THE **CISO VIEW**

An Industry Initiative
Sponsored By **CyberArk®**

Protecting Privileged Access in a Zero Trust Model

5th Annual CISO View **Research Study**

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

→
LEARN MORE about the contributors

CONTENTS

CYBERARK

A WORD FROM OUR SPONSOR

The CISO View report series is developed by an independent research firm, Robinson Insight, and sponsored by CyberArk. The hard-won experience of other security professionals is invaluable for CISOs trying to make informed, empirically based decisions as they work to improve privileged access controls. We are grateful that by sharing their insights, the members of the panel are helping the larger community address this issue.

ADAPTING PRIVILEGED ACCESS CONTROLS AS THE PERIMETER DISSOLVES

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? As the perimeter dissolves, how can organizations protect access to their most valuable resources – data, applications, and infrastructure – on-prem or in the cloud?

To explore these issues, we interviewed the CISO View research panel: a group of 12 leading security executives from Global 1000 organizations. They have been steering their organizations towards a Zero Trust model and have worked through some of the challenges that other practitioners are likely to encounter.

We asked the CISO View research panel:

- How are the risks around privileged access changing as users and resources are increasingly outside the corporate network?
- What techniques are attackers using to try to gain privileged access?
- How should organizations adapt controls to manage the risks and move toward a Zero Trust model?

This report captures the panel's perspectives, informed by actual implementations of controls and, in some cases, their findings from red team exercises. It includes recommendations on how to:

- Prioritize, design, and implement controls.
- Work with stakeholders to maximize acceptance and engagement.
- Enable both employees and third parties to securely access corporate resources.

WHY ZERO TRUST

- The traditional model of security based on a trusted network inside a defined corporate perimeter has become less effective.
- Attackers have many ways to reach corporate resources from outside the network.
- Data, applications, and infrastructure are moving to the public cloud.
- Large populations of users are also not inside the network, given the massive growth of:
  - » Third-party access to corporate resources
  - » Remote work
- A Zero Trust model does not assume implicit trust inside a corporate network, and instead focuses on establishing and maintaining trust for every session with a corporate resource.

Most organizations are early in their journey to Zero Trust and not much peer-to-peer guidance exists yet. Based on the CISO View 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.

Mechanisms to establish and maintain trust

Zero Trust is not a single technology but an approach to information security involving different types of technologies including identity and access management, behavioral analytics, endpoint security, and network micro-segmentation.

The approach is centered on assessing every request to access a corporate resource – data, applications, and infrastructure – before granting access, then tightly limiting access for verified users and devices. It provides mechanisms to establish and maintain trust for every session with a corporate resource:

- **Authentication of user and device** using multi-factor authentication (MFA) and certificates, considering context such as time-of-day, geographic and network location, and device health.
- **Authorization** by enforcing least-privilege policies.
- **Continuous evaluation throughout the session** by analyzing behavior patterns, applying risk scoring, adapting controls (including possibly revoking access), and monitoring usage.

During each session, encryption ensures a safe connection between the endpoint and the corporate resource and can also be used to protect data at rest. Endpoint hygiene is imperative as devices are more exposed to malware in perimeter-less environments.

> "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

ZERO TRUST IS A JOURNEY

Although most organizations are at the early stages of adopting Zero Trust approaches, many already have elements such as MFA in their environments. Organizations tend to gradually add new Zero Trust controls to complement their existing perimeter-based controls instead of replacing existing controls all at once. Each incremental step in the journey will help to better manage information security risks.

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

When we asked panelists about how attackers are trying to gain privileged access in today's environments, they talked about the shift in attack patterns towards precisely targeting individuals. Rather than breach an arbitrary workstation then move around the network searching for a particular system, the trend is for attackers to pursue more direct routes.

Through spear phishing, attackers can gain direct access to the most valuable systems and data

Recently there has been a surge in spear phishing campaigns targeting individuals who have direct access to a particular system the attacker is interested in. First, the attacker determines who within the organization – or at an associated third party – has access to a particular system.

Then the attacker conducts a highly targeted social engineering campaign against this individual to steal their credentials. The target might be an IT admin, but more typically is an end user with high-value access such as:

- Engineer with access to intellectual property
- Scientist with access to R&D data
- Insurance claims manager with access to patient data

> "Adversaries might spend months interacting with a user in non-malicious ways. They focus on the personal side, trying to build a relationship with the user who has the specific files they want. It'll just be chitter-chatter, friendly dialog, until they send that email with the malicious code."
>
> **Mike Gordon**
> VP and CISO
> Lockheed Martin

- Accountant with access to payment systems
- Third-party data analyst with access to customer records

Through impersonation attacks, attackers make direct requests for funds or data

Another technique frequently used in recent attacks is to impersonate an executive or third party and ask an employee to transfer funds or send data to them. In the first stage, the attacker gains the ability to impersonate someone who has authority or a trusted relationship. To do this, an attacker might:

- Steal email credentials or spoof an email (busines or personal email)
- Compromise a collaboration platform
- Compromise a personal social media account
- Set up a fake social media profile

In the second stage, the attacker, posing as the executive or third party, sends a message to an employee with high-value access. For example, say scientists are collaborating with analysts in a partner organization. An attacker could send an email which looks like it is from one of the analysts, asking the scientists to send over the latest data.

Attacks get personal

Attackers are increasingly using tactics that involve their targets' personal lives: The attacker often creates a fake online persona (such as an attractive younger woman), and sends the target requests to connect on social media. In conversations about personal interests, the attacker attempts to gain the target's trust. The attacker then pivots the conversation over to business and sends an email to the target's work email address. Malware is then deployed onto the corporate device to obtain credentials. Figure 1 illustrates an example of a targeted attack.

Trends driving spear phishing and impersonation attacks

In the current environment, attackers can take advantage of several factors:

Remote work

- More users are working remotely and engaging in highly privileged activities never done off corporate premises before.
- Home Wi-Fi networks are often insecure, set up with default passwords, and shared with other family members.

Easier social engineering

- Employees are conducting more of their personal lives online, making it easy for attackers to conduct reconnaissance and connect with them on social networks.

Bring your own device (BYOD)

- BYOD has been increasing for many years and, with remote work, many employees and third parties are using their own devices rather than hardened corporate workstations.

New ways to deceive

- Organizations are embracing new collaboration tools and SaaS applications. As a result, workers may be less likely to question out-of-the-ordinary requests or changes in workflow.

