THE **CISO VIEW**

AN INDUSTRY INITIATIVE SPONSORED BY **CYBERARK**

Rapid Risk Reduction: A 30-Day Sprint to Protect Privileged Credentials

With contributions from a panel of **Global 1000 CISOs:**

Rob Bening
Chief Information Security Officer,
ING Bank

David Bruyea
Senior Vice President and Chief
Information Security Officer, CIBC

Dawn Cappelli
Vice President and Chief Information
Security Officer, Rockwell Automation

Jim Connelly
Vice President and Chief Information
Security Officer, Lockheed Martin

Dave Estlick
Senior Vice President and Chief
Information Security Officer, Starbucks

Steve Glynn
Chief Information Security Officer,
ANZ Banking Group Limited

Mark Grant
Chief Information Security Officer, CSX

Gary Harbison
Chief Information Security Officer,
Monsanto Company

Kathy Orner
Vice President and Chief Information
Security Officer, Carlson Wagonlit Travel

Chun Meng Tee
Vice President and Head of Information
Security, SGX

Munawar Valiji
Head of Information Security, News UK

Mike Wilson
Senior Vice President and Chief
Information Security Officer, McKesson

For this CISO View research report, we drew from the experiences of security professionals and technical experts who have been on the front lines of breach remediation efforts. It provides an inside look at the lessons learned from several high-profile data breaches. This report outlines a proven framework for an intensive sprint of approximately 30 days, to implement a set of key controls around privileged credentials.

TABLE OF CONTENTS

A Word From Our Sponsor

CYBERARK® The CISO View report series is sponsored by CyberArk and developed by an independent research firm, Robinson Insight. 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 and guest contributors are helping the larger community address this issue.

Featuring input from **guest contributors:**

Technical experts and consultants who have worked with major organizations post-breach:

John Gelinne
Managing Director, Advisory Cyber Risk Services,
Deloitte & Touche

Gerrit Lansing
Chief Architect, CyberArk

Security executives from major organizations that have experienced large data breaches*

** Due to legal constraints, these executives have contributed to this research report without attribution.*

INTRODUCTION

How do you avoid a data breach? Ultimately you need to know what techniques attackers are using and what security controls would stop them. To get this information, CISOs often turn to an unenviable group of experts: organizations that have already been breached.

For this CISO View research report, we drew from the experiences of security professionals and technical experts who have been on the front lines of breach remediation efforts. It provides an inside look at the lessons learned from several high-profile data breaches.

In the past 24 months, many successful attacks have used hijacked privileged credentials. For the incidents we studied, attackers were able to obtain domain-level Windows admin credentials by exploiting common vulnerabilities found in most enterprise IT environments.

These attack techniques have become relatively easy to wield with the proliferation of toolkits for creating malware. They have been used to achieve complete network takeover and massive data exfiltration.

Given the increasing risks, protecting privileged credentials is becoming a top priority at many organizations today. Fortunately, significant risk reduction does not take long. With a sufficient sense of urgency, it can be achieved in a matter of weeks — as is often done in the wake of actual breaches.

This report outlines a proven framework for an intensive sprint of approximately 30 days, to implement a set of key controls around privileged credentials. The recommendations, developed in collaboration with our esteemed panel of Global 1000 CISOs, enable security teams to proactively protect their organizations.

How can CISOs and security teams use this research report?

- Apply lessons learned from actual data breaches
- Sharpen your knowledge of attack techniques that exploit Windows admin credentials
- Explain these techniques to stakeholders
- Assess your risks: how susceptible is your organization?
- Analyze your existing controls: how do they measure up against recommended practices?
- Prioritize the implementation of new controls: what to do first?
- Gain the support of executive leadership and convince IT admins

> [In analyzing 2,260 breaches], almost two-thirds of the breaches were made possible by the use of weak, default or stolen passwords.*

*Verizon 2016 Data Breach Investigations Report

KEY FINDING: **ATTACKERS EXPLOITED VULNERABILITIES WITH WINDOWS ADMIN CREDENTIALS**

While privileged credentials have long been prone to compromise, the vulnerabilities associated with the administrative credentials used to manage workstations, servers and domain controllers in the Windows environment have become especially acute. Attackers have learned to take advantage of the way Windows machines store privileged credentials in memory, combined with the way organizations commonly manage privileged credentials in the Windows environment.

In the incidents we looked at, after the initial intrusion through phishing, attackers were able to use extracted credentials to move from machine to machine on the network. According to the Mandiant M-Trends 2016 report, targeting highly privileged accounts and extracting credentials from memory has become “almost trivial” in most Windows environments due to the widespread availability of toolkits. Mandiant’s Red Team, on average, is able to obtain access to domain administrator credentials within three days of gaining initial access to an environment.

These techniques not only work fast; they can also provide attackers unprecedented levels of control. One of the most dangerous is the golden ticket attack whereby an intruder compromises a domain controller and steals the secret key used to encrypt and sign Kerberos tickets. With this master key, the attacker can quietly obtain any privilege for access to anything they want – effectively owning the corporate network, including all the critical assets and all of the security systems joined to the domain.

Microsoft has acknowledged the risks of credential theft associated with the Windows environment and is working on hardening the Windows environment to prevent credential scraping techniques. However, it will be several years before all of the updates are fully released and deployed in organizations.

