THE **CISO VIEW**

AN INDUSTRY INITIATIVE
SPONSORED BY **CYBERARK**

EXECUTIVE SUMMARY

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

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

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. 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

> 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

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

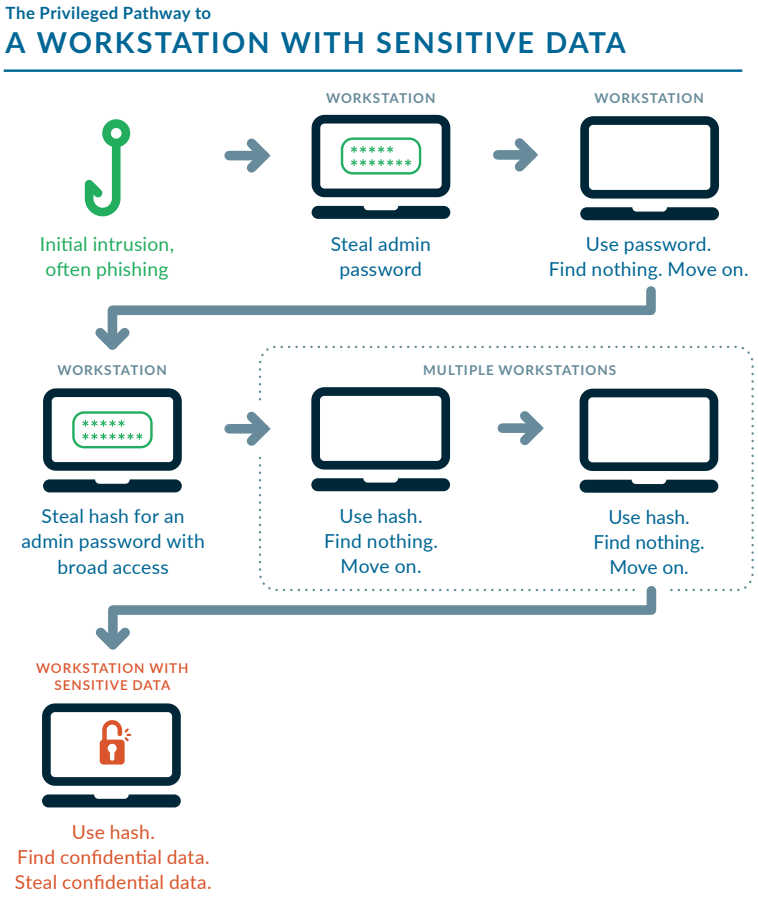
> The number one thing adversaries do once they get into your network is look for the ability to escalate their privileges. Without good practices, you make it very easy for them to instantaneously traverse your whole network.
>
> —**JIM CONNELLY**, VICE PRESIDENT AND CISO, LOCKHEED MARTIN

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

Privileged credentials have long been prone to compromise. However, recently 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.

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.



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.

Recommended Controls

Prioritizing recommended controls starts with three key steps to:

- ***Identify accounts quickly.*** Locate the administrative accounts in Windows.
  - For a fast-tracked initiative, the idea is not to spend time 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.