New identities to exploit

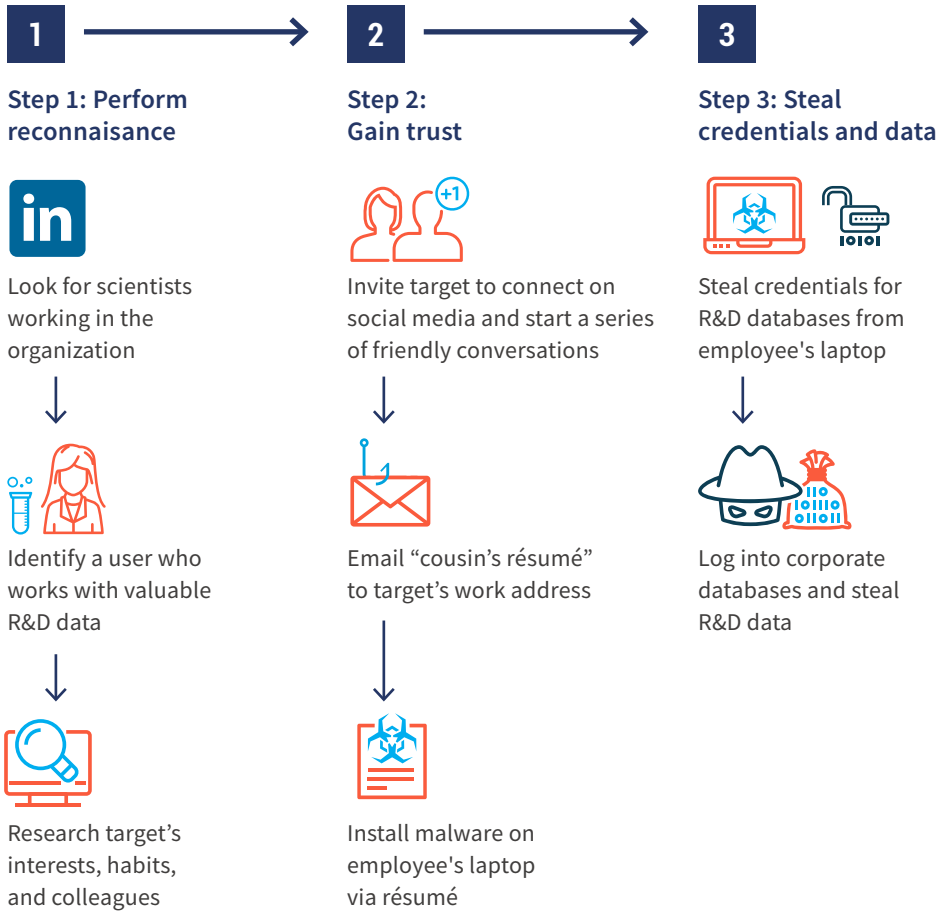
- The expanding use of collaboration tools and SaaS applications is also generating new identities that end up inadequately secured and monitored. With some tools, every time a new team is set up, an email account is created for the team to use. An attacker can compromise this account or generate a fake account to send messages to the team.

Higher receptivity to collusion

- In difficult economic conditions, workers may be more tempted to take payment for use of their access.

Figure 1:

Targeted attack to steal research data



End users are becoming the path of least resistance

End users with high-value access are becoming more interesting targets for several reasons:

IT admin accounts are getting harder to compromise.

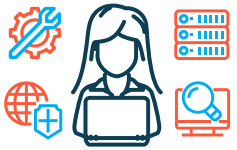
- Many organizations are aware that damaging breaches occur when attackers obtain powerful admin credentials and have put in place strong controls using a privileged access management system.

Opportunities for lateral movement within the network are getting harder to find.

- As organizations move to a Zero Trust model, more endpoints connect to resources directly rather than being given broad access.

Targeted access

The CISOs on our research panel identified three types of access being pursued by attackers and needing strong protection. Workers with these types of access may be employees or contractors.

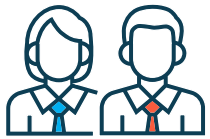


High-level access (human and machine users)

- Powerful administrative access to infrastructure and applications, often across multiple systems
- Ability to manage accounts, reconfigure systems, and make changes to application or security settings
- Examples: domain admin, system admin, application admin, DBA, cloud engineer, DevOps engineer, infrastructure management tool, vulnerability scanner

High-value access (human and machine users)

- End user (business user) access to the organization's most valuable systems and data
- Ability to access confidential data, such as customer records and intellectual property or sensitive operations, such as financial transactions or manufacturing processes
- Examples: researcher, engineer, scientist, accountant, data analyst, backup script, data transfer application



Access subject to impersonation

- Access to accounts for email, collaboration platforms, and social media for key individuals:
  - » Executives: Have authority to request data or transactions based on role
  - » Third parties: Have clout to request data or transactions based on a trusted business relationship

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

In transitioning to Zero Trust, two of the biggest operational challenges will often be: 1) maintaining a complete and up-to-date inventory of users and devices, and 2) minimizing privilege across all infrastructure, applications, and data. Panelists emphasized that although these seem like straightforward concepts, they are particularly challenging to do at scale.

It will take time for organizations to develop comprehensive capabilities. In the meantime, there can be gaps in protecting privileged access that warrant attention. See this report's Recommendations section for tips on building capabilities and dealing with gaps in the interim.

Service accounts can be overlooked

In Zero Trust, the identity of a user is verified, typically using MFA, before access to a resource is granted. While organizations are busy implementing MFA for human users, machine users, such as a script that runs a backup of a database or an automated process that launches an application, can be overlooked.

Organizations often have many service accounts for which credentials are embedded in code or stored locally on a host and not adequately secured. These credentials can be stolen from code repositories such as GitHub, or from files that attackers discover after compromising a host.

The volume and diversity of devices is increasing

Another key aspect of Zero Trust is to verify a device before granting access, including authenticating the device (e.g., using device certificates) and evaluating device hygiene (e.g., ensuring antivirus software is working). The first step is taking an inventory, including OT and IoT devices. Most organizations still struggle with inventories, given the increasing volume and diversity of devices with different operating systems and varying ability to support security software.

> "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

More workers are using unmanaged devices

The difficulties of verifying devices can be compounded by unmanaged devices. Shipping hardened corporate laptops to remote workers is not always feasible and is difficult to scale. And workers may still choose to connect to Internet-facing corporate applications from a personal device. Some organizations leave it up to individuals to harden their BYOD devices, with varying results. When unmanaged devices are used, securing VPN access is problematic since it requires an agent on the device.

Cloud access and remote access can be hard to configure

Least privilege is a central tenet of Zero Trust. However, users are often given too much access, which an attacker can exploit. The growth of cloud and remote work adds to this problem. For example:

- As the number of cloud services proliferates, so does the number of identities and permissions to manage.
- Permissions for cloud services are often difficult to configure.
- Cloud developers often get higher privileges than necessary since some service providers do not offer the ability to precisely minimize privileges.
- Workers who normally do not get local admin access may be given it for working remotely, in order to install applications such as printer drivers.
- Since it is difficult to configure VPN or VDI for fine-grained access at scale, workers often end up with excessive access to the network or applications.

Third parties tend to be undermanaged

For third-party remote access to sensitive corporate resources, all the challenges above apply. Additionally, third-party users are typically not managed in a central location such as a corporate directory or database, which leads to issues such as the following:

- The third-party organization may be given a single account which is shared by all of its workers. This makes it hard to authenticate individual users and track their activities.
- Work assignments may change frequently.
- Access may not be decommissioned promptly when the relationship or task ends.

Key Finding 3: Zero Trust implementations have potential weak spots

A Zero Trust model will better manage information security risks than a traditional perimeter-based model. However, Zero Trust controls can be designed with potential weak spots. The CISO View panelists shared findings from their risk analyses and red teaming activities about how potential weaknesses can be exploited. See this report's Recommendations section for ways to design more effective layers of controls.