> Because many existing implementations of Active Directory Domain Services have been operating for years at risk of credential theft, organizations should assume breach and consider the very real possibility that they may have an undetected compromise of domain or enterprise administrator credentials.
>
> **—MICROSOFT,**
> “MITIGATING PASS-THE-HASH AND OTHER CREDENTIAL THEFT, VERSION 2,” 2014

How Vulnerable Is Your Organization?

Examples of common practices that make organizations susceptible to attack:

- Providing end users such as software developers or remote sales people with local admin rights on their workstations
- Having IT helpdesk staff use domain admin accounts when troubleshooting workstations and servers
- Giving IT admins access to domain admin accounts “just in case”
- Setting up new workstations with cloned images resulting in them having the same local administrator password
- Rotating administrator passwords only every 30-60 days
- Using AD Group Policy to rotate one administrative password used for all machines
- Allowing accounts used by applications to have domain administrator privileges

KEY FINDING: **ATTACKERS USED A PRIVILEGED PATHWAY TO GET TO CRITICAL ASSETS**

For the incidents we studied, the initial foothold was gained by phishing users with a malicious attachment, which then downloaded malware to their workstation. In Windows environments, regardless of the initial intrusion method, there is a well-established privileged pathway that attackers use to expand the scope of their attack, moving from a single compromised workstation towards critical assets containing valuable data.

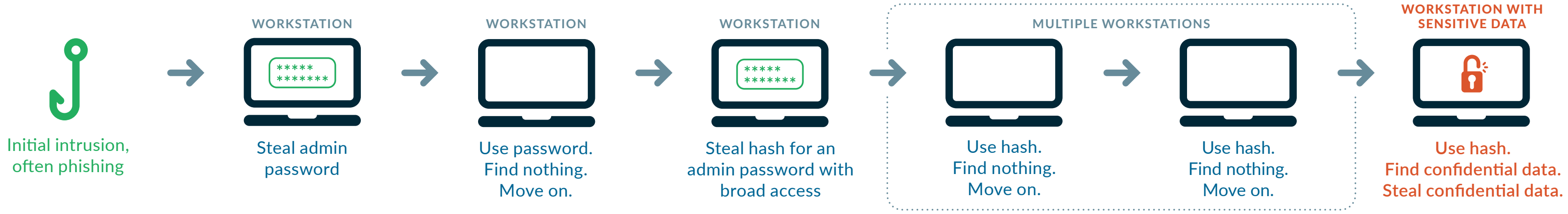
Motives vary. Attackers might be exploring the environment to see what they can find, such as financial data on a sensitive workstation or credit card numbers in a database server. Or they might be more ambitious, aiming to reach the domain controller which would allow them access to all critical assets.

How Attackers Move from Workstation to Workstation

At the first workstation, the attacker might use keystroke logging malware to steal the workstation administrator password. If the same password is used on other machines, the attacker can easily log into another workstation.

Other, more powerful, credential theft techniques do not even require the attacker to see the password and enables them to move very quickly from one machine to another. With the *pass-the-hash* technique, the attacker extracts password hashes which are stored in computer memory for all users who recently logged into that machine – including administrators. Using stolen password hashes, the attacker can *move laterally* to other workstations eventually landing on for example, a sensitive workstation (figure 1).

Figure 1: **To a Workstation with Sensitive Data**


Initial intrusion, often phishing
WORKSTATION
*****
****
Steal admin password
WORKSTATION
Use password. Find nothing. Move on.
WORKSTATION
*****
****
Steal hash for an admin password with broad access
MULTIPLE WORKSTATIONS
Use hash. Find nothing. Move on.
Use hash. Find nothing. Move on.
WORKSTATION WITH SENSITIVE DATA
Use hash. Find confidential data. Steal confidential data.

A specific example of a *pass-the-hash* is: if a helpdesk technician has recently provided assistance on a workstation, the attacker can steal the helpdesk technician's hash from one workstation, then use it to get into other workstations that the helpdesk technician has access to.

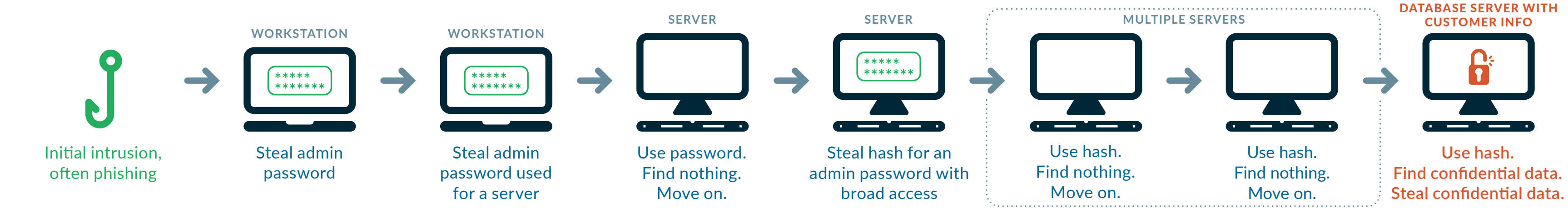
Pass-the-hash is the best-known credential extraction technique. It abuses features of the Kerberos and NTLM authentication protocols that enable transparent authentication. Other variations include stealing Kerberos tickets from a compromised machine to deploy on another machine *(pass-the-ticket)*, or using stolen hashes to create new Kerberos tickets (*overpass-the-hash*).

