THE **CISO VIEW**

AN INDUSTRY INITIATIVE
SPONSORED BY **CYBERARK®**

Protecting Privileged Access in **Robotic Process Automation**

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

Tim Bengson
Vice President, Global Chief Information Security Officer, Kellogg Company

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

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

Dave Estlick
Chief Information Security Officer, Starbucks

Khadir Fayaz
Vice President, Global Information Security, Pearson

Peter Fizelle
Chief Information Security Officer, Asian Development Bank (ADB)

Mike Gordon
Vice President and Chief Information Security Officer, Lockheed Martin Corporation (LMC)

Omar Khawaja
Vice President and Chief Information Security Officer, Highmark Health

Kathy Orner
Vice President, Chief Risk Officer, CWT

Olivier Perrault
Chief Information Security Officer, Orange Business Services

Thomas Tschersich
Senior Vice President, Internal Security & Cyber Defense, T-Systems International

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

→
LEARN MORE about the contributors

TABLE OF CONTENTS

Introduction **3**

What's new about RPA? 3

Key findings **5**

Key finding 1: Obtaining credentials to reprogram robots gives attackers enormous power 5

Key finding 2: Credentials used by robots are vulnerable to theft or exploitation 7

Key finding 3: Malicious use of robots can easily go undetected 9

Recommendations **10**

Recommendation 1: Be proactive in setting security standards for RPA initiatives 10

Recommendation 2: Strictly limit access for reprogramming robots 12

Recommendation 3: Automate management of credentials used by robots 14

Recommendation 4: Establish robust processes for monitoring RPA activity 16

Recommendation 5: Focus conversations with stakeholders on business opportunities and efficiency 18

Conclusion **21**

Appendix: Biographies of CISO View panelists **22**

A WORD FROM OUR SPONSOR

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

CYBERARK®

INTRODUCTION

From a business perspective, Robotic Process Automation (RPA) promises to be a fast route to increased efficiency, productivity, and quality. Organizations are rapidly adopting RPA to automate business processes, from finance and HR to manufacturing and customer service.

From a cybersecurity perspective, RPA also brings a new and attractive attack surface, with a prime concern being the proliferation of privileged access. Robots—and by extension the humans who control them—are often given broad access to a variety of highly sensitive business applications.

How do you provide robots with extensive access while safeguarding the business? We explored this question with the CISO View research panel: a group of 12 leading security executives from Global 1000 organizations that are early adopters of RPA. This report provides practical recommendations based on their first-hand experiences working to protect privileged access in RPA systems.

This report examines issues such as: What techniques might an attacker use to exploit privileged access in RPA systems? What controls are the most useful and feasible? What are the key success factors in working with business stakeholders?

> "There are great benefits with RPA but also great risks. A lot of power is concentrated in the RPA system. If RPA is not well managed, an attacker might be able to organize sabotage across the whole company with just one system."
>
> **— OLIVIER PERRAULT**
> Chief Information Security Officer, Orange Business Services

On many questions, the CISOs on the research panel were in broad agreement. For other issues, this report captures diverse points of view, reflecting varying scales of RPA deployment and a range of organizational cultures. For organizations at any stage of planning or implementing RPA, this fourth annual CISO View report will help accelerate their efforts to enable automation while managing the risks.

What's new about RPA?

In RPA, software applications known as "robots" interact with the user interfaces (UIs) of business applications. RPA requires less technical expertise than automation methods that use application programming interfaces (APIs). Also, more functions can be automated through a UI than through APIs. The upshot is that RPA enables relatively quick automation for a wider range of business processes.

With RPA, professional-level software development skills are not necessarily needed to get robots up and running. A business team with little understanding of application security could buy an RPA tool out of their own budget and program a robot without involving the security team.

In many organizations, business units are racing to identify tasks that can be automated. Often RPA is an enterprise-wide strategy with mandates from executive leadership: "What did you automate today?"

According to a recent study by Deloitte, 58% of organizations across the world have deployed robotic and intelligent automation and the number of organizations scaling automation doubled from 2018 to 2019.[1]

[1] Deloitte Insights: Automation with Intelligence. Sept 2019.

