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

Rob Bening
Chief Information Security Officer, ING Bank

David Bruyea
SVP and CISO, Enterprise Architecture and Information Security, CIBC

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

Dave Estlick
Information Security Chief, Starbucks

Steve Glynn
Global Head of Information Security, ANZ

Mark Grant
Chief Information Security Officer, CSX Corporation

Gary Harbison
Chief Information Security Officer, Monsanto Company

Jim Motes
Vice President and Chief Information Security Officer, Rockwell Automation

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

John Schramm
Vice President Global Information Risk Management & CIRO, Manulife

Munawar Valiji
Head of Information Security, News UK

Mike Wilson
Vice President & Chief Information Security Officer, McKesson

→
LEARN MORE about the contributors

THE **CISO VIEW**

AN INDUSTRY INITIATIVE SPONSORED BY **CYBERARK**

The Balancing Act:
The CISO View on Improving Privileged Access Controls

THE BALANCING ACT: OVERVIEW

There is a growing realization that preventing the theft of highly privileged credentials could short-circuit the majority of today's sophisticated cyber-attacks. The rise of advanced threats is prompting organizations to rethink privileged access controls.

This report provides practical guidance for CISOs based on the first-hand knowledge of leading organizations. Recommendations are based on interviews with an esteemed panel of top information security executives from Global 1000 organizations in various industries.

Implementing better privileged account security at a small scale can be a relatively straightforward task. However a comprehensive program at a large enterprise involves driving many aspects of people, process and technology.

Having already tackled many improvements, the panelists offer insights on how to approach the challenges that organizations typically face. They also provide nuanced recommendations for achieving the balance between enabling and restricting high-levels of access to information assets.

Achieving this balance is crucial. In fact, recent research indicates that overly restrictive access to information represents a growing strategic risk. The study estimates that, "one-size-fits-all risk approaches can cost an average Fortune 500 company more than $20 million a year, in particular by slowing employee productivity, hampering innovation, and derailing major business projects."[1]

Improving privileged access controls is of course an on-going journey, just like improving security controls in general. Based on the combined experience of the panelists, each chapter explores and summarizes a range of views, along with areas of consensus, on what works and what doesn't.

[1] Corporate Executive Board, February 2015

A Word From Our Sponsor

This report is part of the CISO View, an industry initiative sponsored by CyberArk. The report was 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 are helping the larger community address this issue.

TABLE OF CONTENTS

CHAPTER 1

Three Strategic Decisions

INTRODUCTION

A growing concern for most Chief Information Security Officers (CISOs) today is the potential for compromised privileged credentials. In the current threat environment, cyber adversaries and rogue insiders increasingly go after privileged credentials as a way to gain broad and undetected access to information systems.

Therefore many organizations are proactively shoring up privileged access controls to mitigate the risks. This chapter captures the know-how of an expert panel of highly accomplished Global 1000 CISOs and offers peer-to-peer guidance for CISOs who are building comprehensive programs to improve privileged access controls. It focuses on making the core decisions that will power your strategy and address security versus business tradeoffs. In discussions with panelists, three key decision areas emerged:

What should we do when? With a large number of privileged accounts across an organization, how do you determine the order of priority? What's the best time to make various improvements?

What's the best mix of controls? What are specific examples of more advanced preventive and detective controls around privileged access? How do you combine them to achieve business and security goals?

How much is enough? Controls should provide better security without encumbering business processes. Where is the fine line between "sufficiently secure" and "overly restrictive?"

Improving privileged access controls

This involves moving towards more centralized and automated methods, including:

- Stronger cryptographic storage of privileged credentials
- Enhanced accountability for the use of shared accounts
- Systematic enforcement of policy
- Real-time detection of unauthorized activity
- More detailed audit trails

1. WHAT SHOULD WE DO WHEN?

Setting Priorities and Timing

Large enterprises often have tens or hundreds of thousands of privileged accounts across the organization. For an initiative to improve the controls around these accounts, some CISOs set a goal from the start of deploying a comprehensive program. Others begin with a more exploratory approach. They quickly identify a small set of accounts, move them to a more centralized and automated system and gradually expand their ambitions towards more comprehensive coverage.

With either approach, you'll need to prioritize what accounts require better protection and to be aware of opportune times to make changes. As the deployment of better controls progresses, priorities and opportunities need to be regularly re-evaluated.

A focus on privileged accounts must, of course, be done within the context of your overall security strategy and weighed against other goals. When considering these control improvements versus other goals, remember that if privileged credentials are not properly secured, other controls meant to protect the infrastructure could be rendered ineffective, since privileged credentials can be used to turn off or circumvent other controls.

Determine what accounts are potentially in scope

Organizations typically look at improving security for accounts in four general categories: administrative accounts, privileged end user accounts, accounts that are embedded in applications and scripts, and privileged accounts used by third parties.

To identify candidates for improvements, some organizations start by taking a full inventory of all the privileged accounts and establishing ownership for them. This can help to raise consciousness and put a focus on the problem of under-controlled privilege.

Evaluate risks

Determining an order of priority obviously requires identifying which accounts represent the biggest risks. Focus on accounts that provide elevated access to the organization's most critical systems – the highest-value assets and/or sensitive data with regulatory and contractual obligations to protect it. Examples are systems that contain intellectual property or customer account information. The security team will need to work with the business to identify the most critical systems. In many organizations, you will be able to leverage previous work that has been done to identify the organization's "crown jewels."

Also consider how vulnerable the systems are to attacks. Penetration testing can be extremely useful in indicating where the biggest risks are. It could show, for instance, how quickly attackers might be able

Addressing Credential Proliferation

Processes to periodically review privileges across a large organization may not be applied consistently over time. It is common to find an accumulation of accounts and access to credentials that are no longer necessary.