Users can be tricked into providing the second factor for MFA

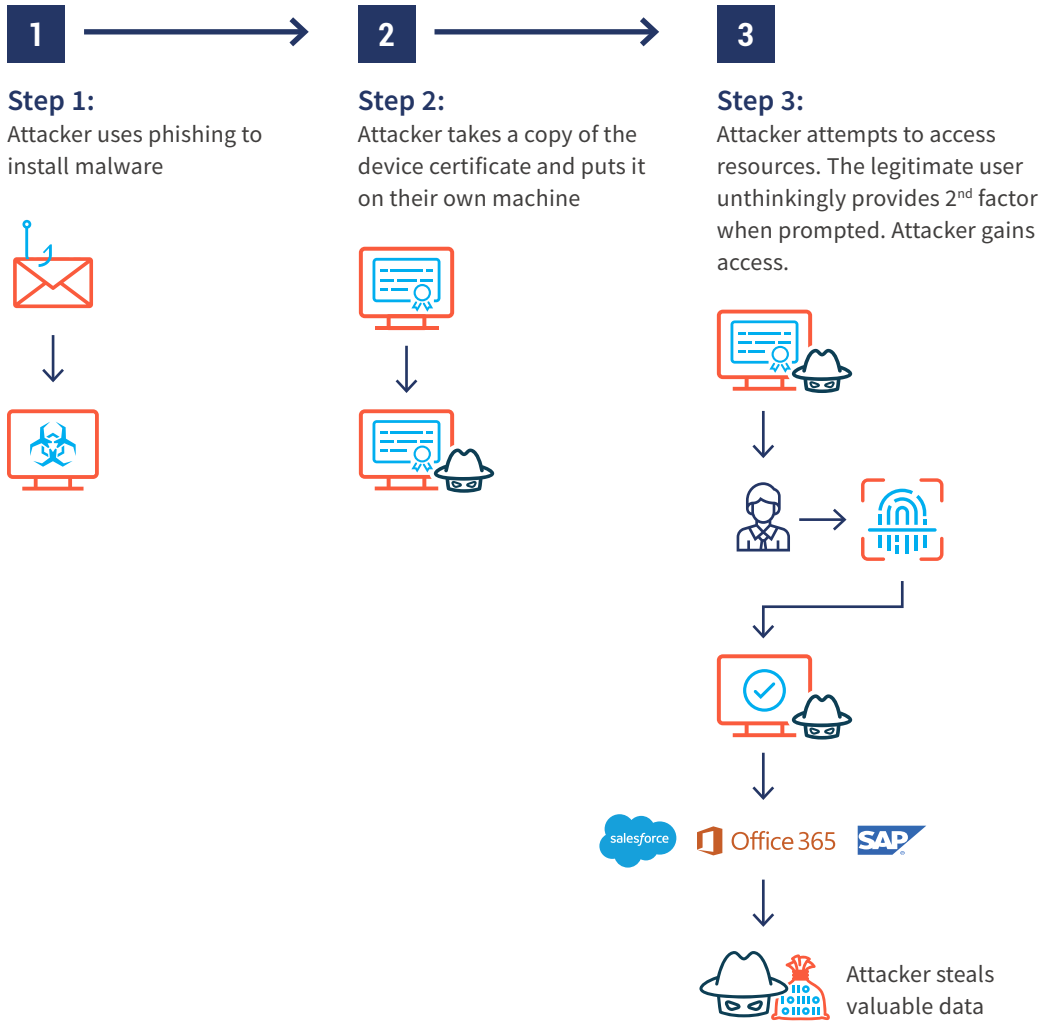
A first step towards Zero Trust is often the implementation of single sign-on (SSO) with MFA. If an attacker steals credentials and then attempts to access a resource, the access should be denied since the attacker will not have the second factor. However, when the attacker makes the access attempt, the legitimate user will be prompted for the second factor. Attackers have several options to trick the legitimate user into responding to the MFA prompt and providing the second factor:

- Attackers could take advantage of MFA fatigue: When workers are asked to re-authenticate over and over, they start to respond without question. Figure 2 illustrates an example of an attack exploiting MFA fatigue.
- By attempting to access the resource over and over, an attacker could flood the user's phone with authentication requests and provoke the user into responding just to get their phone to stop.
- An attacker could, through phishing, present the user with a fake login page to a resource, such as Office 365, then get the user to login and provide the second factor. When the user enters the username and password into the fake login page, the attacker copies them and uses them in the real login page. Office 365 then asks the user for a second factor, which the user expects. The user provides the second factor and the attacker gains access to the user's Office 365 applications.

> "If you present authentication challenges many times throughout the day, humans will learn to just say 'yes' to get rid of it on their screen. You need to factor that into your planning and present challenges as sparingly as possible, so they'll pay attention to it and thoughtfully respond."
>
> **Brad Arkin**
> SVP, Chief Security & Trust Officer
> Cisco

Figure 2:

Exploiting MFA fatigue



Secondary channels can be left unprotected

When resources can be accessed through multiple channels, organizations commonly miss securing secondary channels. For instance, say an organization has set up MFA for an admin to access a server via Remote Desktop Protocol (RDP). If an attacker were to obtain an admin username and password for the server, they would still be prevented from accessing the server over RDP.

However, in Active Directory (AD) environments, remote management ports are enabled by default e.g., Server Message Block (SMB) and Remote Procedure Call (RPC) can be accessed with tools such as PsExec or Powershell. If the attacker uses one of these protocols, a second factor will not be requested. The attacker will be able to log in and gain access to the server using only a username and password. Figure 3 illustrates an example of bypassing MFA through secondary channels.

Figure 3:

Bypassing MFA through secondary channels

1 **Attempt 1:**
Attacker steals password but MFA has been set up for RDP and it stops attacker

2 **Attempt 2:**
Attacker moves to another tool for *non-interactive* access, which does not require a second factor and gets in

*Example: PSExec over SMB, a tool for running processes remotely

Compromised machines are vulnerable to session hijacking

If an attacker can compromise the user's machine, the attacker can bypass the authentication process. For instance, if the user logs into an SSO tool – even with MFA – on the compromised machine, the attacker then has access to the full suite of resources available to the user. Figure 4 illustrates an example of hijacking an SSO session.

New types of privileged security accounts can be targeted

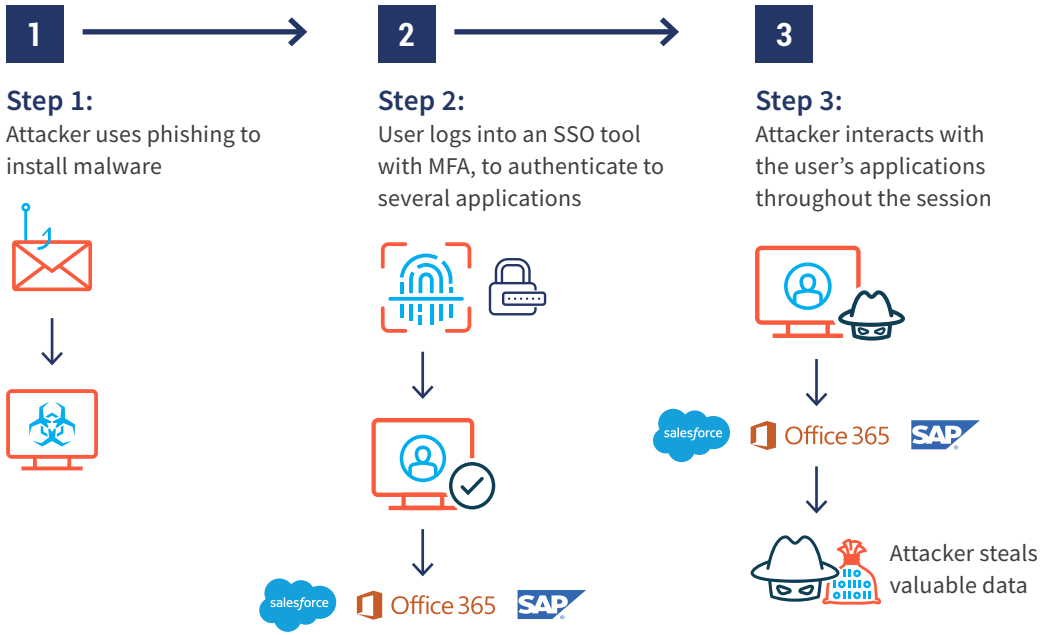
As new security controls are implemented, new security technologies will have new types of privileged accounts associated with them that can be pursued by attackers including:

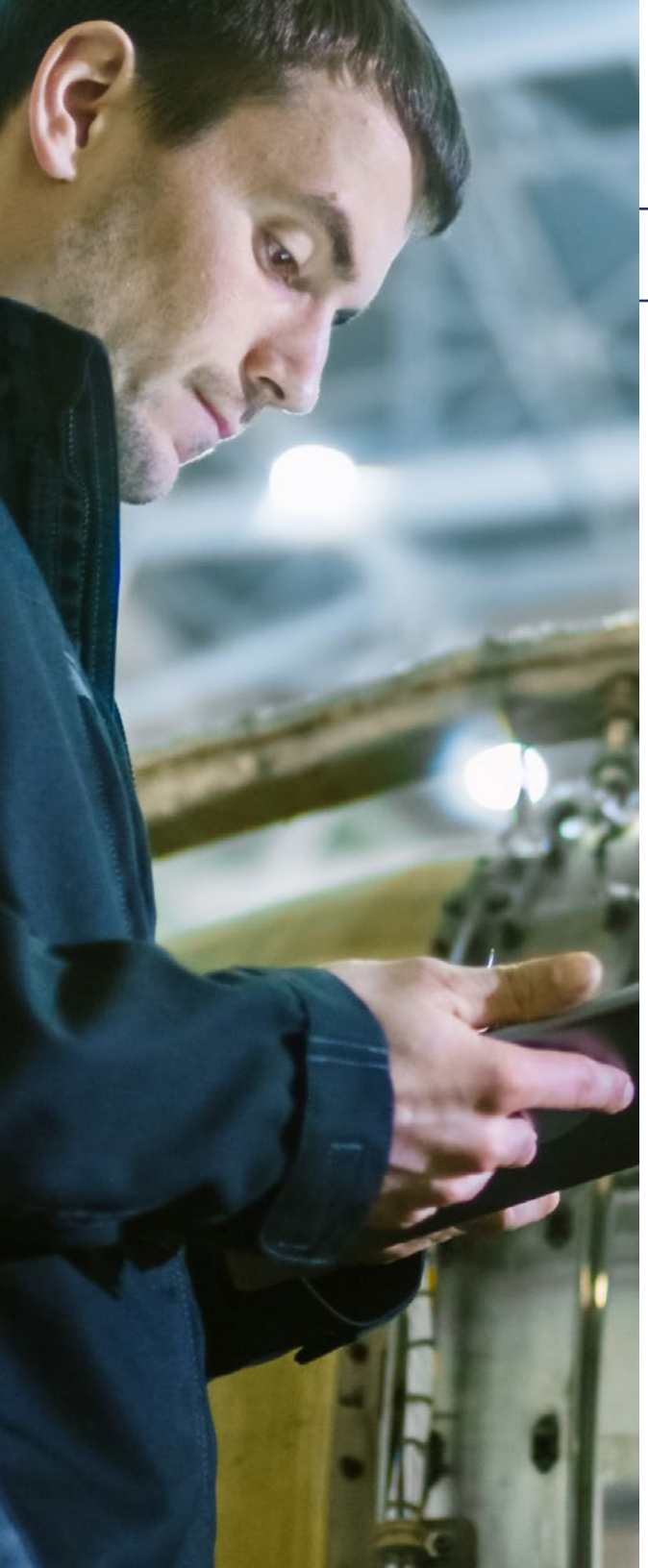
- New admin accounts, such as for MFA, SSO, and PKI
- New service accounts such as Analytics and AI agents

These accounts are exceptionally powerful. If they are not well protected, attackers can misconfigure the system to allow access to resources from the attacker's devices, and/or to deny access requests from legitimate users.

Figure 4:

Hijacking an SSO session





RECOMMENDATIONS

The following recommendations summarize the practical guidance shared by the CISO View panelists regarding evolving a privileged access control strategy for a Zero Trust model.

Recommendation 1: Identify "new" targets subject to increasing attacks

As described in the Key Findings section, attackers are increasingly pursuing end users and other types of new targets with valuable or powerful access. The first step in protecting this access is identifying the targets.

Identify end users with high-value access

Protecting systems and data in a perimeter-less environment typically calls for a more granular level of analysis than many organizations have done. Questions to address include:

What are the organization's most valuable systems and data that are most likely to be targeted by an attacker?

- Where are these systems and data?

What are all the ways that these systems and data can be accessed by users?

- Through what applications and infrastructure?
- What types of users need to interact with them?
- Using what devices?

Depending on the organization, the most valuable systems may be financial systems, customer databases, product development systems and/or manufacturing processes – and targeted by attackers for monetary gain or sabotage.

Inventory your service accounts with high-value access

Service accounts are usually created over time by various developers and not managed centrally. One way to find them is to use analytics to sift through logs for highly sensitive databases and applications, to assess where logins are coming from.

Logins may come from custom scripts developed to automate workflows, do backups, etc. In some cases, logins may come from legacy processes that no longer have a useful purpose. Once identified, service accounts can be better protected or eliminated.

Keeps tabs on new administrative accounts

As organizations implement new security controls, many new types of privileged accounts will need to be protected such as admin and developer accounts for MFA, SSO, and PKI; and service accounts for analytics and AI.

With digital transformation, organizations will also have many other types of new administrative accounts. Maintaining an inventory of all administrative accounts can be challenging, especially for cloud, SaaS, and RPA applications. These applications can be overlooked since the administrator is often not on a technical team.

It can help to work with the procurement team to ensure all new security controls, infrastructure components and applications are identified and brought into the security program.

PROTECTING END USER HIGH-VALUE ACCESS

Technical controls

- Require MFA, using stronger forms of MFA to protect access to higher-risk systems.
- Use adaptive authentication and monitor behavior patterns, applying additional controls if the pattern shows high risk of compromise.
- Consider using time-of-day access restrictions.
- Use a Privileged Access Management (PAM) system to manage certain types of credentials that are shared/ delegated or for emergency access
- Consider using a PAM for especially sensitive access and/or for dual control and session recording.
- Use endpoint security protections.
- Remove local admin access and/or allow whitelisted or greylisted applications only.

Targeted user training

- Provide additional security education and awareness and more frequent spear phishing tests.
- Use gamification to encourage users to better secure their access or remove unnecessary privileges.
- Educate executives on how to keep personal social media and other accounts safe to reduce the risk of impersonation.

Recommendation 2: Ensure MFA implementation is effective

Organizations often start their Zero Trust journey by focusing on MFA. It is important to get it right, which includes taking proactive steps to help ensure attackers do not get around it.

Use standards-based SSO

Panelists strongly advise reducing the vast number of passwords in use within organizations as they are inherently vulnerable to compromise.

- MFA combined with SSO improves the user experience by reducing logons and replacing password usage with methods such as device certificates, biometrics, and push notifications.
- Where possible, use or build SSO tools supporting standard protocols such as SAML or OpenID Connect.

Lock down MFA registration

When MFA is provisioned to a user, the organization must be confident the user is who they claim to be. Otherwise, attackers can steal passwords then attempt to register their own devices as authentication factors. Ways to lock down the MFA registration process include:

- Use an out-of-band process such as a phone call to check if a registration request was made by the legitimate user.
- Consider not allowing registration on more than one device.
- Ensure the user presents valid ID such as a passport.

Own the user experience for authentication

As part of the authentication program, Security should own the user experience. The following guidelines can help to optimize security and user acceptance:

- Make the authentication experience consistent across all types of applications and platforms (e.g., web vs. mobile)

> "Security often thinks that user experience is a product management or application team function, not a security function. But if we go back and look at it, we own the user experience for authentication, and we should normalize that experience, so people know what to expect."
>
> **Dave Estlick**
> CISO
> Chipotle

- Use easier methods such as biometrics or push notifications where possible.
- Align the method to the sensitivity of the system. For example, highly sensitive systems might require a one-time password while less-sensitive systems require a push notification.
  - » Explain the different grades of MFA to users so those who can use easier methods appreciate it.

Present reauthentication requests sparingly and as expected by the user

To prevent MFA fatigue in which users respond to MFA prompts without thinking, which can be exploited by attackers:

- Ensure reauthentication requests make sense to the user, such as for unusual activity or location.
  - » If requests do not make sense, users will find it frustrating and pay less attention. For instance, if a user working from home changes to a different ISP but stays in the same location, a reauthentication request may not make sense to them.
- Do not bombard users with requests that will habituate them to respond without thinking.
- Have requests be out-of-the-ordinary so the user will pay attention, and thoughtfully respond.
  - » Have users contact Security when something seems anomalous.
- Set up a system to send an alert if a user's device is being flooded with reauthentication requests which could be an attacker attempting to get the user to respond.