How Attackers Move to Higher-Value Assets

Using the credential theft techniques described above for moving laterally, an attacker can also escalate their privileges to gain access to higher-value accounts and machines. For instance, an attacker can move from the first workstation to another using a stolen credential. If, at this second workstation, the user uses the same account for administrative access to a server, the attacker can now gain access to that server. The attacker can continue the credential theft process to move from server to server. By finding a hash for a server admin password, they can gain broad access to multiple servers and eventually arrive at a customer database (figure 2).

> The number one thing an adversary does once they get into your network is look for the ability to escalate their privileges. Without good practices, you make it very easy for them to instantaneously traverse your whole network.
>
> —**JIM CONNELLY,**
> VICE PRESIDENT AND CISO,
> LOCKHEED MARTIN

Figure 2: **To a Database with Customer Information**



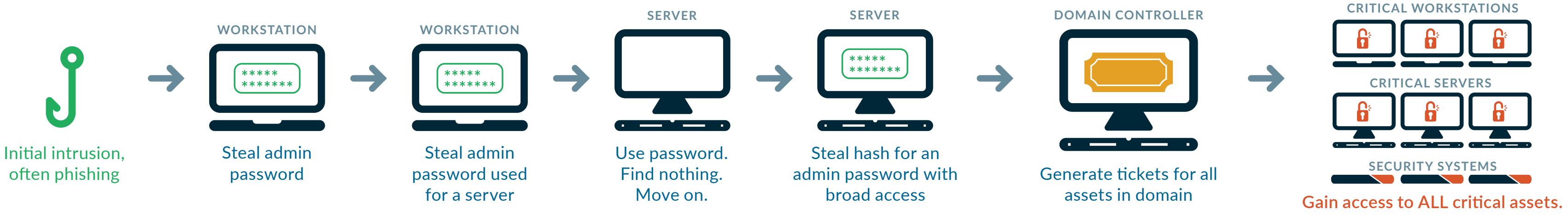
WORKSTATION
WORKSTATION
SERVER
SERVER
MULTIPLE SERVERS
DATABASE SERVER WITH CUSTOMER INFO
*****
****
Initial intrusion, often phishing
Steal admin password
Steal admin password used for a server
Use password. Find nothing. Move on.
Steal hash for an admin password with broad access
Use hash. Find nothing. Move on.
Use hash. Find nothing. Move on.
Use hash. Find confidential data. Steal confidential data.

With the same techniques, an attacker can also move from server to domain controller. Once the domain controller has been compromised, the attacker can potentially pull off a golden ticket attack, whereby the attacker can act as if they were the authentication authority and gain access to all assets in the network, including security systems and non-Windows systems which have been integrated into Active Directory (figure 3).

Common practices that leave organizations wide open to *pass-the-hash* and similar techniques include:

- Permitting users to use accounts with administrative privileges on their own workstations
- Using the same administrator password for all local administrator accounts
- Not consistently enforcing password rotation or uniqueness policies for IT administrator accounts
- Setting up domain administrator accounts to be used to log into to domain controllers as well as servers and workstations
- Allowing administrator accounts to be used for day-to-day tasks such as checking email and browsing the Internet

Figure 3: **To the Domain Controller**


Initial intrusion, often phishing
WORKSTATION
Steal admin password
WORKSTATION
Steal admin password used for a server
SERVER
Use password. Find nothing. Move on.
SERVER
Steal hash for an admin password with broad access
DOMAIN CONTROLLER
Generate tickets for all assets in domain
CRITICAL WORKSTATIONS
CRITICAL SERVERS
SECURITY SYSTEMS
Gain access to ALL critical assets.

Shutting Down the Privileged Pathway

Security teams often focus on implementing controls at the start of the attack route (to prevent phishing) and at the end (to protect critical assets). However, implementing controls to shut down the privileged pathway is key.

Although the workforce is better-trained than ever before, the success rate of phishing is still very high. Research shows employees open phishing messages 30% of the time, and about 13% go on to click the malicious attachment or link*. At the other end of the attack route, security controls around critical assets are undoubtedly important. But by using the privileged pathway, attackers can use non-critical assets to bypass or disable the controls around critical assets.

> “One of the lessons learned has been that if you have pass-the-hash type vulnerabilities on workstations and servers, attackers can use non-critical assets to pivot to a place where they're able to compromise critical assets.”
>
> —**GERRIT LANSING,**
> CHIEF ARCHITECT, CYBERARK

*Verizon 2016 Data Breach Investigations Report

RECOMMENDED PRACTICES

For the incidents where attackers successfully used the privileged pathway to get at critical assets, we asked, *"What practices would have helped to prevent the breach?"* The following practices were identified. These strategies are the underlying foundation for the controls framework (on pages 10–12).

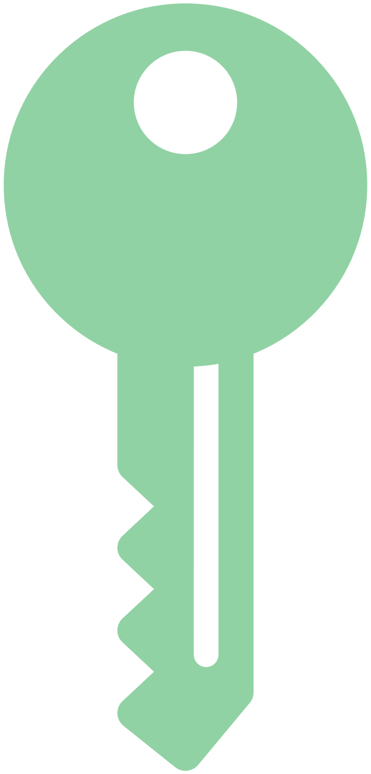
Limit Exposure of Privileged Credentials

It's important to restrict possible points of contact between administrative credentials and attackers. In particular, if malware gets installed on a workstation, ensure it cannot gain local administrator authority, spread to other machines and/or uncover server or domain administrator accounts.