There are two main approaches to credential proliferation: One is to preemptively tackle it by decommissioning accounts in the earliest stages of the initiative. The other is to implement better controls on the identified accounts and use the enhanced audit trail as data to inform subsequent reviews of accounts. Better audit data can substantiate the need to retire accounts.

> For implementing changes to privileged access controls, the real trick, as with many other security initiatives, is prioritization. Classification and risk-rating mechanisms allow you to address the highest risk systems first and make progress over time.

—DAVID BRUYEA
Senior Vice President and Chief Information Security Officer, Enterprise Architecture and Information Security, CIBC

to access different types of privileged accounts, or illustrate the damage that an attacker with particular credentials could do. For example, in an environment with single sign-on, a domain admin account might be able to access the ERP system, confidential customer data and fileshares that hold strategy documents.

Prioritization — Examples of risk factors to consider

Type of Account	Risk Factors
Administrative accounts used by IT and system administrators and developers	Accounts with high-levels of access used to manage and maintain information systems are often prioritized such as: • "Superuser" or Domain Admin accounts (e.g. Windows admin or Unix root accounts) • Administrator accounts for networks, databases, applications, cloud services, and virtual environments and so on These are often considered some of highest-risk accounts given their broad access rights and ability to turn off other controls. They are usually generic or shared accounts, which can create a lack of accountability. Besides server admin accounts, workstation admin accounts are often in scope but may or may not be a top priority. It depends, for example, on whether they are segregated from sensitive data.
Privileged end-user accounts	Accounts used by specialized users who need access to sensitive data might also be a focus for improved controls such as: • Accounts used by top-level executives • Accounts used to access financial records, bank accounts, and employee and customer records • Accounts involved in highly confidential projects
Privileged accounts used by applications, processes, and scripts	Applications that use embedded credentials can be attractive targets for adversaries. Often applications use highest-level privileges because it's easiest in terms of application design, but this means these accounts can have extensive access to sensitive data. Dealing with credentials used by applications can be one of most challenging aspects of securing privileged accounts, since it often involves refactoring applications. Depending on the maturity of the organization's software development lifecycle program, newer applications may have better controls than legacy ones. Also consider the longevity of the application and prioritize accordingly.
Third-party privileged accounts	Higher-risk third party accounts might include accounts used for: • Consultants or contract workers • Outsourced IT, finance or development services • Vendor-supported IT infrastructure (e.g. storage systems) or building systems (HVAC) Third-parties may have policies and practices for credential management that are less stringent than yours. A common risk is the failure of third-parties to inform your organization if there are changes to their personnel.

Be opportunistic

In general, the order of priority is based on risk, addressing the higher-risk accounts first. However, in the very early stages of the initiative, some CISOs will start with accounts in less critical systems and use it as a learning experience to build confidence and maturity with the new control model. Then they move towards addressing more critical accounts later in the initiative.

Control improvements should also be timed to take advantage of opportunities related to other business goals. The optimal time to make changes is when you can enable a business initiative or when stakeholders will be more open to changes.

Timing — Examples of opportunities to consider

When this happens...	Take the opportunity to...
Process improvement initiative	Ride a business initiative to improve a process. Use it as context for integrating better security controls. For example, an overall IT process improvement initiative could be a great time to integrate controls which streamline workflows for review and approval of privileged access.
Business unit finishes wrapping up a major project	Work with that business unit on their privileged access controls. Take advantage of the fact that staff are less distracted by deadlines, and they have more bandwidth to discuss security issues and solutions.
Application development team planning a new version	Discuss ways to incorporate requirements for better management of privileged credentials into the next release of the application. The development team will be more amenable to making security-related changes when there already are plans for a future release rather than devoting a release entirely to security issues.
Strategic sourcing initiative	Make it a requirement that there be robust privileged access controls to manage third party access when partnering with a new outsourced service provider. Position the controls as way to enable the company to achieve costs savings by using a new sourcing strategy without significantly increasing information security risks.
Surge in demand for IT services, that leads to engaging many IT contract workers	Improve controls around privileged accounts that contract workers use. Automating the deletion of access to privileged credentials can help to mitigate the inherent risk of high turnover for contract workers. Often it is difficult to keep pace with the changes if they are done manually.

2. WHAT'S THE BEST MIX OF CONTROLS?

Formulating a Controls Strategy

As with addressing security risks in general, reducing the risks around privileged accounts requires a layering of preventive and detective controls. Preventive controls can help to stop unauthorized activity. Detective controls can help to discover it when it occurs, either maliciously or by mistake, before any significant damage occurs and/or provide an audit trail and accountability.

Take a layered approach

For example, a layering of controls for administrative accounts with broad access to critical systems might look like this:

Preventive	• Store shared credentials in a tamper-proof digital vault • Create accountability by linking the use of shared credentials to unique user IDs • Automatically generate passwords and change them after every use
Detective	• Monitor and record all privileged sessions • Baseline user behavior and use analytics to spot anomalous use of credentials

To manage the risks of an outsourced service provider with administrative access, it might make sense to layer in additional controls such as:

Preventive	• Require two-factor authentication for remote access to privileged credentials stored in the digital vault • Use jump servers to isolate privileged sessions
Detective	• Log all remote access to the credential vault, especially all failed logon attempts

Use detective controls to avoid over-limiting access

The use of detective controls can often help in achieving the balance between enabling and restricting access. Rather than putting in place preventive controls that may potentially be overly restrictive, in some cases, a better approach would be less restrictive access that is carefully monitored for any violations.

> You need to figure out, 'Where's the area that I'm going to be able to demonstrate business value?' not just the uplift in security but operational efficiencies.
>
> **—DAVE ESTLICK**
> Information Security Chief, Starbucks

For example, for a particular workflow, it may be too restrictive to put in place time-of-day limitations for the use of privileged credentials; instead the organization might monitor the use of privileged credentials and trigger alerts based on time-of-day.

