Global Advanced Threat **Landscape Survey**

2015

Table of Contents

EXECUTIVE SUMMARY

CyberArk's 2015 Global Advanced Threat Landscape Survey is the ninth in a series of annual surveys that focus on identifying global cyber security trends.

The survey report is the result of interviews with 673 IT security and C-level executives (CEO, CIO, CSO) across North America, Europe and Asia Pacific (APAC). The primary findings include:

More Than a Data Breach – Complete Network Takeover

Anthem, Carphone Warehouse, the German parliament, K Box Singapore, Sony Pictures, TV5Monde and the attack on the U.S. Office of Personnel Management (OPM) continue to demonstrate that cyber attacks are not just about stealing data, but also about compromising the very ability of an organization to do business. These breaches are the most representative examples of why attackers covet privileged and administrative accounts, and how exploiting access to these accounts can lead to a complete hostile takeover of network infrastructure. This new reality is driving greater awareness of the threat of privileged account vulnerabilities within the enterprise:

- 61 percent cited privileged account takeover as the most difficult stage of an attack to mitigate
  - This number has significantly increased from last year's survey, where 44 percent cited privileged account takeover as the most difficult stage of an attack to mitigate
- More than one-third (38 percent) cited stolen administrative and privileged credentials as their greatest security concern
- Despite these growing concerns, only half of respondents have at least some form of an automated privileged account management system in place

CyberArk View: Privileged accounts are at the epicenter of almost every cyber attack. Once attackers gain these powerful credentials, the organization and its network are at the mercy of the attacker. Of concern is that many organizations, including government agencies, still struggle with identifying and locating privileged accounts.

Corporate Confidence and a False Sense of Data Security

As the number of devastating cyber attacks grows, C-level executives are increasingly held accountable for the cyber security strategies their organizations are deploying. Analysis of the survey results demonstrates that a majority of respondents believe their CEO/directors provide sound leadership and that they can also reasonably detect a breach and keep attackers off a network.

- 44 percent believe that they can prevent attackers from breaking into a network
- 55 percent of respondents believe they can detect a breach within a matter of days; 25 percent believe they can detect a breach within hours
- 57 percent believe the CEO/Board of Directors provide sound leadership for organizational security strategy

CyberArk View: Despite mounting evidence to the contrary, respondents continue to believe that they can keep motivated attackers off the network, or easily discover them once they've infiltrated an organization. This confidence is misplaced. Organizations need to assume they will be breached and monitor the pathway attackers take. Analytics on privileged activity can help identify malicious behavior early in the attack cycle and enable organizations to take action.

Hiding Behind Attacker Sophistication is Not a Security Strategy

Poor employee security habits can no longer be the IT team's scapegoat. It's time to subscribe to the theory that the attacker has already made it inside the perimeter and recognize that phishing and other unsophisticated means of attack will happen, and they will be successful. It's almost as if it's a cost of doing business. However, it's what can be done to stop attackers once inside the network that business and IT leaders should be thinking about.

- 48 percent believe poor employee security habits are to blame for data breaches, while 29 percent believe attacker sophistication is to blame for breaches
- Password hijacking (72 percent) and phishing (70 percent) are the tactics of greatest concern
- Methods like SSH key hijacking (44 percent) and others that enable attackers to escalate privileges and move closer to sensitive information were ranked lower, such as Pass-the-Hash (36 percent) and Golden Ticket (23 percent)

