CYBERARK GLOBAL ADVANCED THREAT LANDSCAPE 2019 REPORT

EXECUTIVE SUMMARY

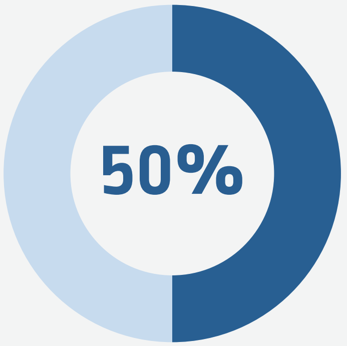
EXECUTIVE SUMMARY

About the CyberArk Global Advanced Threat Landscape 2019 Report

Welcome to the 12th annual edition of the CyberArk Global Advanced Threat Landscape Report. This year's report examines business leaders' engagement with cybersecurity as global organizations transition to true digital businesses, and continues our longstanding focus on the practice of privileged access security.

In total, 1,000 IT security decision makers were surveyed in early 2019, with respondents based in the US, UK, France, Germany, Singapore, Australia and Israel. The majority of respondents (88 percent) surveyed were manager level or above. Of those, 21 percent were C-level executives, while 35 percent represented companies of 3,000 employees or more.

Respondents were from organizations with at least 250 employees in any private and public sector (excluding consumer services). All respondents were interviewed online using a rigorous, multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.



agree that attackers can’t be prevented from penetrating the network each time they try.

Strategic Security Investments to Break the Cyber Kill Chain

Cyber threats – from cyber criminals, competitors, nation states, insiders and other actors – are a given, and the cost to business is increasing. The survey shows that over half (53 percent) have suffered business impact from an attack in the previous three years and that 50 percent agree that attackers can’t be prevented from penetrating the network each time they try. Meanwhile, the impact and demands of digital transformation are creating the need for more risk-aware security investments.

Experienced organizations know that compromised privileged access provides attackers a shortcut to their goals. The survey reveals a shift in security spend, extending beyond perimeter protection to also contain attacker movement inside the network at critical points along the cyber kill chain. More than a quarter of planned security budgets will address preventing privileged escalation and subsequent lateral movement (28 percent on average when combined) in 24 months’ time – a good indication of increasing security robustness. Additional data revealed:

- 78 percent said hackers represented one of their top three greatest threats to critical assets
- Respondents said external attacks such as phishing were among their greatest security risks (60 percent)
- 20 percent report that their organization runs regular Red Team exercises (the average frequency being every three months)

CyberArk View

As businesses embrace digital transformation, the increasing reliance on automation and investments in cloud and DevOps processes mean added pressure on security teams. Often, the need to respond to rapidly changing markets leads to security being overlooked or deprioritized, even as an expanded or altered attack surface increases the risk of security incidents.

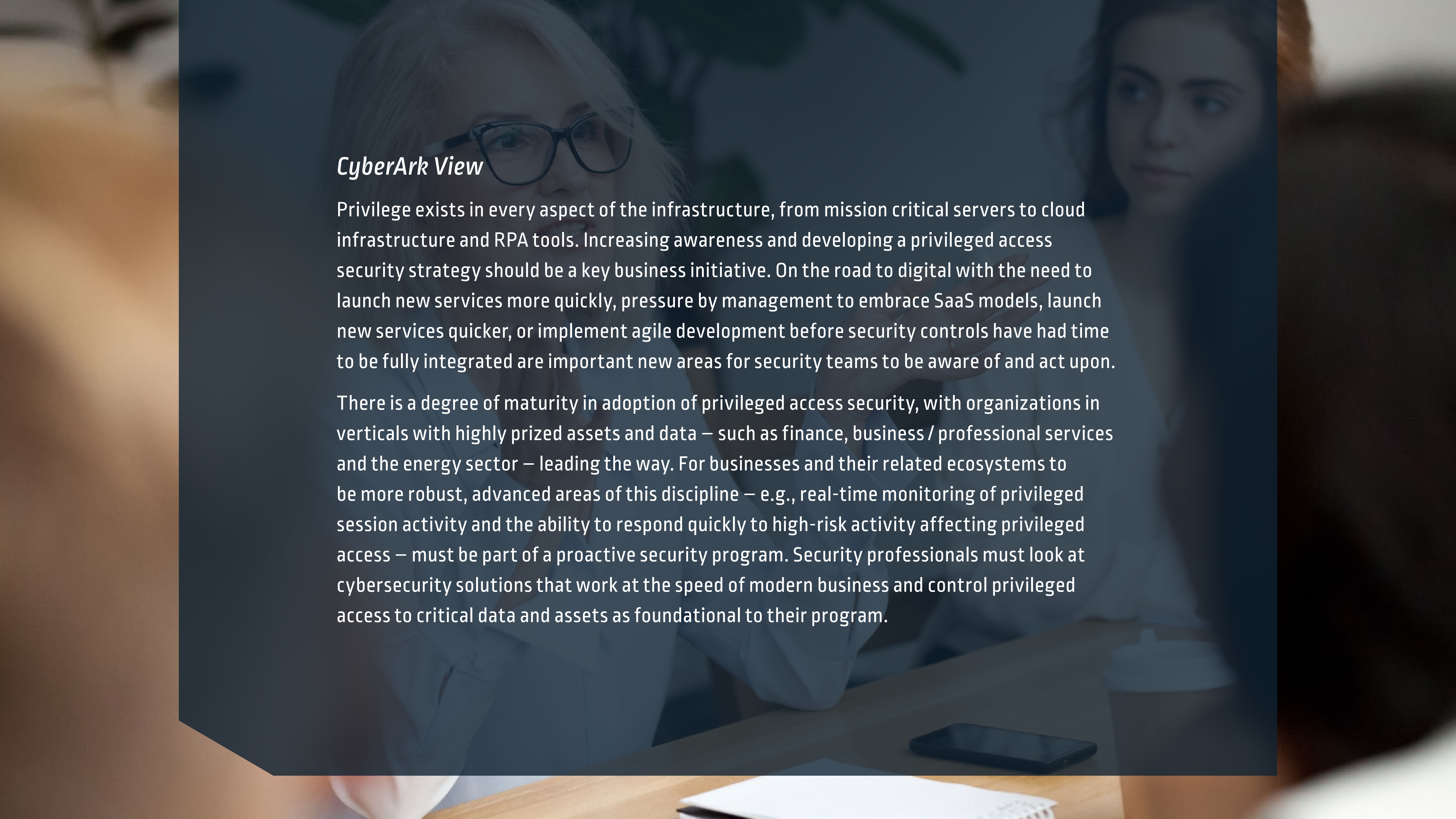
With attacks continuing unabated, it is critical to direct cyber investments toward security controls and skilled personnel that can combat attackers' ability to move laterally in the IT environment, compromise privileged credentials that allow them to gain control of targeted assets, and discover additional resources and assets to exfiltrate or compromise.