To access the full report, go to:
www.cyberark.com/cisoview →

The Sprint Mindset

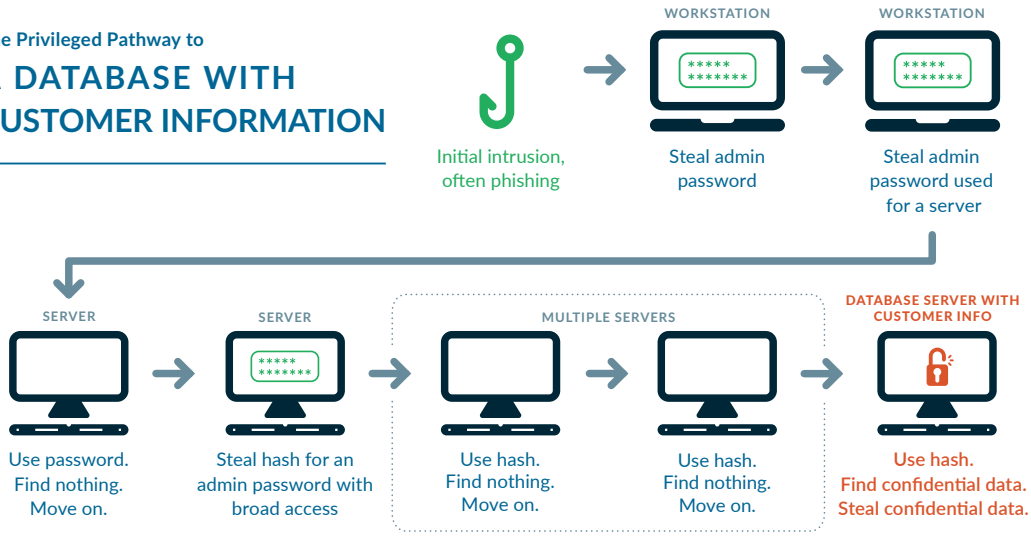
How quickly can a new set of security controls be deployed across an enterprise? It depends on the organization's sense of urgency. In the aftermath of a breach, the organization becomes internally aligned, decision-making speeds up, immediate results take priority over bureaucracy, and tremendous progress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

> 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

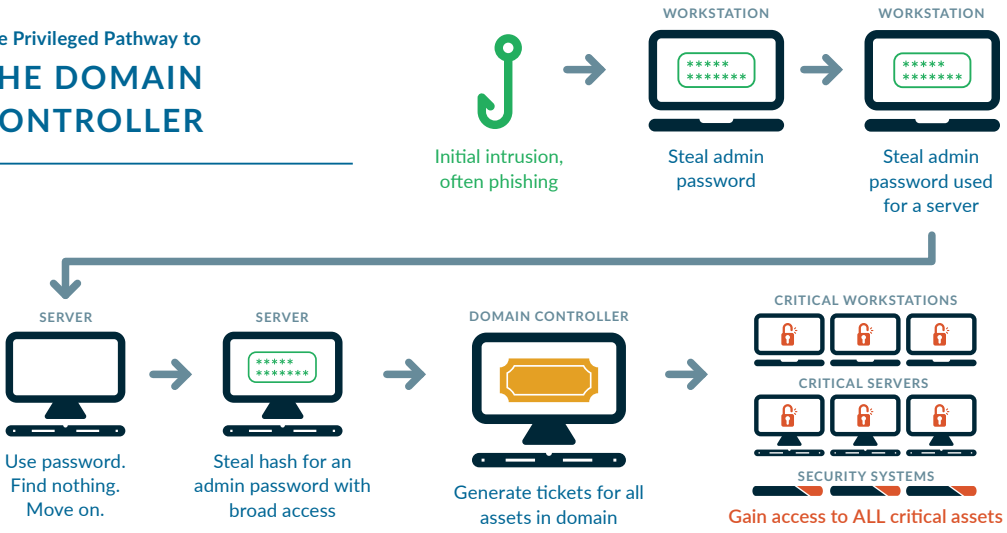
The Privileged Pathway to

A DATABASE WITH CUSTOMER INFORMATION



The Privileged Pathway to

THE DOMAIN CONTROLLER



ABOUT THE CISO VIEW INDUSTRY INITIATIVE

CyberArk has commissioned an independent research firm, Robinson Insight, to facilitate an industry initiative to explore CISO views on topics related to improving privileged access controls. The initiative brings together top CISOs who share their insights into critical issues facing practitioners today. By developing CISO reports, studies and roundtables, the initiative generates valuable peer-to-peer guidance and dialogue.

CyberArk (NASDAQ: CYBR) is a global company providing privileged account security solutions. For more information on CyberArk, go to www.cyberark.com.

To access the full report, go to: www.cyberark.com/cisoview →

CYBERARK