THE **CISO VIEW**

An Industry Initiative
Sponsored By **CyberArk®**

Protecting Privileged Access in a Zero Trust Model

Executive Summary

INTRODUCTION

The trend to a Zero Trust model of information security is gaining momentum. Digital transformation and enterprise mobility are rapidly eroding the traditional perimeter-based model. What does this mean for protecting privileged access?

To explore these issues, we interviewed the CISO View research panel: a group of 12 leading security executives from Global 1000 organizations who have been steering their organizations towards a Zero Trust model.

Based on the panel's first-hand experiences around protecting privileged access while adopting Zero Trust approaches, this report is one of the first to offer practical and operational insights for CISOs and their teams.

Establish and maintain trust

Zero Trust does not assume implicit trust inside a corporate network. Instead, it focuses on establishing and maintaining trust for every session with a corporate resource and tightly limits access for verified users and devices.

Access full report at: www.cyberark.com/cisoview/

Contributors: **The CISO View Research Panel**
Top Information Security Executives from Global 1000 Enterprises

Alissa (Dr Jay) Abdullah
SVP and Deputy Chief Security Officer
Mastercard

Brad Arkin
SVP, Chief Security & Trust Officer
Cisco

Tim Bengson
VP, Global Chief Information Security Officer
Kellogg Company

Dawn Cappelli
VP, Global Security and Chief Information Security Officer
Rockwell Automation

Melissa Carvalho
VP, Enterprise and Customer Identity and Access Management
Royal Bank of Canada (RBC)

Dave Estlick
Chief Information Security Officer
Chipotle

Peter Fizelle
Chief Information Security Officer
Asian Development Bank

Mike Gordon
VP and Chief Information Security Officer
Lockheed Martin

Omar Khawaja
VP and Chief Information Security Officer
Highmark Health

Olivier Perrault
Cyber Security Officer
Orange Business Services

Emma Smith
Global Cyber Security Director
Vodafone

Daniel Tse
Head, Cyber Security, Information & Technology Risk
GIC Private Limited

KEY FINDINGS ON RISKS

The CISO View panelists described how risks to privileged access are changing as the perimeter dissolves and security programs transition to Zero Trust.

Key Finding 1: Escalating spear phishing and impersonation attacks target high-level or high-value access

- Attackers increasingly aim to steal credentials that will give them direct routes to specific data.
- Spear phishing attacks are on the rise whereby an attacker investigates who has access to a particular system (such as an accountant with access to payment systems) then conducts a highly targeted social engineering campaign against this individual to steal their credentials.
- Another technique is to steal email credentials or set up a fake social media profile in order to impersonate an executive or third party, then ask an employee to transfer funds or data.
- To gain trust, attackers do things such as create fake online personas and engage in extensive personal interactions.
- Types of access being pursued by attackers include:
  - High-level (administrative) access
  - High-value access: End user (business user) access to valuable systems and data
  - Access subject to impersonation

Key Finding 2: Inventory and least privilege challenges can leave gaps in protecting privileged access

- Most organizations struggle with asset management. Service accounts are often overlooked. More workers are using unmanaged devices.
- Cloud access and remote access can be hard to configure for least privilege.
- Third-party users are typically not managed in a central location, which leads to issues such as poorly-controlled sharing of accounts and delays in decommissioning access.

Key Finding 3: Zero Trust implementations have potential weak spots

- If an attacker steals credentials and then attempts to access a resource that is protected by MFA, the legitimate user will be prompted to provide the second factor. Users who frequently receive reauthentication requests will often provide the second factor without thinking.
- Attackers can trick the legitimate user into responding to the MFA prompt by using fake login screens or by sending repeated bothersome requests.
- Attackers can also gain access by compromising a device and hijacking a session.
- When resources can be accessed through multiple channels, organizations commonly miss securing secondary channels with MFA.
- New security technologies have new and powerful types of privileged accounts associated with them that can be pursued by attackers.