There was not one area we asked about where more than half of respondents reported that a privileged access security strategy was in place

Security Barriers to Digital Transformation and the Privilege Priority

We found that many organizations are stepping up to the challenge of controlling access to critical assets, with evidence that privileged access security strategies exist across certain aspects of the infrastructure, from mission critical servers to Internet of Things (IoT). While there is some visibility into where privilege exists across the IT environment – including user machines, robotic process automation (RPA), IoT, Infrastructure-as-a-Service (Iaas) and Platform-as-Service (PaaS) environments and more – there is an opportunity to drive greater awareness about the expanding privileged attack surface – especially across foundational digital transformation technologies.

- 84 percent agree that IT infrastructure and critical data are not fully protected unless privileged accounts, credentials and secrets are secured
- Yet, **only 35 percent have a privileged access security strategy for DevOps** or CI/CD pipelines and only 32 percent for the Internet of Things (IoT)
- In fact, **there was not one area we asked about where more than half of respondents reported that a privileged access security strategy was in place**



CyberArk View

Privilege exists in every aspect of the infrastructure, from mission critical servers to cloud infrastructure and RPA tools. Increasing awareness and developing a privileged access security strategy should be a key business initiative. On the road to digital with the need to launch new services more quickly, pressure by management to embrace SaaS models, launch new services quicker, or implement agile development before security controls have had time to be fully integrated are important new areas for security teams to be aware of and act upon.

There is a degree of maturity in adoption of privileged access security, with organizations in verticals with highly prized assets and data – such as finance, business / professional services and the energy sector – leading the way. For businesses and their related ecosystems to be more robust, advanced areas of this discipline – e.g., real-time monitoring of privileged session activity and the ability to respond quickly to high-risk activity affecting privileged access – must be part of a proactive security program. Security professionals must look at cybersecurity solutions that work at the speed of modern business and control privileged access to critical data and assets as foundational to their program.

Compliance Resistance and Reactive Mindsets Persist

Despite the shift toward more risk-aware security investment and practices, persisting levels of cybersecurity inertia and reactive mindsets continue to put sensitive data, infrastructure and assets at risk. A troubling 41 percent of respondents said their organization would prefer to pay a fine for losing data after a successful cyber attack rather than change their security policy.

Our study examines organizations' preparedness to meet increasing compliance demands and avoid record-breaking financial penalties.

- **EU General Data Protection Regulation (GDPR):** Less than half (46 percent) are completely prepared for breach investigation and notification in the mandated 72-hour time period
- **California Consumer Privacy Act (CCPA):** Only 37 percent are ready for this regulation to take effect in 2020 – though 39 percent are actively working to be able to meet it
- **Australia's data breach notification law:** 62 percent of Australian respondents reported that their organization was completely prepared, more than a year after it came into law

Visit **www.cyberark.com/TL19** to read the full report

CyberArk View

While only investing in security to meet compliance regulation is not necessarily good news for overall cybersecurity posture, enforcement of regulations like GDPR and CCPA, plus the prospective amendments to Singapore's Personal Data Protection Act in 2019, are meaningful and comprehensive requirements that require significant investment for organizations.

Often, the time-specified need to notify to a supervisory authority following a data breach will mean businesses will not only need to detect and respond to breaches quickly, but also be able to account for what records, how many, likely impact and steps taken to mitigate the breach. To rapidly and accurately report on a breach – or better yet, detect a threat before a breach occurs – robust operational and security controls are necessary.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk, LinkedIn or Facebook.

CYBERARK®

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

07.19. Doc. 373314832