- Create boundaries within your identity structure to enforce segregation of duties:
  - Domain administrator accounts should only be used to manage domain controllers, not servers or workstations
  - Server administrator accounts should only be used to manage servers, not workstations
  - Workstation administrator accounts should only be used to manage workstations
- Use administrator accounts for administrative tasks only, not day-to-day activities
- Provide domain admin accounts only to those who absolutely need them as part of their regular job
- Ensure accounts that are used by applications and services have the least possible privilege:
  - Removing administrator privileges from application accounts may require refactoring the applications; generally applications never need this level of privilege, although they are sometimes written or configured this way for developer convenience
- Do not allow administrative access to sensitive assets from Internet-connected workstations:
  - Use a jump server or a dedicated administrative workstation not connected to the Internet
- Do not provide local workstation administrator rights to employees, such as software developers:
  - Remove their accounts from the local Administrators group and use tools to provide temporary elevated privileges to perform occasional tasks that require administrator rights

Recommended Practices At-a-Glance

- Limit exposure of privileged credentials
- Enforce strong passwords and store them in an encrypted vault
- Minimize the number of administrator accounts
- Increase monitoring for privileged credential theft



Enforce Strong Passwords and Store Them in an Encrypted Vault

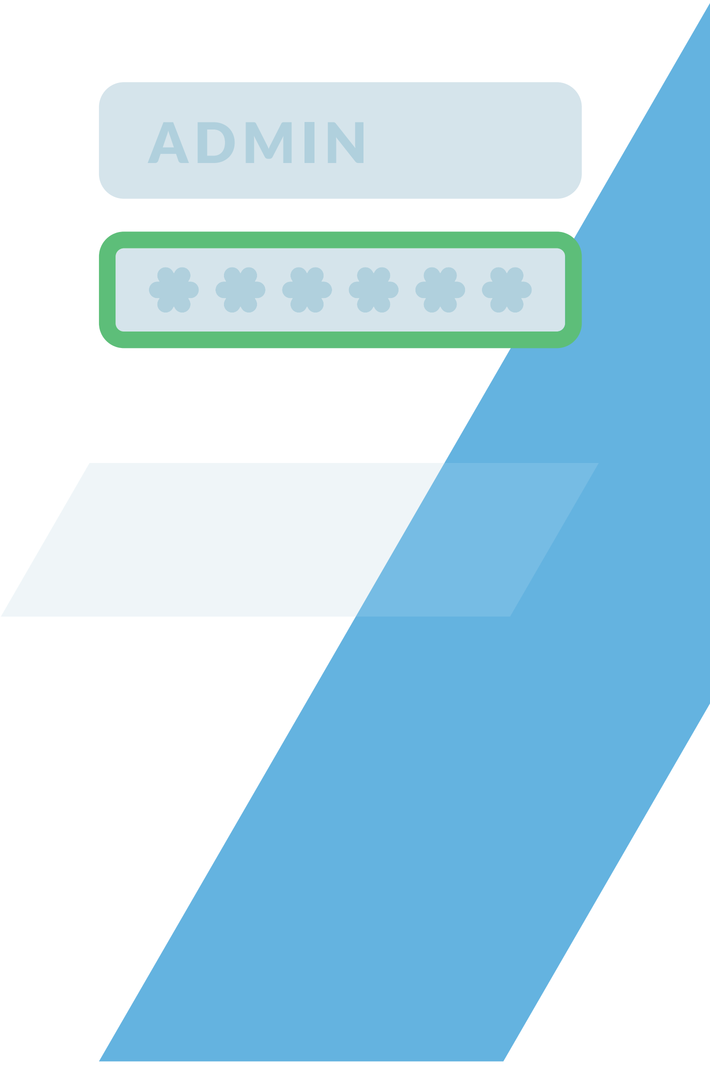
Adhering to these practices helps organizations to ensure attackers can't steal administrative credentials or reuse them on other machines:

- Require unique passwords with stringent criteria for length and complexity
- Frequently rotate passwords, ideally using one-time passwords (or once per day at a minimum)
- Automate password selection and rotation
- Put the passwords in a tamper-proof digital vault that uses encrypted storage
- Require multi-factor authentication when users and applications access the passwords in the vault

Minimize the Number of Administrator Accounts

Ideally, organizations should have the smallest feasible number of privileged accounts to minimize the attack surface and to simplify credential management.

- Avoid setting up individually-assigned privileged accounts for administrators in Active Directory. For example, the following common process is problematic as it leads to account proliferation:
  - An IT helpdesk technician named "Alice" has an account "Alice" for day-to-day work and an "Admin-Alice" account with administrative rights to all workstations
  - A server admin "Bob" has a "Bob" account, and an "Admin-Bob" account with administrative rights to his workstation and servers
  - A domain admin "Charles" has a "Charles" account, and "Admin-Charles" account with administrative rights to his workstation, servers, and the domain controller
- Use the built-in local administrator account that already exists for each workstation and server:
  - These accounts can be shared while preserving individual accountability: Vault the credentials and require the admins to check them out from the vault as needed. Their privileged activities can be controlled and monitored. (The Admin-Alice, Admin-Bob, and Admin-Charles accounts above should be deleted.)
  - Although many administrative tasks can be performed using built-in accounts, there still may be a need to set up personal administrator accounts, but keep them to a minimum



