GLOBAL ADVANCED THREAT LANDSCAPE SURVEY

2014

CYBERARK®

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CyberArk's 2014 Global Advanced Threat Landscape survey is the eighth 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 and targeted attacks.

The survey report is the result of interviews with 373 IT security and C-level executives (CEO, CIO, CSO) across North America, Europe, and Asia Pacific (APAC). The primary findings include:

Snowden and Retail Breaches Influencing Security Strategies

Last year could be considered one of the most historic years ever in terms of cyber-attacks, both in frequency and in business impact – including loss of sensitive IP, threat of customer loss, diminishing brand value, weakening of executive trust, and negative impact on shareholder value. As a result, C-level executives are now held accountable for cyber-security by shareholders, customers and board members. Faced with continued attacks, executives have been forced to adjust organizational security strategies to stop attacks and neutralize the negative business impact of a breach. According to the survey, the attacks that were the most impactful in terms of changing an organization's security strategy were:

- **37 percent of respondents stated that the NSA/Edward Snowden breach impacted their security strategy the most**
- **31 percent of respondents stated that the Target, Neiman Marcus and similar retail-oriented attacks impacted their security strategy the most**

While the NSA breach was an insider-based incident and the retail attacks were conducted by external attackers, the two incidents are linked by the exploitation of privileged accounts. Neither attack could have been successfully executed without the compromise and exploitation of these credentials.

Attackers are on the Inside – Protect Your Privileges

Organizations continue to face a sophisticated advanced threat landscape led by determined attackers seeking to infiltrate networks to steal sensitive information, intellectual property and similar data assets. Many organizations face attacks on a daily basis, typically perimeter-oriented tactical aggressions such as phishing. These attacks are designed to give attackers a foothold from which they can steal the privileged credentials of an employee to give them defacto insider-status. Once an attacker gains insider-status, breaches can be extremely difficult to identify and stop without the proper tools in place. The survey shows:

- **52 percent of respondents believe that a cyber-attacker is currently on their network, or has been in the past year**
  - ***This number is similar to last year's survey, where 51 percent believed an attacker was on the network within the past year***
- **44 percent of respondents believe that advanced attacks that reach the privileged account takeover stage are more difficult to detect, respond to and remediate than any other stage of an attack**

Third-Party Privileged Access Emerges as Critical Security Vulnerability

Analyst firms and security experts agree that privileged account takeover and exploitation is critical for attackers to successfully do harm. Organizations are becoming aware of the 'privileged pathway' attackers use and are starting to limit the exposure of these accounts. However, the bad guys are finding other means of gaining privileged access by going after vendors and partners of the targeted company. As more companies move to the cloud and streamline the supply chain by providing routine network access to third-parties, this vulnerability will grow. This year's survey found that:

- **60 percent of organizations allow third-party vendors remote access to their internal networks**
- **Of this group, 58 percent of organizations have no confidence that third-party vendors were securing and monitoring their privileged access to the network**

CyberArk's View

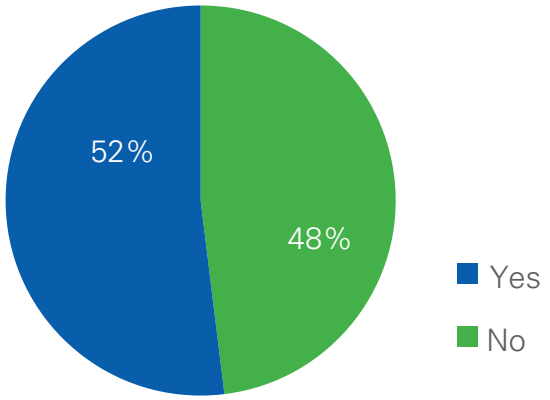
The past year of cyber-attacks provides clear evidence that attackers continue to target, steal and exploit privileged accounts to perpetrate their attacks – primarily because they can't execute attacks without this level of insider access. Whether attacks originate from the outside, or start with a malicious insider, gaining privileged access is critical to the success of an attacker. Eliminating the ability of attacker to gain privileged status is critical to mitigating attacks before real damage is done.