ANALYTICS IS A CORE COMPETENCY IN ZERO TRUST

- Zero Trust is centered on assessing each access request to determine if/how to provide access to a corporate resource.
- This requires sophisticated analytics; organizations plan to build these capabilities over time.
  - » Technologies such as adaptive authentication, PAM, and UEBA include analytics functionality.
  - » Currently getting a complete picture across endpoint telemetry, IAM, UEBA, and the SOC, requires extensive integration work.
- Further developments in technology will be needed to overcome challenges and meet aspirational requirements
  - » AI and machine learning may help deal with complexity of assessing each access request in real-time and at scale and in delivering a smooth user experience.
  - » Aspirational requirements include looking at group behavior.
    - ◦ For example, to assess whether the user is acting in a way that is consistent with not only their own past behavior, but also with others in their role and/or department.

Use analytics to balance security with user experience

With an adaptive authentication system, user and device context are analyzed to determine whether the initial access request and ongoing session are "normal." The system should know, for instance, if the user is attempting to access a database not usually accessed as part of their day-to-day activities or if a device is in a different city than usual. If the context is not normal, the system adapts controls such as requesting reauthentication or adjusting the level of access.

Analytics can help to minimize friction by putting up gates only when absolutely necessary, based on a risk score.

Collaborate with the business to understand what behavioral patterns are to be expected. For example, having someone in a certain finance role log in five times in rapid succession may be normal at a particular time in the quarter. For administrators, tasks can vary greatly so behavior may be more difficult to model. In these cases, rely more on session recording and auditing.

To help defend against attacks which use a fake login page, notify the user and send an alert to Security if unusual logins detected such as:

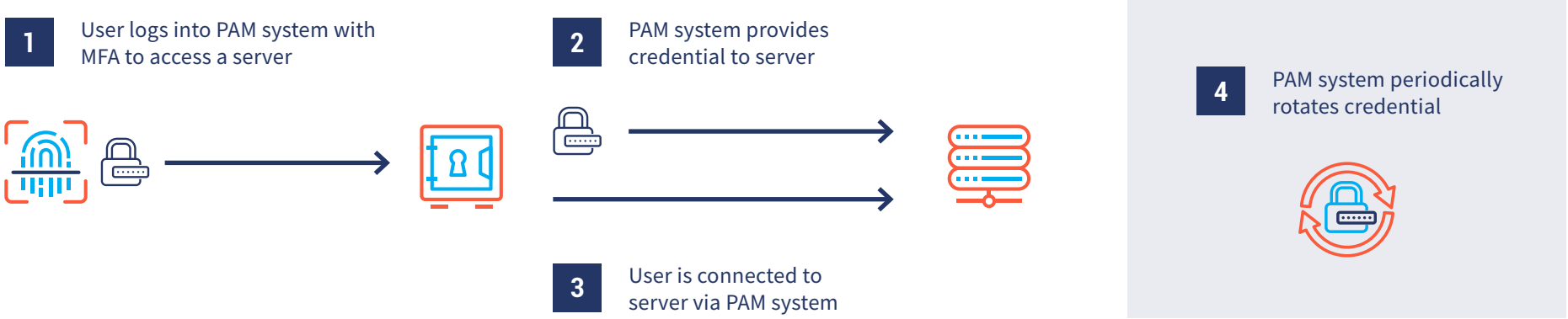
- Username/password entered in a different location from where the second factor was provided.

Combine MFA with privileged access management to protect all channels

For protecting a resource such as a server, to ensure secondary channels are not exposed, combine MFA with a privileged access management (PAM) system. In this approach, credentials for accessing a sensitive server are stored in the PAM system's vault. MFA is required to log on to the PAM system and check out the credential for the server. See Figure 5 below. With a PAM system, the session can be isolated so the credential is not exposed on the endpoint, and all credential usage can be monitored regardless of the channel used.

Figure 5:

Protect admin access to a server



Use alternatives to MFA for service accounts

For protecting service accounts, use various methods including:

- Where possible, have applications authenticate to services or databases via standards such as OpenID Connect, rather than via credentials that can be stolen.
- For some lower-risk cases such as service accounts with read-only permissions, an alternative to MFA is to apply static rules such as allowing the account to be used only from a particular machine and network location, on a particular day of the week, and for a limited amount of time that day.
- For higher risk service accounts, such as accounts with permissions to install software, integrate the application or process with a PAM system.

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

Higher-risk credentials require heightened protection in a PAM system to provide:

- Storage of credentials in a centralized, enterprise-grade vault
- Strong authentication for retrieval of credentials by authorized users
- Ability to trace usage of credentials to individual users
- Automatic rotation of credentials
- Monitoring, auditing, and recording of credential usage
- Revocation of access in the case of anomalous behavior
- Time-of-day restrictions
  - » Access management tools can typically provide time-of-day restrictions for applications. PAM tools can provide a wider range of controls for both applications and infrastructure.

PAM systems should be used to protect all high-level, administrative access for human or machine users, such as an IT admin or a process with administrative access to infrastructure.

Manage certain types of end-user access with a PAM system

In a Zero Trust model, most end-user access to applications is protected with controls such as MFA and adaptive authentication. However, the panelists recommend using a PAM system when certain security benefits are required, as described below.

Individual accountability for use of shared accounts

All shared accounts used by more than one person should be managed in a PAM system. Authorized individuals check out the credential as needed and their usage is monitored, enabling individuals to be held accountable.

Dual control and session monitoring

Some credentials are so critical, they should be used only with dual control and thus managed through a PAM system. Configure the PAM system to require two users to check out the credential, and have the session monitored and recorded for full auditability.

Alternative to federated identity

To provide single sign-on to an application that doesn't support a protocol such as SAML, consider managing the password in a PAM system and integrating the PAM system with the SSO tool. This will be more secure than having the SSO tool store the password.

Protection for higher-risk service accounts

Service accounts with access to very sensitive systems should be managed in a PAM system.

> "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

Plan for resilient IAM infrastructure

With Zero Trust, day-to-day organizational operations are increasingly reliant on high availability of identity and access management systems, including adaptive authentication and PAM systems. To protect systems against destructive attacks, consider having a clean build off site and set up frequent (possibly daily) updates. It is especially critical to have a back-up copy of all emergency access credentials.

Types of access managed through a PAM system

ALWAYS MANAGE IN A PAM SYSTEM:

- Domain, Windows, server, and workstation administrator accounts
- Accounts for developing and managing infrastructure
- Cloud and DevOps accounts
  - » e.g., IaaS admin accounts
- Robotic Process Automation (RPA) accounts
- Accounts for developing and managing all security controls
- Database admin (DBA) accounts
- Application administrator accounts
  - » e.g., SaaS applications
  - » e.g., Collaboration platforms
- Break-glass/emergency access accounts
- Secrets used for emergency admin access to applications, such as secret sign-in URLs that bypass MFA
- Shared/delegated accounts
  - » e.g., Corporate Twitter account
  - » e.g., CEO or other executive account used by an admin or Chief of Staff
- Other accounts as required for regulatory compliance

CONSIDER MANAGING IN A PAM SYSTEM:

- Accounts used for highly sensitive activities which require dual control and/or session recording
- Accounts for sensitive applications whose passwords cannot be eliminated through federated identity in an SSO tool
- Higher-risk service accounts with access to very sensitive systems
- SSO accounts of individuals with extremely sensitive access, such as executives

1 See the previous CISO View report, *Protecting Privileged Access in DevOps and Cloud Environments*

2 See the previous CISO View report, *Protecting Privileged Access in Robotic Process Automation*

> "To defend against ransomware threats and be resilient, keep a clean build of your critical systems, such as PAM, off net."
>
> **Emma Smith**
> Global Cyber Security Director
> Vodafone

Recommendation 4: Allow just enough access

The CISO View panel emphasized the importance of providing "just enough": Just enough access for just enough time to just enough resources. This minimizes the impact of any intrusion, by giving the attacker a smaller footprint in which to move.