Increase Monitoring for Privileged Credential Theft

The following practices help detect attacks that hijack privileged credentials:

- Implement real-time privileged session monitoring, i.e. administrative access
- Use detection tools that look for patterns indicative of credential theft techniques
  - Especially for domain controllers, use detection tools that specifically look for patterns indicative of attacks on the Kerberos authentication system
- Use analytics tuned to detect credential-use anomalies as they occur, such as an attempt to use a credential outside of a user's authorized working hours

THE 30-DAY SPRINT FRAMEWORK

This is a framework for a fast-tracked initiative to help shut down the privileged pathway in Windows environments. It aims to ensure that when an attacker compromises a workstation, they will find it very difficult to move any further and if they do, it will be detected.

The intent is to work at an accelerated pace to implement critical controls in a short period of time, such as 30 days. This has been achieved by organizations by adopting a sprint mindset (see sidebar). The actual amount of time needed for a sprint will vary depending on the organization's size, complexity, maturity, and culture.

Although the framework focuses on specific controls around Windows administrative accounts to protect Windows environments, organizations should, in parallel, implement other critical controls such as patching the operating system, patching applications, and application whitelisting.

Recommended Controls

The following table outlines the set of recommended controls, indicating what controls to implement first and what to do after you've gotten the first set of controls in place.

Prioritization

The suggested prioritization is based on endeavoring to:

- **Identify accounts quickly** – Locate the administrative accounts in Windows
  - For a fast-tracked initiative, the idea is not to spend a lot of time on upfront analysis as the accounts are relatively easy to identify within Active Directory (AD) and local Administrator Groups.
- **Give precedence to the riskiest accounts** – Implement controls on the most powerful accounts first
  - Domain administrator accounts and administrator accounts with access to large numbers of machines, particularly servers, as well as application accounts that use domain administrator privileges.
- **Be realistic about addressing the volume of accounts** – Work quickly to get some controls in place and make improvements over time
  - For example, ideally accounts for workstation users should not have administrative privileges, but breach survivors say this is one of the more difficult practices to implement and maintain due to the sheer volume of workstations.

The Sprint Mindset

How quickly can a new set of security controls be deployed across an enterprise? It depends on the organization's sense of urgency. In the aftermath of a breach, the organization becomes internally aligned, decision-making speeds up, immediate results take priority over bureaucracy, and tremendous progress in security becomes possible in a short timeframe.

Inevitably, all breach survivors wish that they had made that spurt of progress in time to have prevented the damage, which is the purpose of the proactive 30-day sprint.

> Even if CISOs aren't able to put all of the controls in place in 30 days – the intent is obvious. You have to prioritize. The framework breaks it down – 'Start here. Do these things first.' It's absolutely valid whether it's 30, 60, or 180 days.
>
> —**STEVE GLYNN,** CISO, ANZ BANKING GROUP LIMITED

THE 30-DAY SPRINT FRAMEWORK

Recommended Controls	FIRST: Tackle these accounts first *Aim to implement the controls for these accounts within a short period of time such as 30-days.*	NEXT: Tackle these accounts next *Depending on the organization, these controls may need more time.*
• Reconfigure accounts to segregate duties	Domain Administrator Accounts *(Used only to log into domain controllers)* Server Administrator Accounts *(Used only to log into servers)* Workstation Administrator Accounts *(Used only to log into workstations)*	
• Put admin passwords in a vault – Automate password selection and rotation (i.e. one-time passwords) – Monitor password usage	Domain Administrator Accounts Server Administrator Accounts	Workstation Local Administrator Accounts
• Require multi-factor authentication to access passwords in the vault	All accounts for which the passwords have been vaulted *As passwords are vaulted, organizations will continue to implement MFA over time.*	→
• Randomize passwords for administrative accounts to make them unique	Workstation Local Administrator Accounts	
• Do not allow administrative access to sensitive assets from Internet-connected workstations – Use a jump server or a dedicated admin workstation not connected to Internet • Limit use of admin accounts to admin tasks only – Not day-to-day activities	Domain Administrator Accounts Server Administrator Accounts Workstation Administrator Accounts	
• Minimize the use of individually- assigned administrative accounts (which leads to account proliferation) – Instead have administrators use built-in accounts and access the passwords via a vault (see page 9 for more details)	Domain Administrator Accounts Server Administrator Accounts *For some organizations, it may not be feasible to remove individually-assigned administrator accounts in the short term. An initial approach is to vault the passwords for the individually-assigned administrator accounts, then over time move from using individually-assigned accounts to the built-in accounts.*	Workstation Administrator Accounts

Continued on next page

THE 30-DAY SPRINT FRAMEWORK

Continued from previous page

Recommended Controls	**FIRST: Tackle these accounts first** *Aim to implement the controls for these accounts within a short period of time such as 30-days.*	**NEXT: Tackle these accounts next** *Depending on the organization, these controls may need more time.*
• Remove workstation administrator privileges from end users – Provide temporary elevation of privilege when required		Workstation Local Administrator Accounts *End-user accounts should be removed from the local Administrators group. If users need to perform tasks on their workstations which require administrator privileges, provide temporary elevation of privilege to perform specific activities only.*
• Implement detection tools to look for signs of lateral movement or privilege escalation in real time	Domain Administrator Accounts Server Administrator Accounts Workstation Administrator Accounts	
• If any applications use domain administrator privileges, such as domain rights to multiple servers, remove those privileges	Application Accounts *For some organizations, it might not be feasible to address all of these applications within the short term and work to reconfigure or rewrite applications will continue over time*	→