Detective controls are especially important in cases where increasing restrictions is simply not feasible at this point in time. For example, the security team might recommend a business unit reduce the use of privileged accounts for a particular business process, but it might be too difficult to change the process. Instead they can keep a close watch on these accounts and use analytics to determine whether a particular credential is being used outside of the norm.

The key is to capture enough information to create context around an event so that you only investigate truly "interesting" events. For instance, say a privileged user accesses a financial system just before the release of the company's annual figures. You need context to determine if the event is malicious:

- Is it out of the ordinary for this particular user to access this system at this time?
- Were the credentials checked out from the company's password vault?
- Was the use of credentials linked to a help desk ticket indicating a problem with the financial system that would indicate legitimate IT admin activity?

Secure credentials used by applications and scripts

Credentials used by applications and scripts often need better security controls. If possible, applications should meet the following requirements:

- The credentials for the account should be stored securely.
  - If an application obtains an account's credential from a configuration file, an attacker can easily read it. Instead, reconfigure applications to call the password from an encrypted password vault.
- The account password or SSH key should be changed regularly.
  - Changing a credential used by applications is often a sensitive issue, especially if it has been used for so long that nobody knows what the effects of changing it will be. Weigh the value of changing a credential against the operational risk associated with changing it.
- The application should be designed using the principle of least privilege.
  - For example, an application that performs backups should not need permissions to install software.

Applications that do not meet all of these requirements present a potential risk. Ultimately applications — or at least the most critical ones – should be refactored to use more secure methods. However, this is not always feasible, especially with legacy applications and commercial off-the-shelf applications.

> If you don't have good practices in privileged account management, you're making it very easy for adversaries to traverse your whole network. If they get a hold of an over-privileged account, they'll run through the environment like a brushfire.
>
> **—JIM CONNELLY**
> Vice President & Chief Information Security Officer, Lockheed Martin

Compensating controls for embedded credentials

For applications that cannot be refactored right away, compensating controls might be appropriate such as:

- Configure the account to be non-interactive and unusable for logging on
  - You can often configure an account to restrict its use to processes initiated by the operating system, and to make it not valid for logging onto the system.
- Increase monitoring on the accounts
  - Some organizations set up alerts for any event in which a user attempts to log on using an account that is not valid for this purpose. Test for adverse effects on application performance, as some applications are very sensitive to event logging.
- Use analytics to detect possible misuse of an application's account
  - As described above, analytics can help to detect malicious use, if you have enough data from your logging system to provide a rich context around the usage of these accounts.

3. HOW MUCH IS ENOUGH?

Optimizing Tradeoffs between Security and Usability

Changing controls around privileged credentials will impact the workflow for privileged users, such as system administrators and developers. Security staff will need to work with the business process owners and users to create appropriate controls that will not hinder operations or be thwarted by users. There is no magic formula, but useful tactics include the following:

- Use metrics to measure the impact of security control changes
  - Ask how you will know that security has improved. For instance, watch for decreases in the number of unauthorized attempts or access errors.
  - Ask how you will know if improvements have negatively impacted business processes. Look for signs of decreased productivity or complaints from users.
- Provide a break-glass procedure
  - For people to feel comfortable with additional controls around credentials, they often need to know there is a backup plan so that if the system is not functioning properly for any reason, administrators will still be able to access critical assets quickly.
- Consider task frequency
  - Changing the workflow for certain tasks will be more accepted than for others. Getting into the PCI zone, for example, is an occasional task and everyone understands it is important to secure.

> Centralized privileged account management can streamline the logon process and create reliable procedures. If administrators are logging onto each individual platform and there is variation in the way accounts are managed, the complexity of doing it manually can be a nightmare.
>
> **—MIKE WILSON**
> Vice President & Chief Information Security Officer, McKesson

- Organize changes to minimize the change curve
  - Try to package up changes so that users don't have to change their workflow more often than necessary. For example, if you plan to implement multi-factor authentication to access privileged credentials, do it when you implement other new controls.

Seek win-win strategies

Security and usability need not always be in conflict. Unlike many other types of security controls, better processes and technologies for privileged access management can offer the business improved productivity and user satisfaction, in ways such as:

Increased efficiency	• Administrators save time through single sign-on, automated password resets and production of audit reports.
Streamlined workflow	• Approving or reviewing privileged actions can become more reliable and predictable if automated security controls are well-integrated into business processes.
Fewer user errors	• Every IT department has incidents of accidental mistyping that suddenly wipe out files or bring down a machine. Controls can be configured to force review and confirmation when certain commands are used to prevent damaging accidents.
Increased uptime	• System availability can improve as a result of preventing user error. • The time to recover from an outage can decrease through better forensic capability. If privileged sessions are recorded, it is faster to review recent changes in recordings than server logs.
Easier trouble-shooting	• IT issues can be easier to diagnose if detailed user access logs are available to show, for example, that repeatedly, a particular set of user actions was made before a particular type of problem occurred.

Summary

Formulating a strategy to improve privileged access controls across a large enterprise requires making some key decisions and judgment calls. Strong awareness of the business context, such as events that create an opening for change will help ensure an effective strategy that aligns with business goals.

Any effort that impacts business and IT operations will be met with some resistance, however the belief that making changes to privileged access controls will make tasks more difficult is usually more a matter of perception than reality. A successful initiative will require ongoing engagement with users, developers and other stakeholders. The next chapter, Four Pivotal Conversations, will explore these conversations and how to prepare for them.

CHAPTER 2

Four Pivotal Conversations

INTRODUCTION

As described in Chapter 1 of this report, *Three Strategic Decisions*, improving privileged access controls involves working with the business to decide on priorities, the right mix of controls and optimal control design. Implementing these changes requires CISOs and their teams to navigate the organization and get support from many groups.

This chapter is based on insights from an expert panel of Global 1000 security executives who have successfully influenced and negotiated with major stakeholders in their organizations, in order to gain their cooperation and build lasting support for change. Our panelists identified the effectiveness of stakeholder engagement as being one of the most important success factors in the entire initiative.