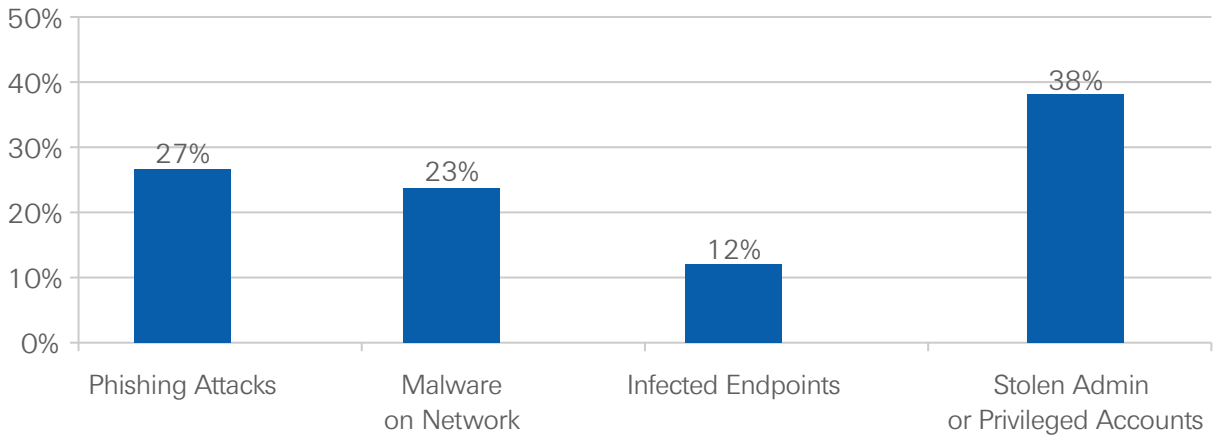
CyberArk View: Organizations often point to attacker sophistication or blame poor employee security habits as the reason for a breach. Organizations should accept that the security battle has shifted to inside the enterprise network. Attackers will always find a way past the perimeter. Security strategies must assume this and focus on limiting attacker movement once they infect an endpoint or trick an employee into clicking a malicious link. In particular, business leaders need to understand the damage that can be done with hijacked privileged credentials, including passwords and SSH keys, once an attacker is inside a network and able to use those credentials to gain access to valuable data. Additionally, there needs to be greater awareness associated with Pass-the-Hash and Kerberos attacks, such as Overpass-the-Hash, Silver Ticket and Golden Ticket, which if executed by an attacker, could mean 'game over' for the enterprise.

KEY REPORT FINDINGS

Growing Security Concern – Complete Network Takeover

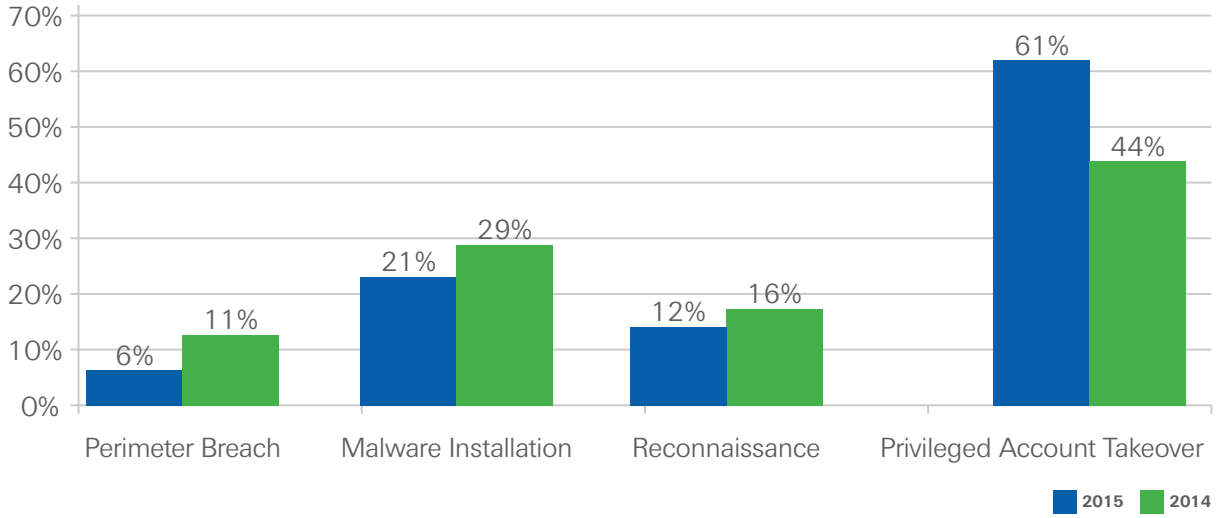
Devastating attacks on organizations like Anthem and OPM show that today's cyber attacks ***use privileged accounts to exfiltrate data***, and in cases like Sony Pictures, ***completely take over network infrastructure.*** These disastrous scenarios may be why respondents cited stolen administrative and privileged credentials as their #1 security concern. (figure 1)

Fig. 1: Which of these represent your greatest security concern?