Notes to the table:

- Domain Administrator Accounts: Accounts in AD used to manage domains and domain controllers
  - E.g. Enterprise Admins and Domain Admins
- Server Administrator Accounts: Accounts in AD used to manage servers
  - E.g. Accounts used by data center personnel to maintain multiple servers
- Workstation Administrator Accounts: Accounts in AD used to manage large numbers of workstations
  - E.g. Accounts used by Help Desk and personnel to provide technical support
- Workstation Local Administrator Accounts: Accounts in the local Administrators group on each workstation
  - E.g. Accounts used to perform admin activities on individual workstations
- Application Accounts: Non-user accounts used by applications to run systems or processes
  - E.g. Accounts used to perform backups or software installation

BEFORE THE SPRINT

By the start of the sprint, you will need to have selected technologies for password vaulting, multi-factor authentication, and detection, and put a team in place. A small team can put controls around the most important privileged accounts quite quickly: In one case, in the aftermath of a breach, a team of just eight members working with a security consultant vaulted the administrator accounts for 20 domains and 6,500 servers in four weeks. Compared with implementing controls in a hostile, post-breach environment, doing the work proactively is likely to proceed relatively smoothly.

AFTER THE SPRINT

Typically, organizations emerge from a sprint with a to-do list comprising the threads below.

Add Controls to More Accounts: For coverage beyond Windows accounts, understand the scope of all privileged accounts. Privileged accounts exist for a wide range of technologies such as Oracle databases, Unix and Apple computers, NAS and SAN storage devices, any device with an IP address, hypervisors and operating services in virtualized environments, and cloud services.

Increase the Depth of Controls: Look at enhancing controls to monitor account usage. For the most sensitive accounts, for example, add video recording of privileged sessions or user behavior analytics.

Continue to Refactor Applications: Applications, especially legacy ones, are often designed to require administrator privileges and have passwords embedded in ways that make password rotation difficult. Ensure in general, all applications are granted the minimum necessary privileges and use passwords securely. To address these issues usually requires reconfiguring or rewriting applications. This includes not only homegrown but also third-party applications. In some cases, organizations will have to work with vendors to make changes.

Formalize the Program: Establish processes for maintaining and supporting the new controls, looking at questions such as “What are the processes for adding new assets to the system and de-provisioning obsolete ones?” Ensure that processes can keep up with changes in the business and regularly validate that security and business goals are being met.

CISOs and their security teams can use the momentum from the sprint to transition into a more comprehensive enterprise program, which can be a multi-year effort. The CISO View report entitled ***The Balancing Act: The CISO View on Improving Privileged Access Controls*** offers peer advice in three key areas:

- The **strategic decisions** that CISOs and their teams will need to make
- The **conversations** CISOs need to drive across the organization
- The **essential components** of a successful program

> Putting security controls in place in the middle of a cyber-attack is like putting storm windows on your house in the middle of a hurricane. It’s a lot easier to implement the controls to protect high-risk privileged credentials now than to recover from a breach later.
>
> —**JOHN GELINNE,** MANAGING DIRECTOR,
> ADVISORY CYBER RISK SERVICES,
> DELOITTE & TOUCHE

Measuring Progress

Examples of useful metrics:

- Use penetration testing to measure the amount of time attackers take to compromise high-value accounts before and after implementation of controls
- Scan the network with automated tools that identify accounts needing better protection. After the implementation of controls, scan the network again to show the reduction in vulnerable accounts.

CONCLUSION

Attackers have honed the use of the privileged pathway in Windows to reach critical assets and steal sensitive data. Without adequate controls to protect administrative accounts, organizations leave themselves exposed. The sprint framework provides a fast-tracked initiative to implement a set of controls to shut down the privileged pathway.

To be successful, the security team will need to gain support across the organization. Convincing IT admins will be crucial. They may resist workflow changes or having privileges reduced. However better security controls not only protects the organization but also them personally. If an incident occurs where an attacker takes control a privileged account, the admins can be quickly cleared of wrongdoing. The chapter on "Four Pivotal Conversations" in the CISO View report, *The Balancing Act*, offers more advice on persuasion and handling objections.

Another key group to win over is leadership. They will need to help set organizational priorities and create a sense of urgency. For guidance on communicating with the executive leadership and/or Board, see the FAQ in the Appendix that follows.

To access other CISO View reports, visit www.cyberark.com/cisoview

> Behave as if you've just been breached. If you had, you'd be forced to figure it out. The mindset changes from 'It's too hard. We can't do it,' to 'We must do it!' There's now an imperative.
>
> —GUEST CONTRIBUTOR

APPENDIX 1: **FAQ FOR EXECUTIVE LEADERSHIP AND BOARD OF DIRECTORS**

This FAQ is intended to help executives and the Board understand the risks and mitigation plan.

1. Why do we need an intensive effort to protect privileged credentials?

Without adequate protection, we are at risk of a data breach similar to the major attacks that have been featured in the news, affecting many large organizations. In these cases, attackers used techniques that exploited vulnerabilities in the Windows environment to steal privileged credentials and move around the network without detection in order to gain full control of the organization's information systems.

The risk of these attacks is increasing. Attackers have access to widely-available toolkits that enable them to easily create tailored to conduct attacks. Microsoft itself recommends putting in place better controls to reduce the risk.