This chapter zeros in on four key conversations that the CISO and security team will need to drive:

Getting Executive Buy-In How do you get the support of executive leadership to make improving privileged access controls an organizational priority?

Working with Business and IT Process Owners How can the security team effectively partner with process owners to design more advanced controls?

Engaging IT Admins and Other Privileged Users What does it take to win over critical user groups such as IT administrators?

Asking Developers to Refactor Applications How can developers be persuaded to rework applications to improve the security of privileged credentials?

Improving privileged access controls

This involves moving towards more centralized and automated methods, including:

- Stronger cryptographic storage of privileged credentials
- Enhanced accountability for the use of shared accounts
- Systematic enforcement of policy
- Real-time detection of unauthorized activity
- More detailed audit trails

1. "IT'S TIME TO MAKE THIS A PRIORITY"

Getting Executive Buy-In for Improving Privileged Access Controls

Support from the C-Suite for this initiative is obviously critical to obtain the necessary budget and resources. But in addition, executive leadership can rally employees to make it an organizational priority, impart a sense of urgency and ownership across the organization, and prevent it from being derailed by minor issues.

According to our panelists, getting executive buy-in is relatively easy compared to other groups. C-Suite executives have become acutely aware of cybersecurity risks, mostly due to the reports they've seen in the news. With a growing number of highly publicized and catastrophic breaches, many involving compromised privileged credentials, executives are increasingly receptive to proposals for improving privileged access controls.

Some ways to help build your case with executives include:

- Analysis of high-profile breaches
  - Describe how privileged access controls factored into particular breaches and relate it to your company's own risk profile.
- Penetration testing results
  - Assess how long it would take for a skilled adversary to compromise your organization's privileged accounts. Show what information assets an attacker can get to once they have gained high-level privileges.
- Benchmarking
  - Reference industry practices for securing privileged access used at peer organizations.
- Compliance requirements
  - Outline the regulations and standards applicable to your organization (e.g. SOX, PCI, and ISO) that have requirements around privileged access.
- Proof-of-concept results
  - Do a proof-of-concept in which you implement increased privileged account monitoring and report on the results. This can illustrate, for instance, the need for better visibility into how and why critical systems are being accessed.

An opportune time to discuss an initiative to improve privileged access controls might be when recent news reports or audit findings have created a sense of urgency. Once there is recognition of the problem, you will need to have a story around how you intend to solve it. Chapter 3, *Five Essential Components*, will explore the elements of a project plan and provide a sense of what the overall effort might look like.

> "Make it real. Show the executives how business data can be accessed through privileged accounts. It's the quickest way for an attacker to go after data and one of their main tools to drive a data breach."
>
> **GARY HARBISON**
> Chief Information Security Officer,
> Monsanto Company

2. "LET'S OPTIMIZE HOW PRIVILEGED CREDENTIALS ARE USED IN THIS PROCESS"

Working with Business and IT Process Owners

Privileged accounts will be involved at some level in almost every critical business and IT process - from the preparation of financial reports to performing maintenance on a customer database. For the most part, improving the security around privileged accounts will not deeply affect existing processes. However, if the security team works closely with the owners of these processes to understand the underlying credential usage, they can bring that knowledge into the design of controls and see opportunities that not only improve security but also streamline tasks and reduce errors.

The following table shows some examples of useful questions for these conversations:

Questions to Ask	Possible Improvements
Who really needs elevated privileges and at what stages of this process?	In some business and IT processes, certain individuals might have access to more data than their role requires. Reviewing how privileges are used may be an opportunity to reinforce the principle of least privilege.
Would it be feasible to restrict a particular account's use of certain commands, by time of day or physical location?	With automated privileged access technology, granular restrictions can be enforced, limiting access to certain business hours or only from within the office.
Do the risks justify adding steps to the process, such as requiring that a reason be logged for using a privileged credential?	This type of question helps you balance the level of protection with the need to meet other business goals such as efficiency. Gauge whether an additional step would be tolerated considering the frequency and urgency of tasks.
How does the principle of separation of duties apply to this process?	Look for ways to redesign processes so that technology automatically enforces separation of duties.
Are there any patterns of errors which might be prevented if certain steps required approval?	For instance, you can configure controls to ensure that if junior IT operations staff use certain commands, a review process will be automatically triggered to prevent accidental misuse.
Do you still use this application in this process?	Uninstall applications with embedded credentials if the application is no longer used in the process.
Why does this script require a session to be open for so long?	If a script needs to have a privileged session open for a very long time while it runs, consider putting effort into redesigning the script so that it requires shorter sessions.

By helping leaders in business and IT to improve the security and efficiency of their processes, the security team can gain important allies. If prominent leaders in business and IT are champions of the initiative to improve privileged access controls, it can influence the privileged users within their groups. Privileged users are often the most resistant to the changes.

3. "WE'RE GOING TO CHANGE PRIVILEGED ACCESS PROCEDURES... FOR THE BETTER"

Engaging IT Admins and Other Privileged Users

Getting buy-in from those who will use the new access procedures or tools day-to-day is usually one of the more challenging types of conversations. For example, in the case of IT administrators, typically, their "default" view is that they could do their job better with unfettered access and freedom to choose their own tools. They may see any additional steps or restrictions as making their job harder and slowing them down.

Show empathy, challenge perceptions

Encourage the security team to acknowledge that there will be changes to workflow and show empathy for the potential disruption. At the same time, make sure these perceptions get challenged. Demonstrate that the recommended security practices will actually streamline some tasks and make how they operate with credentials much more efficient – with benefits like single sign-on and less tedious password changes.