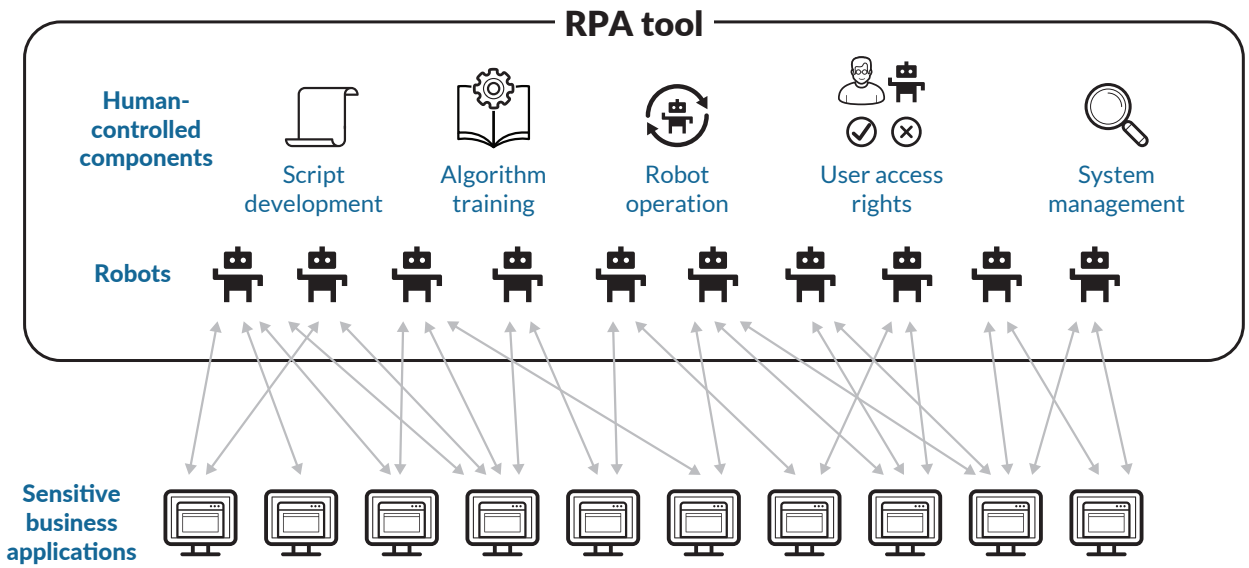
How RPA systems work

RPA tools typically include the following components:

- Script development and algorithm training
  - Scripts are developed that instruct a robot how to interact with applications in order to perform a set of tasks. Many RPA tools also have features to train the algorithms that robots use through machine learning.
- Robot operation
  - After a script is developed, it is deployed to a robot, which executes the script to perform the business process. Robots usually need to log into multiple sensitive business applications while performing a set of tasks.
- User access rights and overall system management
  - RPA system administrators perform tasks such as setting up permissions and configuring logging.

Typically, users of RPA systems are business users who are automating their business processes, and sometimes specialists in IT and development who are working with them to deploy robots.

Figure 1: **Conceptual overview of an RPA system**



KEY FINDINGS

The organizations covered in this research analyzed how privileged access in RPA systems might be exploited by attackers, including malicious insiders. Their findings are outlined below.

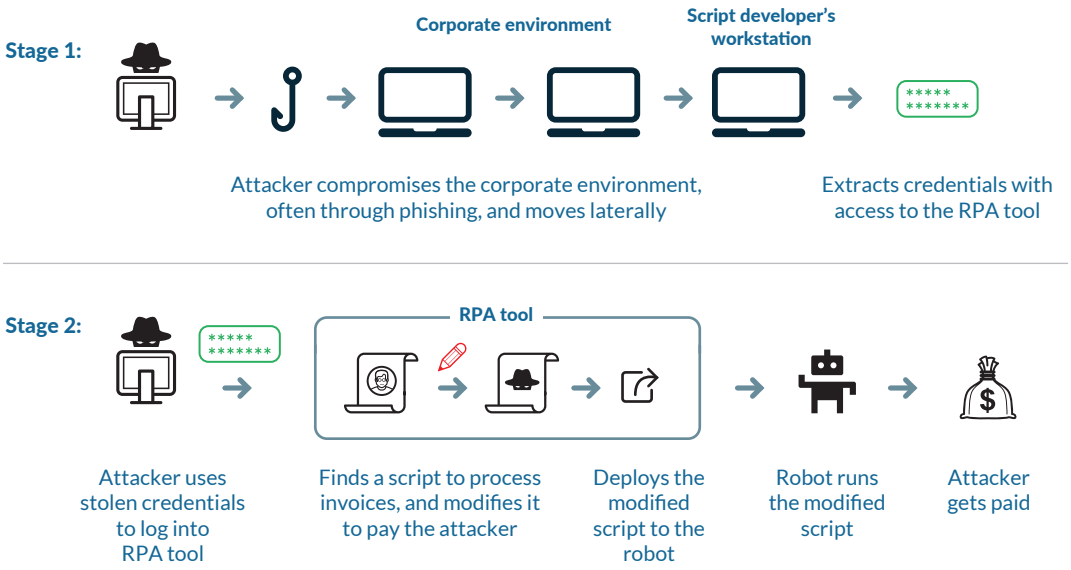
Key Finding 1: Obtaining credentials to reprogram robots gives attackers enormous power

If an attacker is able to reprogram a robot, i.e. change the instructions that the robot will follow, the attacker can use all of the robot's access rights for malicious purposes. A robot that's tasked with distributing software could be reprogrammed to send out malware instead. Or a robot that processes customer orders could be reprogrammed to transmit the customer database to the attacker.

Robots can be reprogrammed with end user credentials for the RPA tool

To reprogram a robot, an attacker needs to obtain credentials for the RPA tool with the rights to modify and deploy the robot's scripts. These credentials are commonly held by business users; they are not necessarily "administrative" credentials for the tool.