KEY REPORT FINDINGS

Attackers are Already Inside – Looking to Steal Privileges

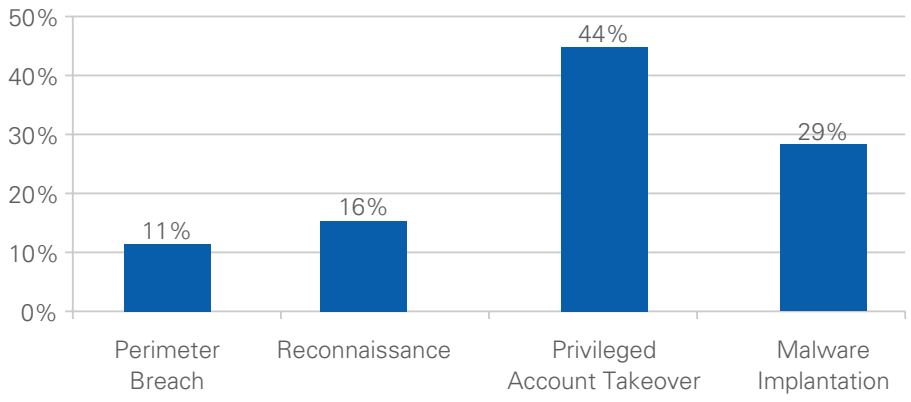
While many things are uncertain in the security world, the failure of the traditional 'perimeter' is nearly universally agreed upon. The mantra of 'where there is a will, there is a way' is clearly becoming the accepted norm, with 52 percent of organizations reporting that an attacker is currently on their network, or has been within the past year. CyberArk believes this number is low given the preponderance of attacks and the ability of hackers to hide infiltrations for months.

Fig. 1: Do you believe a cyber-attacker is currently on your network or has breached your network in the past year?



Once attackers are inside, they immediately target the privileged credentials of an approved employee. Privileged-based attacks are incredibly difficult to identify and stop because attackers can use these credentials to emulate normal business traffic. Results show 44 percent of organizations stated that attacks at the privileged account takeover stage were the most difficult to detect and remediate, compared to 29 percent who believe malware infection is the most difficult to manage.

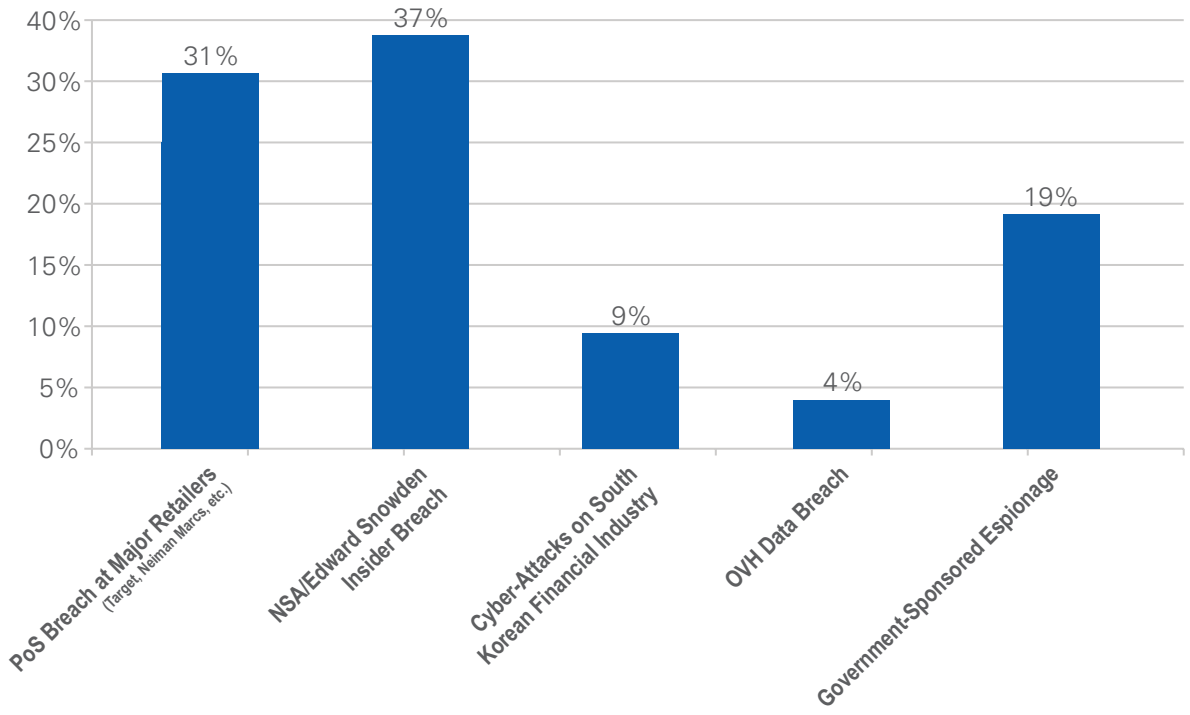
Fig. 2: At what stage of an attack does it become the most difficult to detect, respond and remediate?