Having a strong executive mandate and allies in business and IT will be important for these conversations, however persuading administrators to accept changes takes real credibility. The team member that you put in charge of this type of conversation needs both an ability to articulate the threat and technical knowledge of the platforms and applications involved. If the security team doesn't deal with objections at a detailed technical level, it is very possible that the process will become subtly but deliberately derailed.

Staff in non-IT roles who have privileged access – such as those who need to work with financial reports and bank accounts – tend to have more appreciation for how new controls will help them stay out of trouble. These groups are typically much more accepting of new controls than IT.

> "An advantage IT admins can really understand is nonrepudiation. Explain to them, 'For shared accounts, if we're able to track exactly who is doing what and when, if something goes wrong with an account, you won't be a suspect. For investigations, we'll have a forensic trail to know it was definitely not you.'"
>
> **JIM MOTES**
> Vice President and Chief Information Security Officer, Rockwell Automation

4. "HOW CAN WE BETTER SECURE THE USE OF PRIVILEGED CREDENTIALS IN THESE APPS?"

Asking Developers to Refactor Applications

Many applications, scripts and configuration files include hardcoded privileged credentials. Chapter 1, *Three Strategic Decisions*, describes how applications should be refactored so that credentials are securely managed and accounts with lower-level permissions are used. But refactoring can often be challenging, partly because of the inherent difficulties in updating older code, and because platforms make it hard to operate with less than the highest possible permissions.

The security team will need to work through these issues with developers (including third-party application vendors) and determine the right level of privilege for each application. Keep in mind that although certain privileges might not be in use now, new features in future versions of the application might need them.

Depending on the organization, developers may already use the principle of least privilege as part of their software development lifecycle practices, especially for new applications. However, in some cases, if a particular application is set up to require excessive privileges, the security team may need to help developers understand the consequences.

WHY ARE WE DOING THIS? WHY NOW?

Developing a Message Platform

In most organizational cultures, employees will be partly driven by a top-down mandate to improve privileged access controls. However, the initiative will be much more successful if everyone involved supports the effort. To prepare to drive conversations with stakeholders, work with other executives to proactively develop a set of key messages around why the organization and individual stakeholders need to improve controls.

"Here's how we know there's a problem"

Explain the threats, including serious attacks that have actually happened to other organizations, or that your organization potentially faces. Describe how the lessons learned apply to your own organization. Include actual results from penetration testing and benchmarking.

"Here's how it affects you personally"

Many stakeholders will not have thought through how the organization's security affects them personally. Describe the process by which a compromised privileged account could lead to stolen intellectual property or the loss of customer data, which in turn could reduce competitive advantage and/or damage the company's reputation. Ultimately a decrease in business would have a direct and negative impact on an individual's bonuses, pensions and job security.

> The security team absolutely needs to explain the purpose. You can't just explain the process changes. You need to explain why it needs to be done. Otherwise, people won't listen.
>
> **—ROB BENING**
> Chief Information Security Officer, ING Bank

"This will keep you out of trouble"

Point out that if their account is compromised and misused, they could become part of an investigation that they'd certainly rather avoid. Advanced controls can automatically eliminate bad practices which create suspicious behavior, such as keeping privileged sessions open for very long periods, and can ensure individual accountability when something goes wrong.

"This will help you comply with policy"

Without automated methods, consistently keeping up with organizational policy can be difficult over time. For example most organizations have a policy regarding shared privileged accounts that states credentials must be rotated when somebody leaves the organization. Organizations often have periods of high turnover or they may cycle through many short-term IT contractors. Explain that automated credential rotation makes it much easier to comply with existing policy.

"What do you think?"

Stakeholders need to have a sense of ownership. Request their input and then incorporate it into the plans. Make sure the people who follow the new processes get a chance to review them ahead of time.

HANDLING OBJECTIONS

Be prepared to manage, and possibly preempt, the following types of objections that may emerge as the organization rolls out its deployment.

"You can't take away those rights! I need them!"

Tackling Concerns about Removing Credentials

In many initiatives to improve privileged access security, credential proliferation comes up as an issue. Removing access to credentials, even unnecessary ones, can make people feel like something has been taken away from them. Depending on organizational culture, you may be able deal with objections by saying, "Sorry, this is our new policy." But often times, you will need to convince people that the privileges they are losing are really not necessary. Point out that the change protects them personally by reducing the risk that their account is compromised.

In some organizations, responsibility for this conversation can be shared with or owned by managers. In these cases, the security team provides evidence to management that there are unnecessary credentials, and management handles the decision to remove access.

Getting People through the Change Curve

Keep in mind that change will be difficult for some stakeholders. Here are some ways to provide reassurances and build trust:

Let people practice

- Consider setting up workshops, training sessions, and technology labs before, as well as during, the implementation of new controls. Workshops give stakeholders an opportunity to practice using the technology and provide feedback.

Identify influencers

- Take time to understand who the thought leaders are within each group. Focus on getting buy-in from these people, and then ask them to help you convince others.

Leverage initial wins

- Ask the stakeholders involved in the initial pilot to apprise others of the benefits they are seeing. In the proof-of-concept phase, bring in various teams so that they can see how the new processes and technologies work first-hand. This helps them foresee how things will work in their own areas.

"I tried it and it doesn't work"

Responding to Problems and Measuring Impact

As changes to controls are implemented, users may report problems. Proactively set up a process ahead of time for responding to concerns. It's key to be responsive as people adopt new processes and technologies. In fact, it can be useful to be overly responsive, in order to change how people think about the initiative as a whole. If people start with low expectations and then have a surprisingly good experience getting exceptional support, they remember it. Work closely with those who run your service center or helpdesk. You'll need to make sure that support is available 24-7 to ensure that privileged users globally don't have any issues with accessing systems and can get their jobs done.

Besides support, think about control design. If new procedures are excessively awkward or risk reduction isn't materializing, the design of controls might need to be re-evaluated. Be able to measure the impact of your controls, so that you can adjust them appropriately. Chapter 3, *Five Essential Components*, will describe metrics in more depth.