Review and minimize access regularly

For all valuable resources, minimize the number of accounts, users with access to accounts (human and machine) and their privileges. Less access is easier to protect, restrict, and review.

- Make it a priority to know who has access to what.
- Establish processes to regularly remove unnecessary privileges and accounts.
- For third party access, set it up to be automatically revoked after the contract expires.
- Aim to implement analytics to review and tighten access. For example:
  - Accounts or permissions that have not been used in a long time could be identified and automatically removed.
  - Access only needed at a certain times of day could be identified.

Limit user connections to a single resource or narrow subset

There are various ways to avoid providing excessive access when connecting users to corporate resources. Proxy technologies provide a secure connection to a specific resource (on-prem or in the cloud) rather than using VPN, which provides a secure connection to a large part of the corporate network. For using VDI to connect to resources, VDI templates can help configure access so that specific user roles are provided with limited access to specific resources. VDI can also be configured to restrict downloading of data.

> "To get to market faster, businesses might put apps in the cloud and run their own services. And they might not go through IT. In this case, it doesn't matter if they don't call themselves administrators, they're still performing elevated functions."
>
> **Melissa Carvalho**
> VP, Enterprise and Customer Identity and Access Management
> Royal Bank of Canada (RBC)

Use a tiered jump server to connect admins to infrastructure

Connecting admins to infrastructure through a jump server (bastion host) isolates the user's endpoint from the corporate resource. Using a tiered jump server in conjunction with a PAM system ensures privileged credentials are not exposed on the endpoint, and also ensures credential boundaries are not broken. Require MFA to access credentials from the PAM system.

- Users with different tiers of privilege should not be granted OS-level access to the same jump server, as this could be used to escalate a user's privilege.
- A jump server can be configured to prevent data from being transferred from the corporate resource to the endpoint, and vice versa.

Isolate unmanaged devices connecting to corporate resources

If an employee or third-party contractor is using their own device or if endpoint hygiene is unreliable, there is increased risk the device may be compromised. To reduce the risk of malware spreading from an infected endpoint to corporate resources, isolate the device using a jump server (bastion host) or VDI.

Compartmentalize cloud resources to minimize access

One way to avoid giving any one person broad and pervasive power is to compartmentalize resources. For instance, instead of having one cloud account that is shared among many users across an organization, have many cloud accounts (say one for each application), so that each account is used by a smaller set of users.

This approach can be simpler to manage than managing fine-grained permissions for many users of one cloud account.

> "In my opinion, Zero Trust is really focused on separation of duties, making sure you don't give all the power to one person. With the cloud, it's even more important. If you have a single account for your whole company, one technical administrator will have full privileges on everything."
>
> **Olivier Perrault**
> CISO
> Orange Business Services

Minimize local admin access and restrict software installation

If an attacker compromises a user's device, their ability to install damaging malware and move laterally is greater if the attacker obtains local admin privileges.

- Many organizations do not allow local admin access or allow it only for certain roles.
- If users are provided with local admin access, ensure they fully attest to their obligations under an acceptable use policy.
- Endpoint protection technology can restrict installations to whitelisted or greylisted applications.
- Just-in-time access, described below, can enable users to temporarily elevate privileges to install software such as a printer driver.

Provide just-in-time access to privileges

Minimizing "standing" privileges can help ensure least-privilege. Rather than providing credentials that have all privileges all the time, a just-in-time (JIT) approach analyzes requests in real time and gives privileges to users for limited amounts of time.

- Adaptive authentication technology can be used to set up JIT access:
  - » Additional access is based on a risk score.
- PAM systems can also be used for JIT access:
  - » Have users check out privileged credentials for a specified period.
  - » Send a request to temporarily add the user to the Admin group on the user's device.

TERMINATE OBSOLETE SAAS ACCOUNTS

Each account in a SaaS application typically has an access path via SSO and a direct access path via the application. When someone leaves an organization, a common mistake is to terminate SSO access but not the actual SaaS application account, so that the username/password combination for these accounts could continue to be used. Have a process to terminate obsolete SaaS accounts.

Develop ways to make JIT easy to use and audit

- Use automated approvals as much as possible
  - » Approving requests adds to the workload of managers and if given constant requests, they will end up approving them without thinking.
- Err on the side of granting more time than estimated
  - » If a task takes longer than expected, having access expire before the work is complete can cause problems.
- Combine JIT with session recording to help ensure accountability
  - » Verify that the reason given for requesting the credential matches the use.
- Consider integrating all requests for JIT access with the organization's ticketing system to ensure all access requests are tracked and monitored.

Recommendation 5: Drive a cultural change

Zero Trust is not just a set of controls; it is also a mindset and requires a cultural shift. An organization must rein in access, add security steps to workflows (like requests for reauthentication), and get users to accept more responsibility for security. To be successful, the CISO and security team will need the support and engagement of stakeholders throughout the organization.

Emphasize "trust" versus zero trust

Several panelists noted that the term "Zero Trust" can be misinterpreted as implying that the organization does not trust their employees. Some organizations avoid the term "Zero Trust" altogether, replacing it with terms such as "Earned Trust" or "<Company name> Trust".

The access request "earns" trust by having the characteristics of the user, device, and environment be tested.

> "For just-in-time, there can be challenges. For example, you don't want to block an admin halfway through a server reconfiguration because the time allotted was too short. Give them more time than they need and record the session to avoid these situations."
>
> **Peter Fizelle**
> CISO
> Asian Development Bank

Convey "less is more" when it comes to privilege

Make sure employees realize they are responsible for the access they have been granted and that having less privilege is in their own interest; having too much creates risk for them. Be clear that privilege reduction is happening across the organization – in other words, "It's not just you." If possible, start awareness campaigns well in advance of taking concrete action. For instance, announce that local admin access will be broadly revoked in six weeks. This gives employees time to think of new ways of working and to vent early on if they need to.

> "It's a big cultural change. People have to understand that least privilege means they're not going to have unlimited access. You have to explain why you're taking access away. 'It's not just for the sake of removal, it's to make sure we're secure as a company.'"

Tim Bengson
VP, Global CISO
Kellogg Company

CONTROLS FOR THIRD-PARTY ACCESS TO CORPORATE RESOURCES

- For administrative access and/or if an account will be used by multiple individuals, use a PAM system to ensure access is traceable.
- Set up an individual account in the PAM system for each third-party employee.
- Isolate corporate resources from the third party's network and endpoints. Require the use of jump servers (bastion hosts) or VDI.
- Frequently review access and remove it when the relationship ends.