Based on research that analyzed these major data breaches, we know what improvements to our security controls are needed. During an intensive effort of approximately 30-days, we will put in place controls that make it much more difficult for attackers to carry out these types of attacks against us.

2. Why are privileged credentials a priority compared to other security goals?

Privileged credentials give adversaries very high-levels of access to information systems. Typically, they are passwords used by employees such as IT administrators to operate and manage computing resources across the enterprise.

With privileged credentials, an attacker can access intellectual property, business secrets, and customer information. The attacker can also deactivate any security technologies, such as data encryption, firewalls, and detection systems, which the organization has put in place.

3. What techniques are attackers using to steal privileged credentials?

A well-known first step in most of these attacks is phishing. Users are tricked into clicking on a link or opening an attachment in an email, which downloads malware to their workstation. Studies show, despite major efforts such as anti-phishing training for users, global success rates for phishing have actually increased.

Once the malware is downloaded onto a workstation, attackers gain entry to the Windows environment and can take advantage of the way that Windows machines store credentials. Windows stores password "hashes" (i.e. fixed-length encodings of passwords) in computer memory for all users that have recently logged into that machine. By stealing the hash for an administrative password, an attacker can get access to multiple machines. They search each machine's memory for other password hashes that, in turn, provide access to more valuable machines like database servers or, the biggest prize, the domain controller used to manage access to all computing resources. Once they reach the domain controller, they can create "tickets" to log into any critical asset on the network, shut down security systems, and take full control of information systems.

4. How will you increase protection of privileged credentials?

Our strategy is to implement controls such as:

- Automated selection and rotation of unique and complex passwords for all admin accounts
  - Limits the attackers' ability to compromise multiple machines if they learn one password
- Segregation of accounts used to manage domain controllers, servers and workstations
  - Reduces ability of attackers to use a stolen credential across different types of machines
- Use of a password vault which automatically enforces password policies and enables monitoring of administrative activities to detect credential theft
  - The digital vault is tamper-proof and uses military-grade encryption to store passwords
- Use of a two-factor authentication for authorized users to access credentials in the vault

This strategy is in line with Microsoft's recommendations for preventing credential theft in enterprise Windows environments.

5. How does this initiative compare with what other organizations are doing?

Many organizations affected by cyber-attacks in the past 24 months have focused on implementing better protections around privileged credentials as part of their remediation efforts. At the same time, other organizations worldwide have improved security controls around privileged credentials proactively (as opposed to after a breach). A group of Global 1000 CISOs has published guidelines for developing a comprehensive program to improve privileged access controls, including ING Bank, CIBC, Rockwell Automation, Lockheed Martin, Starbucks, ANZ Bank, CSX, Monsanto, Carlson Wagonlit Travel, News Corp, and McKesson. See ***The Balancing Act: The CISO View on Improving Privileged Access Controls.***

6. What do you need from corporate leadership to make this initiative successful?

By setting the right tone from the top, you can help ensure that we can quickly and successfully deploy a new set of security controls across the enterprise. Although security will drive the project, the affected systems are owned by the business. It will require cross-functional support.

Adopting a "sprint mindset" is one of the most important factors in being able to achieve rapid risk reduction. We are trying to achieve the same sense of urgency and progress as is often done in the wake of actual breaches—without the overarching pressure of resolving a breach. Some will balk at the changes that must be made—such as giving up access rights or following new processes. Direction from leadership is crucial to move ahead rapidly.

APPENDIX 2: **BIOGRAPHIES OF CISO VIEW PANELISTS**

The CISO View Panel – Top Security Executives from Global 1000 Companies

Rob Bening

Chief Information Security Officer, ING Bank

Rob Bening is CISO of ING Bank. He was previously Chief Architect Technology and Group Chief Technology Officer, responsible for developing Group IT standards and several global standardisation programs. His last assignment was setting up the architecture function within Operations and IT Banking, leading architecture and engineering teams in Infrastructure. Since 1985, Rob has held several positions in HR, Audit, Security, Infrastructure and Architecture at ING.

David Bruyea

Senior Vice President and Chief Information Security Officer, CIBC

David Bruyea is responsible for CIBC's information security intelligence, strategy, policy, standards, risk assessment, architecture and program management. From an enterprise architecture perspective, his mandate includes providing technology vision and leadership in the definition and implementation of IT related initiatives. With over 25+ years' experience, David has also held various technical, consulting and management positions at CIBC in the Technology and Operations Division.

Dawn Cappelli

Vice President and Chief Information Security Officer,
Rockwell Automation

Dawn Cappelli leads the global information security program to ensure Rockwell's products and infrastructure are secure. Her team uses a risk-based approach to execute their information security strategy, working closely with business units, IT, and functional leaders. Previously, Dawn was Founder and Director of the CERT Insider Threat Center at Carnegie Mellon and co-authored The CERT Guide to Insider Threats. She also developed software at Westinghouse. Dawn is on the RSA Conference Program Committee and Domestic Security Alliance Council (DSAC).

Jim Connelly

Vice President and Chief Information Security Officer,
Lockheed Martin

Jim Connelly is responsible for overall information security strategy, policy, security engineering, operations, and cyber threat detection and response for Lockheed's global computing environment. With 25+ years of experience, he oversees Lockheed's Intelligence Driven Defense operations and leads an industry-recognized team of cyber security professionals that manage the company's end-to-end security infrastructure, defend against APTs, and enable open collaboration and information sharing with Lockheed's partners.