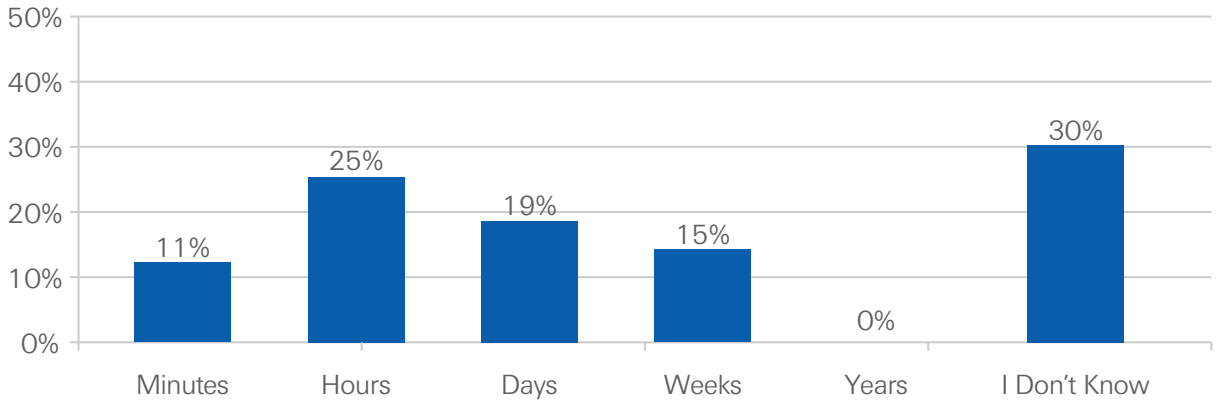
Once attackers steal and exploit privileged credentials, it becomes incredibly difficult to stop the attack cycle. Sixty-one percent of respondents cited privileged account takeover as the most difficult stage to mitigate, up from 44 percent last year. Twenty-one percent believe that malware on the network is the most difficult stage to mitigate. (figure 2)

Fig. 2: At what stage of an attack does it become the most difficult to mitigate?



Once a cyber attacker steals and exploits privileged credentials, not only is it difficult to dislodge them, it's incredibly difficult to even detect them. Attackers that exploit privileged accounts can delete logs and history, install malware and backdoors, and easily evade detection by hiding in plain sight as normal business traffic. Industry reports highlight that attackers are on a targeted network an average of 200 days prior to detection[1]. This is why it is counterintuitive that 55 percent of respondents believe they can detect a breach within a matter of days (with 25 percent stating they can detect a breach within hours). (figure 3)

Fig. 3: How long would it take you to discover that you've been breached?

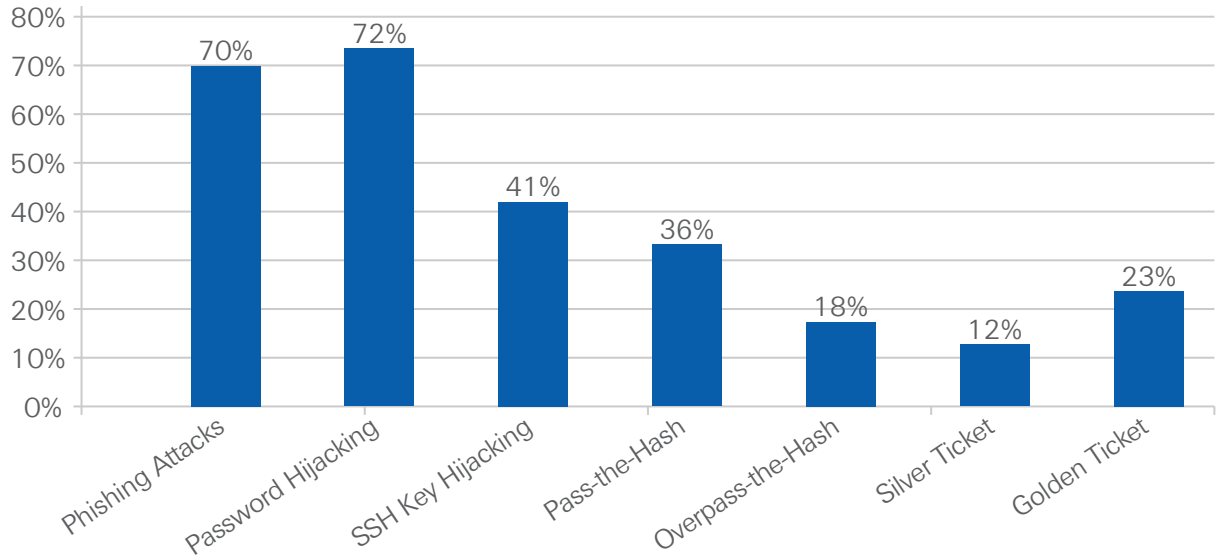


Security Strategies vs. Attacker Sophistication

Privileged accounts are at the epicenter of every successful cyber attack. This is why attackers are evolving their tactics for stealing these powerful credentials. While traditional attacks such as password hijacking (72 percent) and phishing (70 percent) were cited as most concerning, organizations are missing the bigger picture. Potentially more devastating are those attack techniques that happen once an attacker is inside the network - like SSH key hijacking, Pass-the-Hash and Golden Ticket.