"I don't have time for this"

Overcoming Pockets of Resistance

It is easier to get some groups on board than others. You can expect that when a business unit is stressed and distracted by trying to meet their main targets, it will be a challenge to get them to align around privileged access improvements.

When you encounter pushback, strong executive sponsorship of the initiative is extremely important. Handling these cases is also an art in terms of personalities and change management. As much as possible, focus on the value you bring to users and help them to see the benefits.

In some cases, it will be necessary to play the risk card. At these times, it may be helpful to partner with the legal and/or compliance teams to emphasize that these changes are necessary, and it is an organizational priority to reduce risk.

"This feels like Big Brother"

Ensuring Transparency

For detecting misuse of privileged credentials, organizations often increase monitoring, such as recording privileged sessions. Administrators can sometimes be sensitive about this, and worry if everything they do is going to be watched. They can be reassured by transparency: Work with them to address governance issues such as what reports are run when and by whom.

> Don't assume that because it's an executive-sponsored initiative, it will be implemented without any issues. It requires you to drive a cultural change program. From the earliest phases, evangelize what you're doing and showcase the improvements you're making in the control environment.
>
> **—MUNAWAR VALIJI**
> Head of Information Security, News UK

Summary

Clearly, both technical expertise and soft skills are needed to pull off these conversations. Indeed, openness, honesty, and empathy are key success factors for the entire initiative. The next and final chapter will expand on the skillsets you need to be successful and will explore in more depth some of the elements of a successful effort.

CHAPTER 3

Five Essential Components

INTRODUCTION

What do the CISO and security team need to successfully improve privileged access controls? Chapter 1, *Three Strategic Decisions*, offered direction on making the core decisions that power your overall strategy. Chapter 2, *Four Pivotal Conversations*, recommended ways to engage a variety of stakeholders across the organization.

This chapter provides specific guidance on the team, techniques, and tools you'll need to drive this initiative. Based on discussions with an expert panel of Global 1000 CISOs who shared their experiences from various stages in the journey, it focuses on five important elements:

Realistic Expectations What kind of effort is involved in implementing more advanced controls around privileged accounts? When does the organization start to benefit in terms of increased security?

The Right Skillsets What skills does the security team and/or its partners need to make the initiative work?

Metrics What specific metrics can help ensure and measure your success?

A Plan with Milestones What are some ways to break up the initiative into manageable phases? How can the team keep momentum throughout the implementation?

The Right Tools What types of technologies and features are most useful in a privileged access initiative?

Improving privileged access controls

This involves moving towards more centralized and automated methods, including:

- Stronger cryptographic storage of privileged credentials
- Enhanced accountability for the use of shared accounts
- Systematic enforcement of policy
- Real-time detection of unauthorized activity
- More detailed audit trails

1. REALISTIC EXPECTATIONS

For a large organization, with tens or hundreds of thousands of privileged accounts, the effort involved in improving privileged access controls over the entire IT environment compares to other comprehensive IT initiatives. It is common to scope initial "quick win" phases to be completed in a matter of weeks, in order to gain traction and prove the value of the initiative. Often the initiative is split into phases that can be managed as individual projects over a period of months each.

Rolling-out better privileged access controls across an enterprise, depending on the size of the organization, can typically be a year to multi-year effort. However, organizations can expect to see results in terms of risk reduction almost immediately after deploying improved controls around the first set of accounts. Risk then continues to decrease as you put the controls around more and more accounts.

Panelists say the implementation of advanced privileged access controls is "not rocket science," however, they note it can be technically challenging at times because the overall platforms are not designed with the least-privilege principle in mind.

Business impact

Modifying privileged access controls will affect workflows, for example by changing procedures for logon and/or approvals. Yet typically workflow changes help streamline tasks, such as by providing a single sign-on environment or by replacing manual steps with automation.

During the implementation of improvements, there will be some temporary disruption to business processes. However the panelists report that post-deployment, business processes are typically not slowed down and are often sped up. If well-planned, improving privileged access controls can provide benefits such as increased efficiency, fewer user errors, increased uptime and easier troubleshooting. See page 23 for some suggested metrics to use in measuring business impact.

After the initial deployment, an ongoing effort will be required to ensure that privileged access controls keep up with changes in the environment such as applications moving to the cloud, servers moving from development to production, or corporate mergers and acquisitions. Robust information security and IT asset management processes can help to ensure that privileged access controls will continue to work reliably over time.

2. THE RIGHT SKILLSETS

The following sections outline the full range of skillsets that the panelists have found to be essential for their implementations. In organizations where the CISO is responsible for end-to-end security services delivery, these skills will be needed on the extended security team which includes close partners in IT and possibly external consultants and system integrators. In organizations where the CISO's role is more consultative, the security team will set the requirements but not own the technical implementation. In this case, many roles will be driven by IT, therefore the CISO and security team will need a robust oversight process.

Technical/design

A large part of a privileged account security effort consists of working closely with the infrastructure group, IT administrators, developers and so on. Members of the security team must be able to demonstrate credibility in handling technical issues, and questions and any arguments that might arise. The team should have expertise in areas such as:

Areas of expertise	Examples of particular knowledge or skills
Infrastructure used in the organization	How applications interact with infrastructure
Platforms such as Microsoft Windows and Linux	Active Directory or LDAP
Applications and databases	Oracle and SQL
Application development practices with respect to permissions	Code reviews
Privileged account security controls	Secure logon, credential management and so on
Security control design	Development of repeatable processes
Processes around technology service management	Standards such as ITIL

> The security architect has to have credible technical skills. You can't send someone who doesn't have a high level of technical skills to talk with these various groups or they'll very quickly be written off.
>
> **—MARK GRANT**
> Chief Information Security Officer, CSX Corporation

Security governance and risk

When implementing advanced controls around privileged access, questions will arise around processes and policies, such as:

- How often should a particular password be changed?
- Should a particular network be accessible to administrators who are working outside of the office? What about administrators based in other countries?
- What is the optimal workflow for requesting and approving access to a set of credentials for a particularly sensitive database?