Protect your user population from impersonation

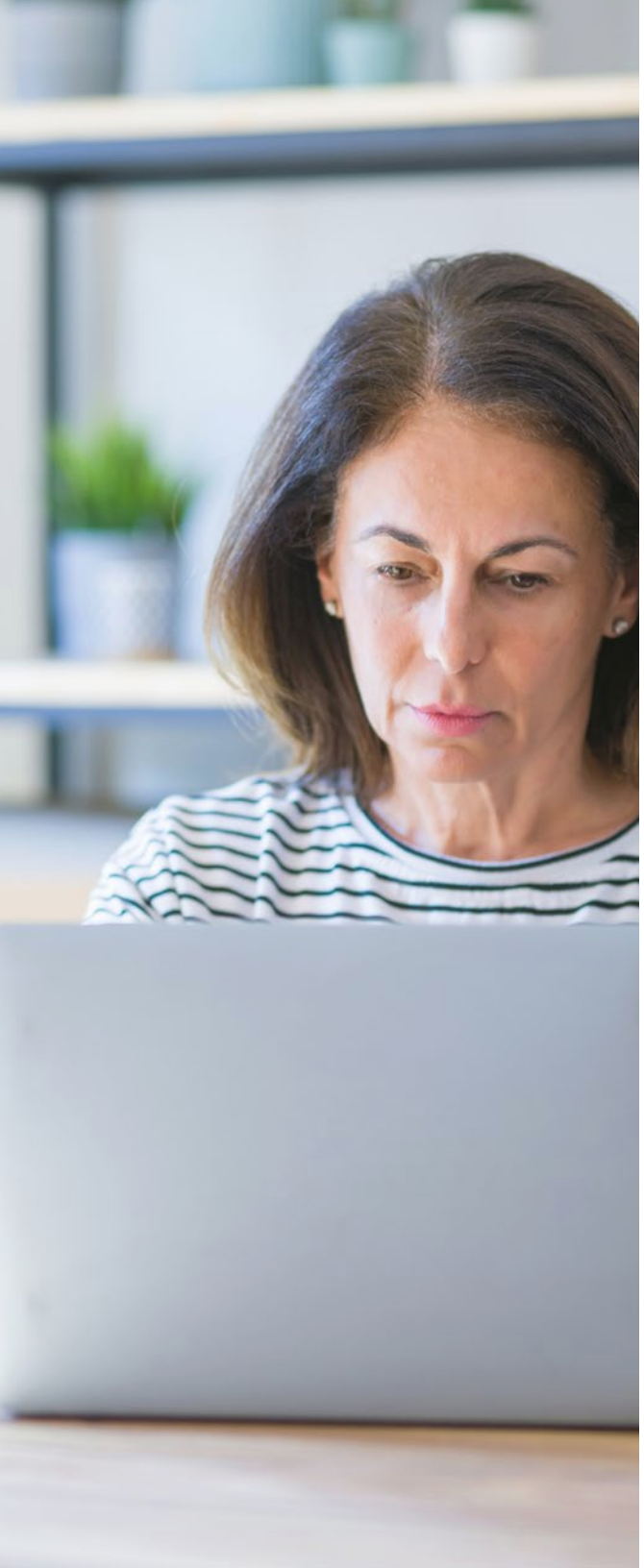
As discussed in Key Finding 1, attacks based on impersonating executives or third parties are on the rise. To mitigate the risks of these attacks:

- Raise awareness of the potential for attackers to impersonate executives, partners, or customers using email spoofing, collaboration platforms, and fake personal accounts.
- Analyze incoming emails to assess whether they come from the domain they claim to be from and whether they have known characteristics of malicious actors.
  - » Have an inventory of social media accounts for key executives and be able to detect when a fake account for an executive is created. Social media companies will take down these accounts if notified.
- Provide recommendations to executives on how to secure their social media and mobile phone accounts.
- Aim to develop a culture in which an unusual message makes everyone think of picking up the phone and asking the sender if they actually sent it. This may require adjustment in leadership styles if leaders are used to getting their requests implemented immediately.
- Consider an awareness campaign to simulate business email compromise, such as having the Chief Data Officer send data scientists an email that unexpectedly asks for a large amount of sensitive data.

Panelists noted that this cultural change aligns to the spirit of Zero Trust: Everyone should assume attackers are present, constantly assess risk, and verify claims that others are who they say they are.

KEEPING UP WITH SPEAR PHISHING TECHNIQUES

- Communicate newer attack techniques such as the use of fake personas on social media. Remind users to inform Security when they see social engineering attempts.
- Research types of attacks being perpetrated at other organizations. Educate users so that they are aware of these techniques.
- Make sure the intended targets of spear phishing know they were targeted, even if the attempt was blocked by technical controls. If there is an actual account compromise, consider telling the whole company. "It happened here" is a powerful message.
- Awareness campaigns cannot always prevent a user from falling for attackers' techniques.
  - » Use analytics to detect abnormal behavior of the user or changes to the device during a session.
  - » When deploying endpoint security controls and IAM, consider prioritizing users who have a record of clicking on phishing attempts.



Use targeted marketing and gamification

Panelists suggested ways to focus education and awareness efforts for maximum benefit:

- Prioritize users who are likely targets of spear phishing for education and awareness efforts.
- Use marketing techniques such as social media campaigns to develop more compelling content about security risks.
- Tailor messages to specific departments. E.g., Finance may have a different communication style than IT.
- Give remote workers specific guidance on securing their home working environment, such as changing the default password on their home router.
- Use gamification, scoring, and dashboards to drive competition between users to avoid risky behavior.
- Incentivize users to look for ways to minimize their own privileges. As they reduce privileges, they gain points.

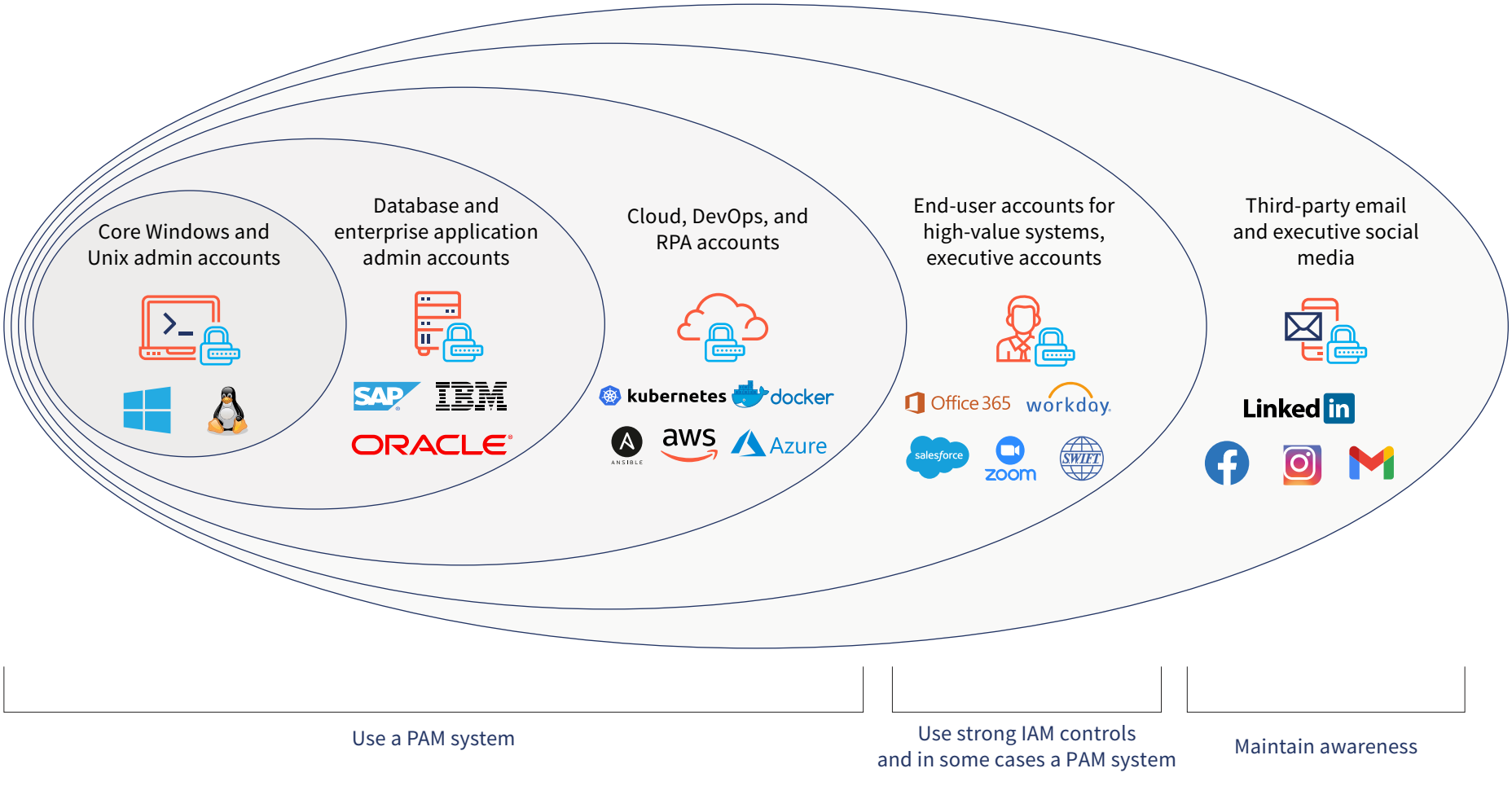
> "Executives are often targeted by spear phishing attacks, and they might not even realize it. Make sure to tell them, 'Hey, you were targeted by this phishing email and we caught it.' It's like knowing that houses are being broken into in your neighborhood; if you know, you're going to be more careful."