Edward Snowden, Target Attacks Influence Security Strategies the Most

Despite the differences between the execution of the NSA breach and the Target attacks, 68 percent of organizations said these two attacks changed their security strategy more than any other attack in the past year (37 percent NSA; 31 percent Target). Both types of attacks have had a greater impact on security strategies than the well documented cyber-espionage activity sponsored by governments around the world. ***While the retail attacks originated from outside and the NSA was the ultimate insider attack, both attacks shared one critical commonality – neither attack could have occurred without the theft and exploitation of privileged accounts***.

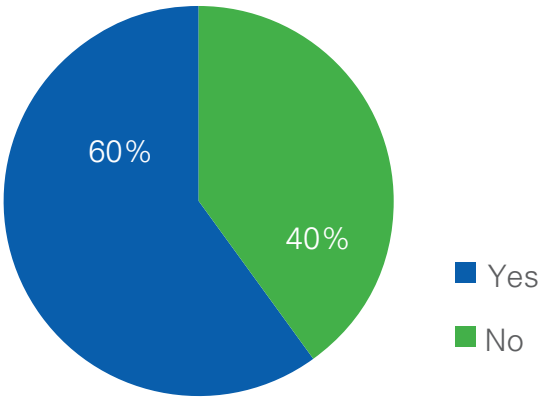
Fig. 3: What type of recent data breach or cyber-security incident impacted your security strategy the most in the past year?



Third-Party Privileged Access Emerges as Critical Security Vulnerability

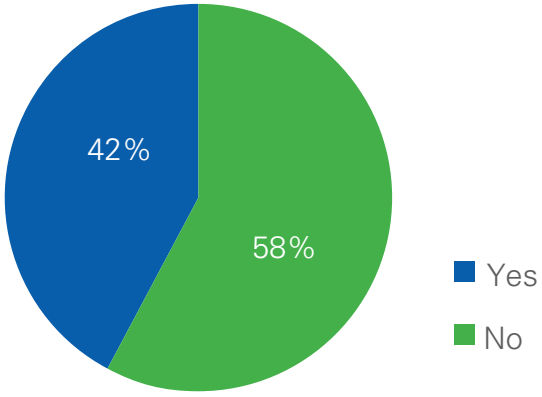
Determined attackers will find a way onto a network. Attackers are now bypassing their primary target by infiltrating partners with network access who may have weaker security controls than the targeted company itself. This type of third-party access is common in the industry: 60 percent of respondents allow third-party vendors remote access to internal networks.

Fig. 4: Do you allow third-party vendors (supply chain, IT management firms, etc.) remote access to any of your internal networks?



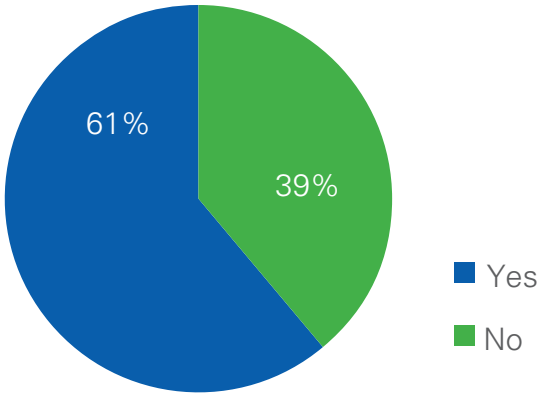
Despite providing this access, only 42 percent of organizations have confidence that third-party vendors are properly securing privileged access to their internal network.

Fig. 4a: If yes, do you have confidence that your third-party vendors secure and monitor privileged access to your network?



Because of the failure of third-parties to secure the access provided to partner networks, organizations are increasingly monitoring partner activity on their networks, with 61 percent of respondents monitoring and recording vendor activity on their network. Organizations need to incorporate privileged behavior as part of their monitoring – attackers use privileged accounts to emulate normal business activity. Detecting anomalous privileged behavior is critical to securing the enterprise.

