	23	11	12
Energy/Utilities	20	9	11
Insurance	30	13	17
State/Local Government	27	14	13
Banking	85	55	30
Entertainment/Media	27	10	17
Manufacturing	39	19	20
Technology	172	79	93
Central Government	60	25	35
Financial Services	66	37	29
Pharmaceutical	8	3	5
Telecommunications	46	33	13
Education	69	39	30
Healthcare/Pharmaceutical	33	11	32
Retail & Wholesale	21	12	9
Other	82	38	44
Did not answer	2	0	2
TOTAL	**820**	**408**	**412**

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 1,000 customers, including more than 35 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

Ben Roberts
Johnson King (Europe)
Phone: +44(0) 20 7401 7968
Email: cyberarkteam@johnsonking.co.uk