Dawn Cappelli
VP, Global Security and CISO
Rockwell Automation

Figure 6

The widening range of targeted accounts

Security teams must consider a wider variety of accounts than ever before, including applications beyond the corporate boundary and fake accounts created by attackers



APPENDIX: BIOGRAPHIES OF CISO VIEW PANEL

Top Information Security Executives from Global 1000 Enterprises

Alissa (Dr Jay) Abdullah

SVP and Deputy Chief Security Officer, *Mastercard*

Dr. Jay leads the Emerging Corporate Security Solutions team and is responsible for protecting Mastercard's information assets and driving the future of security. Previously, she was CISO at Xerox where she established and led a corporate-wide information risk management program. She was the first CISO of Stryker, a leading medical technology company, and also served as the deputy CIO of the White House where she helped modernize the Executive Office of the President's IT systems with cloud services and virtualization.

Brad Arkin

SVP, Chief Security & Trust Officer, *Cisco*

Brad Arkin leads Cisco's Security and Trust Organization, whose core mission is to ensure Cisco meets its security and privacy obligations to customers, regulators, employees, and other stakeholders. Previously he was Chief Security Officer at Adobe and has held management positions at @Stake and Cigital. He holds a B.S. in computer science and mathematics from the College of William and Mary, M.S. in computer science from GWU, and MBA from Columbia University and London Business School.

Tim Bengson

VP, Global Chief Information Security Officer, *Kellogg Company*

Tim Bengson is responsible for building and maintaining a security program that protects Kellogg's critical assets, its workforce, and that enables business capabilities. Tim is responsible for all aspects of information security – operations and cyber defense; business engagement and solutions; governance, risk and compliance; identity and access management; and security transformation. Prior to joining Kellogg's, Tim held senior leadership and management roles in information security and It at Mastercard and Express Scripts.

Top Information Security Executives from Global 1000 Enterprises (continued)

Dawn Cappelli

VP, Global Security and Chief Information Security Officer, ***Rockwell Automation***

Dawn Cappelli is responsible for developing and executing a holistic cybersecurity strategy to ensure Rockwell Automation and its Connected Enterprise Ecosystem – the company's infrastructure, products, and customers – is safe, secure, and resilient. Dawn started at Rockwell Automation as Director, Insider Risk. She was previously Founder and Director of Carnegie Mellon's CERT Insider Threat Center and co-authored the book "The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)."

Melissa Carvalho

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

Melissa Carvalho leads a team of over 200 security professionals providing cyber solutions and services for the bank's 80,000 employees and 16 million clients worldwide. Over 15 years, her work has covered many aspects of information technology including business needs impact assessments, software development, and infrastructure implementations. An industry-recognized leader in IAM, Melissa has implemented Identity Programs at Canada's five major banks and consulted on over 50 IAM programs across North America.

Dave Estlick

Chief Information Security Officer, ***Chipotle***

Dave Estlick is responsible for the creation and governance of Chipotle's global information security roadmap. Previously, Dave was CISO at Starbucks and has held security leadership roles at PetSmart and Amazon. Most recently, he was inducted into the 2020 CSO Hall of Fame. He serves on the Board of Advisors for Cyberstarts, Clear Sky and PCI Security Standards, and the Board of Directors for Internet Security Alliance, Retail Cyber Intelligence Sharing Center, and Security Advisor Alliance.

Peter Fizelle

Chief Information Security Officer, ***Asian Development Bank***

Peter Fizelle leads information security at ADB, focused on enabling the business to pursue leading digital transformation strategies, while reducing risk to the organization and increasing operational effectiveness. He has many years of experience in information security and technology within banking, government, managed services, and an intelligence agency. Prior to ADB, his roles in banking also included technology and risk management roles at Commonwealth Bank, ANZ, UBS, RBS, ABN-Amro and Deutsche Bank.

Top Information Security Executives from Global 1000 Enterprises (continued)

Mike Gordon

VP and Chief Information Security Officer, ***Lockheed Martin Corporation (LMC)***

Mike Gordon is responsible for overall information security strategy, policy, engineering, operations, and cyber threat detection and response. With 19+ years of experience at LMC, Mike oversees a globally recognized team of cyber security professionals. His prior roles include Director of Intelligence and Operations. Mike is a founder and board member of the Defense Information Security Exchange (DSIE) and National Defense Information Sharing and Analysis Center (ND ISAC), and chairs the Defense Industrial Base Sector Coordinating Council (DIB SCC).

Omar Khawaja

VP and Chief Information Security Officer, ***Highmark Health***

Omar Khawaja has been developing and managing security solutions for startups, service providers, consulting firms and enterprises. He is currently CISO at Highmark Health, an $18 billion integrated health care delivery and financing system, employing 40,000 and serving 50 million Americans. Prior to Highmark Health, he was at Verizon Enterprise Solutions, where he was responsible for a portfolio of security solutions with customers in 72 countries.

Olivier Perrault

Cyber Security Officer, ***Orange Business Services***

Olivier Perrault is Cyber Security Officer at Orange Business Services, a global IT and communications services provider. His mission is to prepare Orange Business Services to anticipate, prevent, resist, manage and recover from cyber-attacks, which could cause tremendous damages to the company or to its customers. Previously, Olivier was CISO at Orange Cloud for Business, one of the major cloud services providers for businesses in Europe, leading the security department. His 20+ years at Orange includes also several director roles in R&D and wholesale divisions.

Top Information Security Executives from Global 1000 Enterprises (continued)

Emma Smith

Global Cyber Security Director, ***Vodafone***

Emma is responsible for information and cyber security globally across Vodafone. Her team sets policy, manages security risk, defines security architecture, delivers security solutions and operates global 24/7 cyber defense capabilities. Enabling a secure connected future for our customers and society is the Vodafone security vision. Emma is passionate about security and how we can build diverse teams to collaborate across the communities we operate. Previously, Emma was CISO at the Royal Bank of Scotland, leading an integrated team responsible for physical and information security, fraud prevention, and business resilience.

Daniel Tse

Head, Cyber Security, Information & Technology Risk, ***GIC Private Limited***

Daniel Tse leads cyber security at GIC Private Limited, a sovereign wealth fund which manages Singapore's foreign reserves. Daniel has experience in operational risk management, enterprise architecture, application delivery, infrastructure services and project management. With a demonstrated history in the financial services industry, his previous roles include executive positions in IT risk management at UBS AG and Citi; most recently as Executive Director, APAC Head of IT Risk at UBS AG.

ABOUT THE CISO VIEW INDUSTRY INITIATIVE

Sharing information on good security practices is more important than ever as organizations face increasing cyber security risks. At CyberArk, we believe if security teams are armed with the leading wisdom of the CISO community, it will help strengthen security strategies and lead to better-protected organizations. Therefore, 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. By developing CISO reports, studies and roundtables, the initiative generates valuable peer-to-peer guidance and dialogue. For more information on this initiative, go to **www.cyberark.com/cisoview**.

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