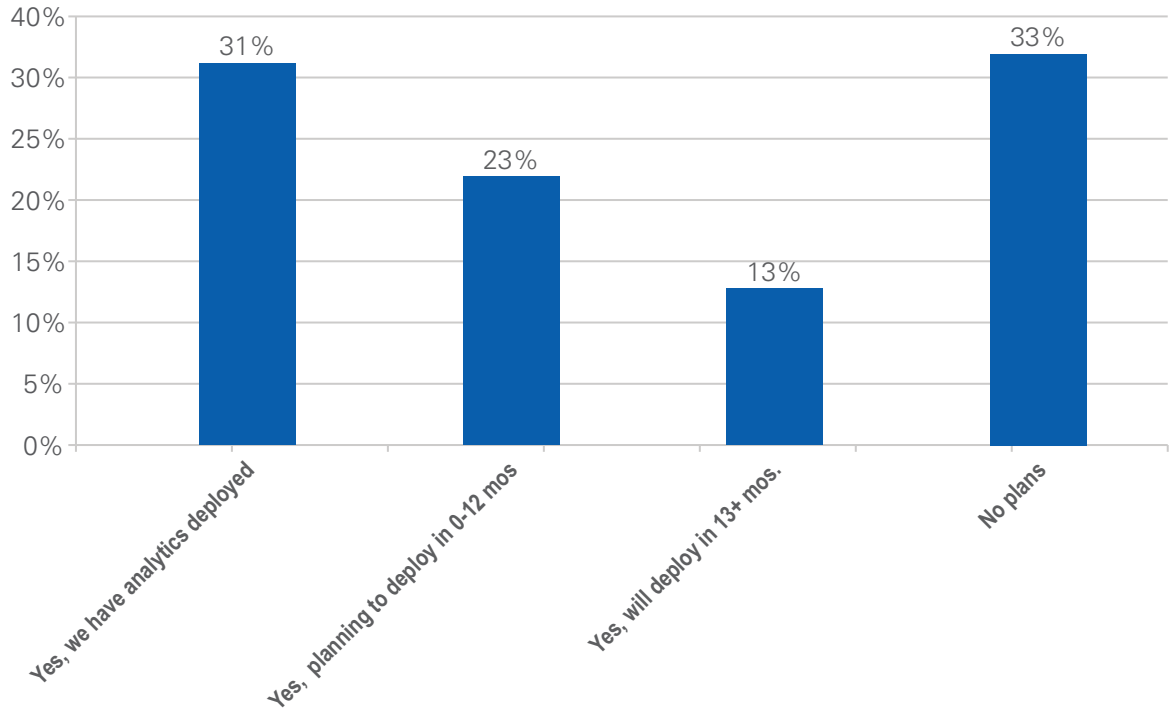
Fig. 4b: If yes, do you record and monitor your third-party vendor activity on your network?



Moving to Analytics-Based Security Practices

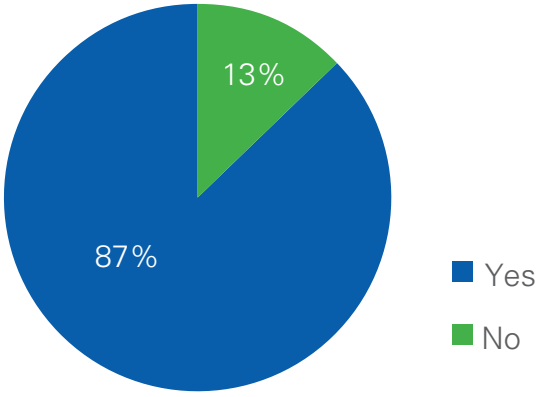
Security analytics have emerged as a critical tool to help organizations combat a menacing threat landscape. While 31 percent of organizations have already deployed security analytics, 23 percent more plan to do so in the next 12 months.

Fig. 5: Do you or are you planning to use security analytics as part of your security infrastructure?



To address the 'privileged pathway' that attackers use for attacks, organizations need to move to analytics that monitor user behavior. Detecting anomalous privileged activity is critical to mitigating today's advanced threats. Eighty-seven percent of organizations believe that detecting and alerting on unusual privileged activity would be valuable to its overall security strategy.