The team should be able to help business and IT leaders make the governance and risk decisions and guide the optimization of policies and processes. This requires a thorough understanding of the business operations and goals. Knowledge of identity and access management (IAM) and account provisioning and maintenance practices are also important aspects. Team members should be aware of the processes in the organization such as how access rights are issued, reviewed and removed.

Project management

A large-scale privileged access security initiative requires methodical planning and tends to have many moving parts. You will need people with strong project management skills on the team to keep all of the various stakeholder groups aligned and focused on what needs to be done and to make sure it happens.

Soft skills

Soft skills are absolutely essential in this endeavor. Chapter 2, *Four Pivotal Conversations*, described how engaging stakeholders is key. The security team will need people with diplomatic skills and an aptitude for negotiation, politics and communication.

Members of the team need to be able to explain why new processes need to be followed and be competent at listening to stakeholders and taking their concerns into consideration. They need the ability to navigate the culture, identify key people who will influence each group and help everyone feel comfortable with
the changes.

3. METRICS

Panelists found metrics valuable in order to illustrate the need for better controls, measure improvements and demonstrate the value of the program. The following table provides some examples:

Use Metrics to...	Example Metrics	Example Results
Test effectiveness of controls	Through penetration tests, measure the potential vulnerabilities of credentials and show how vulnerabilities have been reduced after implementing improvements. Test how long it would take for an attacker to get control of domain admin accounts.	Tests might show that before improvements, the would-be attackers could take over a domain admin account within a few days, while better controls keep attackers at bay for weeks and the account takeover is now detected in real-time.
Show when to make course corrections	Measure access violations before and after implementing control changes. Be prepared to rework controls if expected results are not materializing.	After implementation, the number of access violations for a particularly sensitive database might still be too high. The team may decide a two-person approval and verification system is needed. Or the number of violations may have declined but created too many help desk calls. In this case, the team may decide to modify the granularity of controls.
Gauge the effect of controls on efficiency	Calculate the amount of time admins are spending on tedious tasks, such as resetting passwords.	One large organization showed that system administrators could save 40 hours per month by automating password resets.
Measure how the controls impact system availability	Applications with embedded credentials must periodically go through scheduled downtime so credentials can be changed. Take note of the amount of downtime required.	By refactoring applications to remove hardcoded credentials, this downtime can be eliminated while improving security.
	Admin errors can inadvertently bring down a system. Compare the time required to recover from an outage before and after implementing control changes.	The time it takes to correct errors can be reduced by reviewing privileged session recordings rather than reviewing server logs.
Assess impact on application performance	Test application performance and functionality before and after removing embedded passwords from applications.	Testing can ensure there are no adverse effects on applications and help reassure application developers.

4. A PLAN WITH MILESTONES

Identify early goals

Chapter 1, *Three Strategic Decisions*, described a risk-based approach to deciding on priorities and explored ways to time your efforts to take advantage of opportunities in the enterprise. After identifying priorities, you'll need to further break down the identified priority areas into phases.

Here are some ideas for identifying early goals:

- Do a pilot project
  - A small pilot project demonstrates whether the initiative can work using the tools and processes that you have selected and serves as a template for future phases.
- Make the problem smaller
  - Large organizations often have too many privileged accounts in the environment, often because policies and review processes have not been consistently applied over time or there have been a series of mergers and acquisitions and so on. In some organizations, it makes sense to rein-in privileged accounts in your organization early on.
- Make less-risky changes
  - Some organizations are more comfortable implementing new processes and technologies with less critical systems, and building experience within the team before moving on to more critical ones. This is particularly true when it comes to refactoring applications: start with applications that are relatively non-critical and easy to change.
- Select a small part of a larger deployment
  - If you plan to tackle accounts in large parts of your IT environment, you could set a goal of completing a small part of the effort – such as a particular group of servers – as a quick-win project.

Define phases

The way you define phases and checkpoints will depend on overall scope and on how the company is set up. Examples of how phases could be organized include:

- By platform/technology
  - Create phases for administrative accounts in Windows, Linux, mainframes, databases and so on.
  - In some cases, dealing with all the machines on a particular platform first, then another platform, for example, addressing all Unix servers and then all Windows servers, can help to reduce the risk of intruders being able to move laterally between machines.

> "You're setting yourself up for failure if you treat this as purely a technical security project. Don't just do a pilot with security folks. Include some of the users who may be the biggest naysayers in your pilot. Prove to them that it works. Get their buy in early."
>
> **—KATHY ORNER**
> Vice President & Chief Information Security Officer, Carlson Wagonlit Travel

- By region or by business unit
  - In organizations where each region has its own IT group and infrastructure, create phases by region.
  - Likewise, if the company has separate IT groups for each business unit, address each one as a phase. Possibly leverage the risk officers in the individual business units to help move the program forward.
  - If some infrastructure and applications are centrally managed and others are managed regionally, it may make sense to work on accounts for centrally-managed technology as an initial phase and then regionally-managed accounts.
- By application team
  - If you have multiple application development teams, work with each team in phases.

For scheduling work in phases, consider what would cause the least disruption while adding the most value. If your team has enough bandwidth, certain phases can be done in parallel.

Keep momentum

After you have success in one phase or area, you are in a position to scale up the program. Look for ways to standardize your approach across the organization. For instance, if a pilot project has applied a new approach to managing Unix accounts, use that process and strategy as a blueprint for managing accounts in other platforms.

Some examples of metrics that can be used to track your progress include:

- Number of accounts to be evaluated and those determined to be over-privileged, unnecessary and requiring better controls
- Number of accounts that have been shut down or converted to fewer privileges
- Number of applications or accounts to be moved to a centralized and automated privileged account security management system and number completed

Implementing more advanced controls across a large enterprise often requires a certain persistence and fortitude. A common reporting model is a weekly status meeting for the project team and a monthly review by an executive steering committee.