> "The adversary is looking at, 'What access can I get?' In a Zero Trust model, it is an identity and access management issue."
>
> **Alissa (Dr Jay) Abdullah**
> SVP and Deputy Chief Security Officer
> Mastercard

RECOMMENDATIONS

Recommendation 1: Identify “new” targets subject to increasing attacks

- Identify the systems and data that are most likely to be targeted by an attacker, then identify which people and machines can access them.
- A way to find higher-risk service accounts is to use analytics to sift through logs for highly sensitive databases and applications, to assess where logins are coming from.
- Identify new types of privileged accounts that will need to be protected, such as admin and developer accounts for MFA, SSO, and PKI; and service accounts for analytics and AI.
- Identify all application administrator accounts, including for SaaS applications.
- Prioritize users with high-value access for MFA, adaptive authentication, endpoint security, and other controls. Consider additional security education and spear phishing tests for these users.

Recommendation 2: Ensure MFA implementation is effective

- Reduce password usage by using standards-based SSO and methods such as device certificates, biometrics, and push notifications.
- Lockdown MFA registration for example, by using an out-of-band process to verify request made by the legitimate user.
- Have the Security team own the user experience for authentication. Design processes to present reauthentication requests sparingly and as expected by the user. Use analytics to provide context for risk decisions, minimizing friction.
- Combine MFA with privileged access management to protect secondary channels.

Recommendation 3: Protect higher-risk credentials in a PAM system

- PAM systems typically protect administrative access to infrastructure and databases. For high-value applications, the panelists recommend using PAM for administrator accounts, break-glass accounts, and end-user accounts that are shared by multiple users.
- Also consider using a PAM system to implement dual control and/or session monitoring for sensitive functions, for higher-risk service accounts, and for SSO accounts of individuals with extremely sensitive access, such as executives.

Recommendation 4: Allow just enough access

- Review and minimize access frequently.
- Limit user connections to a single resource or narrow subset. Options include proxy technologies and VDI. Use tiered jump servers (bastion hosts) to connect admins to infrastructure. Isolate unmanaged devices connecting to corporate resources to reduce the risk of malware spreading.
- Minimize local admin access. Consider using endpoint protection technology to restrict installations to whitelisted or greylisted applications.

> "Some high-value accounts tend to be overlooked. A typical example is accounts that enable bulk download of sensitive personnel details including compensation records. Those credentials should be managed in a PAM system so that no single person will have direct access."
>
> **Daniel Tse**
> Head, Cyber Security,
> Information & Technology Risk
> GIC Private Limited

- Provide just-in-time (JIT) access through adaptive authentication technology or a PAM system.
- Make JIT easier to use and audit via automated approvals, granting more time than estimated, combining with session recording, and using a ticketing system for access requests.

Recommendation 5: Drive a cultural change

- Emphasize "trust" versus zero trust: Some organizations choose alternative terminology.
- Convey well in advance that having less privilege is in each employee's own interest and that privilege reduction is happening across the organization.
- Raise awareness of the potential for attackers to impersonate executives, partners, or customers using email spoofing, collaboration platforms, and fake social media accounts.
- Use targeted marketing techniques to develop more influential content about security risks. Use gamification to drive competition between users to avoid risky behavior. Incentivize users to look for ways to minimize their own privileges.

> "Organizations should absolutely do Zero Trust but do it with eyes wide open. There are going to be some impediments along the way. Don't be surprised. Know how to address them."
>
> **Omar Khawaja**
> VP and CISO
> Highmark Health

To access the full report please visit
www.cyberark.com/cisoview/

ABOUT THE CISO VIEW INDUSTRY INITIATIVE

CyberArk has commissioned an independent research firm, Robinson Insight, to facilitate an industry initiative to explore CISO views on topics related to improving privileged access controls. The initiative brings together top CISOs who share their insights into critical issues facing practitioners today.

CyberArk (NASDAQ: CYBR) (**www.cyberark.com**) is a global company providing identity security solutions.
Robinson Insight (**www.robinsoninsight.com**) is an industry analyst firm focused on CISO initiatives.