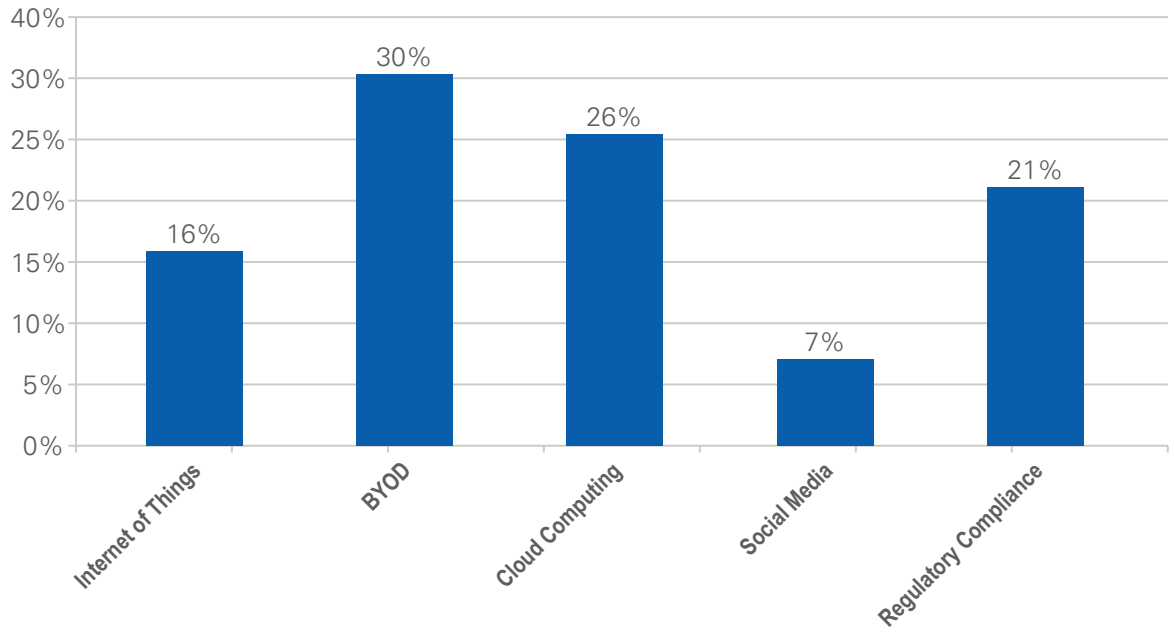
Fig. 6: Would the ability to detect & be alerted on unusual privileged activity be valuable to you?



Security Trends – BYOD and Cloud Keep C-Level up at Night

The confluence of trends – from connected devices, to cloud computing and BYOD – have made organizations more productive, and vulnerable, than ever. Each trend has eroded the corporate perimeter to the point where it no longer exists. As a result, organizations are more reliant on third-parties and employees to help maintain tight security controls over sensitive data, leaving them extremely vulnerable.

Fig. 7: What recent industry or technology trend impacts your security strategy the most?



APPENDIX

What are Privileged Accounts?

Privileged accounts are valid credentials used to gain access to systems, providing elevated, non-restrictive access to the underlying platforms. These accounts are designed to be used by system administrators to manage network systems, run services, or allow applications to communicate with one another. The most common privileged accounts are local admin, privileged user, domain admin, emergency, service and application. Privileged accounts can be found in any device with a microprocessor, including PCs, databases, networked devices like copiers, operating systems and more, and too often are 'secured' by default or hardcoded passwords easily found through basic Internet searches.

Securing Privileged Accounts

The lack of accountability and protection of privileged accounts in corporate networks is the vulnerability most often exploited by advanced and insider threats, and the benefits of securing privileged accounts cannot be underestimated. Regardless of resources available, there are practical solutions for every organization with every budget. Best practices solutions range from manual processes to incrementally improve security to automated enterprise solutions that provide analytics and best in class security.

For more information on CyberArk's best practice recommendations for preventing privileged account compromise, please visit cyberark.com/contact/white-paper-securing-privileged-accounts-best-practices-guide#.U8lcdLE3ctE.

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 more than 35 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, MA. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com, read the company blog, www.cyberark.com/blog/, follow on Twitter @CyberArk or Facebook at www.facebook.com/CyberArk.

MEDIA INQUIRIES:

Eric Seymour

CyberArk
Phone: +1 617-796-3240
Email: eric.seymour@cyberark.com

Brian Merrill

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