> Don't bite off too much initially. Phase it in, manage the effort piece-by-piece in an incremental approach. Use a scoreboard to track your progress as things move into your privileged ID process so you can see month over month what it looks like as you continue to drive the advancement.

—JOHN SCHRAMM
Vice President Global Information Risk Management & Chief Information Risk Officer, Manulife

5. THE RIGHT TOOLS

Instead of starting with a tool in mind, the panelists recommend that you start by understanding your strategic goals and formulating your approach, then find tools that will help achieve those goals. However, they also stress the importance of taking the time to select privileged account security and management tools that support your specific security and enterprise requirements. Some technology features that panelists described as especially important include the ability to:

- Securely store credentials in an encrypted vault
- Create a single sign-on environment so that users do not have to remember multiple unique passwords
- Uniquely identify users and restrict their use of privileged accounts to the minimum necessary
- Limit the length of privileged sessions for a user or application
- Centrally monitor and record the use of privileged accounts for detecting unauthorized activity and maintaining a detailed audit trail
- Automate password changes to run on schedule or trigger when an employee leaves the organization
- Scale and meet performance demands in a large enterprise environment
- Integrate with the organization's infrastructure, applications and other security technologies

Other key tools and technologies that can be helpful in this endeavor include:

- Enhanced monitoring and alerting systems such as Security Information and Event Management systems (SIEM) and Security Analytics/Big Data Platforms
- Technology for two-factor authentication to be used for remote access, third parties and infrastructure administrators who have root or domain admin privileges

> "Don't underestimate the change management side of it in terms of processes. Understand that if you just drop a tool in, you might fail. You need to understand the processes wrapped around that tool to make it truly effective."
>
> **—STEVE GLYNN**
> Global Head of Information Security, ANZ

Adopt processes to get the most out of tools

To ensure technologies work smoothly in your environment, the panelists recommend paying particular attention to processes such as:

- Assigning, reviewing and revoking privileges
  - Adding new tools to weak processes will not be successful. In conjunction with the implementation of new tools, the processes involved in privilege management should be reviewed and strengthened.
- Deploying new information assets or adding new accounts
  - Set up processes so that when adding new infrastructure or a new application to the IT environment, each automatically uses the new controls. Any new privileged accounts that are created should also use the new privileged account security solution instead of creating a backlog.
- Planning and testing
  - Before deploying new privileged account technologies in a production environment, thoroughly test the system and make sure that you have assessed the compatibility of all platforms and applications.

Conclusion

It's well-recognized that the theft of privileged credentials and privilege escalation are key stages in most successful cyber attacks. Today's threat environment is prompting many enterprises to address the gaps in their security program to better protect privileged credentials. It requires a strong combination of technical and soft skills, a methodical project plan, appropriate tools and persistence.

The panelists and their teams have successfully put together these components to implement comprehensive enterprise-wide initiatives in privileged account security. Their experience illustrates that successfully improving privileged access controls and reducing the risks of compromised privileged credentials is within reach even for very large and complex organizations.

CONTRIBUTORS

Top Information Security Executives from Global 1000 Enterprises

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 standardization 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, Enterprise Architecture and Information Security, 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.

Jim Connelly
Vice President & 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
Information Security Chief, Starbucks

Dave Estlick is responsible for global infrastructure and enterprise security programs in more than 63 countries across 5 continents. He has over 20 years of experience in software development, architecture, risk and security gained through a variety of technical and leadership roles at organizations including PetSmart, Amazon, Sun Microsystems and Boeing. Dave is a member of the PCI Security Standards Council Board of Advisors.

Steve Glynn
Global Head of Information Security, ANZ

Steve Glynn leads the information security and technology risk function which provides global services for information security strategy; technology risk management and assurance; and identity management. Steve is accountable for implementing robust controls to meet global regulatory requirements and industry standards. Previously he held senior information security, risk and technology leadership roles for ABN AMRO and the Royal Bank of Scotland in Australia and Singapore.

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.

CONTRIBUTORS (CONTINUED)

Top Information Security Executives from Global 1000 Enterprises

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.

Jim Motes
Vice President and Chief Information Security Officer,
Rockwell Automation

Jim Motes is responsible for global information security strategy, policy and programs. Previous roles include VP, Information Security, Invensys PLC; Chief Information Security Officer, Perot Systems Corporation; and Director, Information Security Engineering and Operations, Affiliated Computer Services. Jim also served as a commissioned officer in the United States Army. He has over 15 years of experience in information security and holds multiple security certifications.

Kathy Orner
Vice President & 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.

John Schramm, CISA, CISSP
Vice President Global Information Risk Management &
Chief Information Risk Officer, Manulife

At Manulife, John Schramm is responsible for information security, business continuity, technology risk, risk and regulatory management and GRC technology services across Canada, the United States and Asia. Previous roles include Senior Vice President of Information Security for Fidelity Investments; Chief Information Security Officer for Investors Bank & Trust; and Vice President of Security Architecture and Engineering at FleetBoston Financial and Bank of America.

Munawar Valiji
Head of Information Security,
News UK

Munawar Valiji leads security strategy for News UK, where he is responsible for designing, building, and maintaining highly secure and easily maintainable security platforms. Prior to News UK, he was Head of Information Security for Financial Times. Munawar's extensive experience in information security and IT risk management includes consulting, technical and senior management roles at 2e2, Deloitte, Citi Bank, JPMorgan Chase, National Australia Bank and Sun Microsystems.

Mike Wilson
Vice President & 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 industry organizations including Health Security Alliance, Cloud Security Alliance, and CSO Bay Area Council, and is a board member for Health Information Trust Alliance (HITRUST).

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.