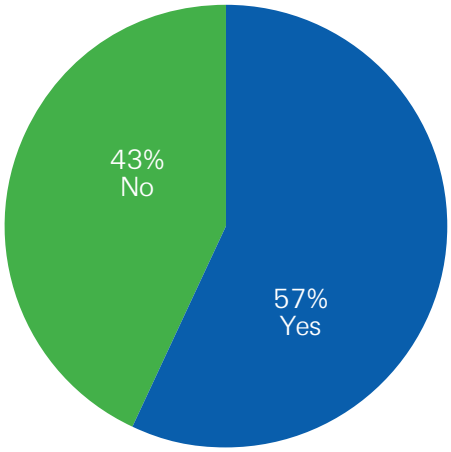
Cited by 41 percent of respondents as a top concern, SSH keys not only grant an attacker root access, but they can also enable lateral movement throughout the Unix/Linux environment. Others, like Golden Ticket (23 percent) and Overpass-the-Hash (18 percent) are flavors of Kerberos vulnerability attacks that can give full control over a target's network to the external attackers. An organization's Active Directory and domain controller need to be treated the same way as their most sensitive, confidential data. This supports the need for greater awareness of vulnerabilities within environments using Kerberos authentication and the types of attacks that leverage those weaknesses. (figure 4)

Fig. 4: **Which of the following types of attacks are you concerned about? (select all that apply)**



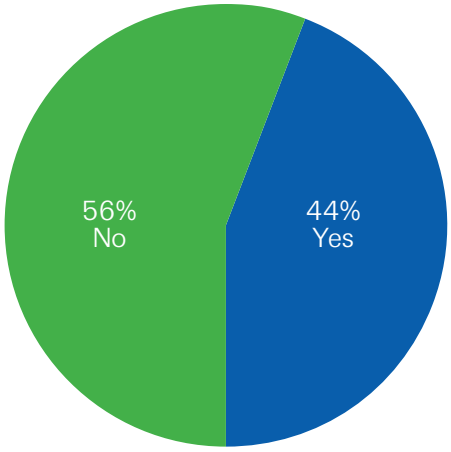
Security is no longer a challenge for security teams alone. Responding to today's attacks is about more than just protecting data, it's about protecting the ability to continue conducting business as usual. As the lessons of Sony Pictures, Sands and similar attacks sink in, corporate directors and officers need to become more involved with security strategies. Executives need to define their tolerance for risk and calibrate cyber security strategies accordingly. Fifty-seven percent of respondents believe that their CEO/Board of Directors provide sound leadership for organizational security strategies. (figure 5)

Fig. 5: **Are you confident that your company's CEO and/or Board of Directors provides sound leadership for your organization's cyber security strategy?**



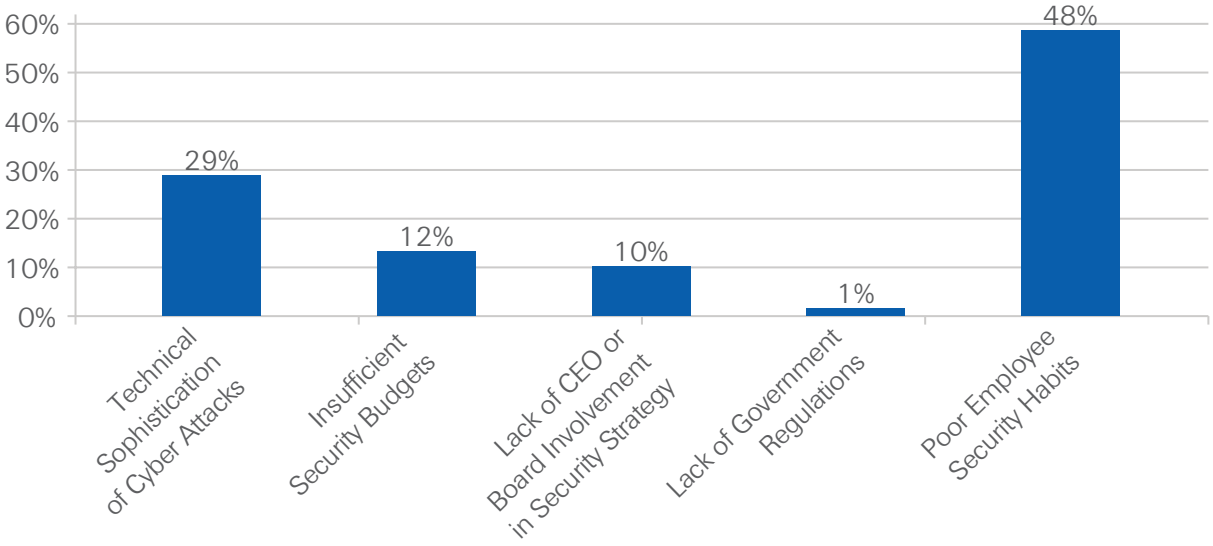
CyberArk believes this confidence in executive leadership around security strategy is contradicted by how today's attacks are conducted and the security approaches being deployed. For instance, despite clear evidence that motivated cyber attackers will always find a way to breach perimeter security and gain access to a targeted network, ***organizations still maintain the belief that they can keep attackers off of their networks with the right security strategy.*** Forty-four percent of respondents still believe that they can prevent attackers from breaking into their network. (figure 6)