Dave Estlick, CISSP, CSSLP, CISA, CISM, CIPP

Senior Vice President and Chief Information Security Officer,
Starbucks

Dave Estlick leads information protection and global cyber security including operations, engineering, architecture, identity and access management, as well as IT risk and compliance. Previously, Dave led Starbucks global technology infrastructure. He was responsible for strategy and execution in technology standardization, infrastructure convergence and the establishment of the Starbucks private cloud. Prior to Starbucks, Dave held security leadership positions at PetSmart and Amazon, led infrastructure services for ePods and Icebox, and held key technical roles at both Sun Microsystems and Boeing.

Steve Glynn

Chief Information Security Officer, ANZ Banking Group Limited

Steve Glynn leads the Information Security and Technology Assurance functions at ANZ. He is accountable for the delivery of the information security strategy built around people, enablement, trust and community to ensure ANZ is protected against evolving cyber threats across 34 markets globally. Steve has almost 20 years of experience. Prior to ANZ, he held a number of senior Information Security, Technology Risk and Technology leadership roles for ABN AMRO and the Royal Bank of Scotland in Australia and Singapore.

The CISO View Panel – Top Security Executives from Global 1000 Companies (CONTINUED)

Mark Grant, PhD, CIPP

Chief Information Security Officer, CSX Corporation

Mark Grant protects the confidentiality, integrity and availability of CSX's information resources. His responsibilities include cybersecurity, access control, corporate disaster recovery and progressing the enterprise architecture role and vision across the IT environment. He is a member of the Rail Information Security Committee and participates in numerous security working groups. Since joining CSX, Mark has held key positions responsible for the planning, delivery and reliability of IT services.

Gary Harbison

Chief Information Security Officer, Monsanto Company

Gary Harbison leads the Information Security Office focused on managing Monsanto's risks and cyber threats globally, and enabling the business with pragmatic security solutions. His prior roles focused in the information security domain including technical, architecture, strategy and leadership roles at multiple Global Fortune 500 companies and the Department of Defense. Gary is an Adjunct Professor in the Cybersecurity Master's Program at Washington University.

Kathy Orner

Vice President and Chief Information Security Officer, Carlson Wagonlit Travel

Kathy Orner has global responsibilities for information security governance, risk and compliance; security operations and engineering; physical security; and IT compliance and audit. Previously, she was VP of Enterprise Services and CISO for Carlson. Her extensive IT leadership experience includes CISO roles at United Health Group and Blue Cross Blue Shield of Minnesota. She currently serves on the Payment Card Industry (PCI) Organization Board of Advisors.

Chun Meng Tee

Vice President and Head of Information Security, Singapore Exchange

As the Head of InfoSec for SGX, Chun Meng Tee has the functional and operational responsibilities for the Exchange's information security program. Prior to SGX, Chun Meng consulted for financial institutions and government agencies with the Ernst and Young information security practice. He also served in Information Security roles in the public sector for the Ministry of Defense and the Singapore Police Force where he was the Head of the Information Security function.

Munawar Valiji

Head of Information Security, News UK

Munawar Valiji is the News Corp Regional CISO responsible for the security strategy for News UK, Dow Jones, Wall Street Journal and Harpercollins Publishers in the UK and EMEA including designing, building, and maintaining highly secure and easily maintainable security platforms. Previously, he was Head of Information Security for Financial Times. Munawar's extensive experience in information security includes consulting, technical and senior management roles at Morse Computers, Deloitte, Citi Bank, JPMorgan Chase, National Australia Bank and Sun Microsystems.

Mike Wilson

Senior Vice President and Chief Information Security Officer, McKesson

Mike Wilson leads security and IT risk management. His IT and risk management experience spans across several geographies and industries, including financial services, healthcare and consumer products and distribution. Prior to McKesson, Mike worked for a global professional services organization. Mike supports thought leadership and industry organizations including NH-ISAC, Cloud Security Alliance, and CSO Bay Area Council.

BIOGRAPHIES OF GUEST CONTRIBUTORS

Technical Experts and Consultants Who Have Worked with Major Organizations Post-Breach

John Gelinne
Managing Director, Advisory Cyber Risk Services,
Deloitte & Touche

John Gelinne is a part of Deloitte's Resilient practice that helps organizations prepare for, respond to, and recover from cyber incidents. His responsibilities include cyber war gaming and building technical resilience enabling organizations to rapidly adapt and respond to dynamic changes, disruptions, or threats. John retired from the U.S. Navy after 30 years; he played a pivotal role defending the Navy's network against advanced cyber threats. He holds advanced degrees in Info Systems Management and National Security and an undergraduate degree in Engineering.

Gerrit Lansing, CISSP
Chief Architect, CyberArk

Gerrit Lansing recently assumed the role of Chief Architect at CyberArk. Previously he led CyberArk's consulting services, including strategic guidance, architecture, and large project services teams. Gerrit has advised many of the world's largest companies, including several Fortune 10. He brings expertise in designing security controls and working with organizations in the wake of large data breaches. Prior to CyberArk, Gerrit was an information security analyst at a large insurance company where his responsibilities included systems security, forensics, incident response, and investigations.

Security Executives from Major Organizations That Have Experienced Large Data Breaches

Due to legal constraints, these executives have contributed to this research report without attribution.

ABOUT THE CISO VIEW INDUSTRY INITIATIVE

Sharing information on good security practices is more important than ever as organizations face increasingly sophisticated cyber threats. 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 privileged account 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.