Fig. 6: Do you believe you can prevent attackers from breaking into your network?



In addition, 48 percent of respondents state that poor employee security habits are the leading factor in most data breaches, with 29 percent citing the technical sophistication of attackers. CyberArk believes that ***C-level executives and Boards of Directors can no longer simply state that 'attacks are too sophisticated' or 'employees are to blame for security lapses.' This needs to be accounted for in a holistic security strategy that assumes motivated attackers will always find a way to breach a network.*** (figure 7)

Fig. 7: What do you believe to be the leading factor in most data breaches?

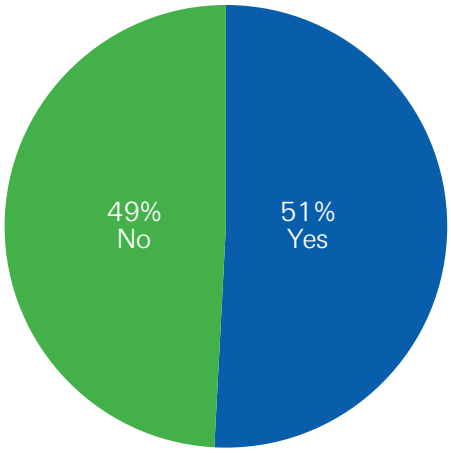


Security Program Leadership

The disconnect between the sound leadership of the C-level and actual security approaches is further seen in the failure of a majority of organizations to automate the security of privileged accounts (49 percent). (figure 8)

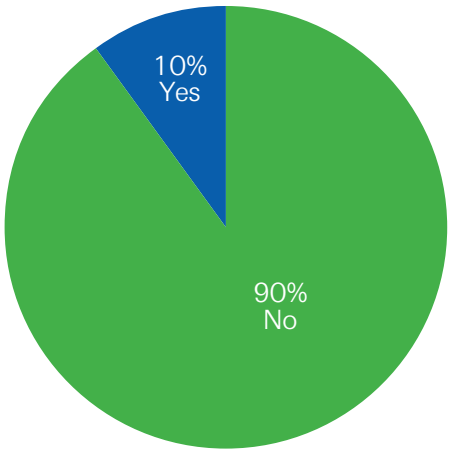
Organizations often underestimate how many privileged accounts exist across their systems (organizations today have at least 3-4 times as many privileged accounts as employees), and often don't know where to find them. ***A single exploited privileged account can lead to complete network takeover.*** The sheer scale of the privileged account attack surface requires automation to enforce strong security policies – from automatically discovering all accounts across a network to enforcing strong policies like one-time password use and two-factor authentication.

Fig. 8: Do you have an automated privileged account management system in place across your organization?



A common security mistake organizations make is to confuse good compliance for good security. ***Following security-related rules doesn't make a business more secure, but represents the minimum obligatory requirements for security.*** A resounding 90 percent of respondents believe that compliance with industry regulations is not enough to prevent a breach. (figure 9)

Fig. 9: Do you believe that compliance with industry regulations is enough to prevent a data breach?



TERMINOLOGY

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.

The lack of accountability and protection of privileged accounts in corporate networks is the vulnerability most often exploited by cyber attackers. The benefits of protective controls and detection capabilities on privileged accounts and credentials should not be overlooked as part of a comprehensive security strategy.

ABOUT CYBERARK

CyberArk (NASDAQ: CYBR) 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 40 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, Mass. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com

[1] Mandiant M-Trends Report 2015