Figure 2: **Attacker reprograms a robot**



Robots are typically given extensive access

The damage an adversary can do with a reprogrammed robot depends on the permissions provided to the robot. These are usually more extensive than what most humans would have.

To keep a robot busy, it is often programmed to do a wide variety of tasks, working across geographies and roles, and operating 24/7. Robots typically automate repeatable tasks that were performed by multiple people, so they are given access to more business applications—and a wider range of databases and records—than a human. Additionally, robots, like humans, are often given more access than they need (see below).

An attacker who gains control over a highly privileged robot could direct the robot to:

- Exfiltrate, destroy, or modify sensitive data
- Shut down operations
- Sabotage information systems
- Redirect payments
- Weaponize the robot to distribute malware
- Execute denial-of-service

Whatever the robot ends up being reprogrammed to do, it will do it fast, and multiple reprogrammed robots could be set up to wreak havoc at the same time.

> Business users don't necessarily think of an RPA tool as enterprise software, or of the need to protect access to it. In the rush to deploy, they might give too many people access or give everyone admin access.

– MELISSA CARVALHO
Vice President, Enterprise and Customer Identity and Access Management, Royal Bank of Canada (RBC)

Over-privileged robots

In addition to highly privileged access for legitimate business reasons, robots might be given unnecessary privilege:

- **Overloading an account:** Robots that need access to multiple machines are given admin accounts such as Windows domain accounts.
- **Taking shortcuts:** Robot developers don't take time to figure out least privilege.
- **Reusing code:** Scripts containing highly privileged credentials reused where less privilege would suffice.
- **Underestimating risk:** Robots given privileges "just in case" since they won't misuse privileges.

Key Finding 2: Credentials used by robots are vulnerable to theft or exploitation

For an attacker in search of power, a very attractive target is the collection of credentials that robots use to access business applications.

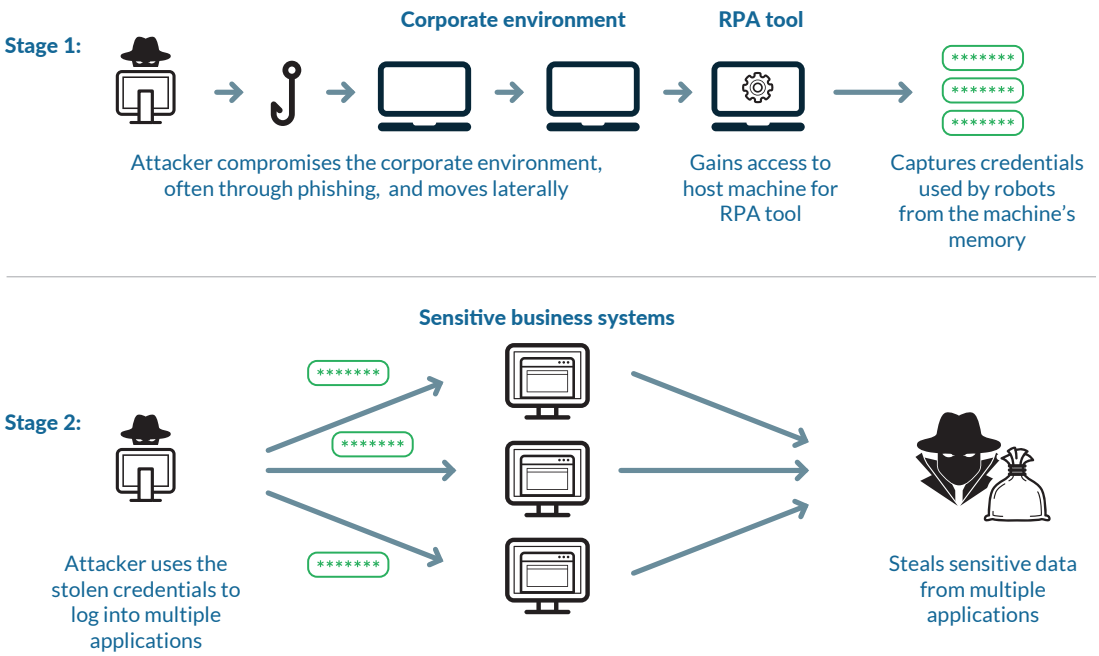
Attackers can find credentials in host machines and scripts

There are several locations in an RPA system where attackers could potentially find credentials such as passwords, access keys, SSH keys, and tokens. They could also find other ways of gaining access such as open sessions and stored hashes.

> "Each individual robot will need access to a number of applications. You have to think about the aggregated access that robots will be given."
>
> **— DANIEL TSE**
> Head, Cyber Security, Information & Technology Risk (CSITR), GIC Private Limited

- In the RPA tool database:
  - Most tools store credentials used by robots in an encrypted database (often referred to as a "vault") on the RPA host machine, which are retrieved by robots at run-time.
  - The RPA tool must temporarily decrypt a credential before passing it to a robot. Attackers who gain access to the host machine can discover these credentials. Various attack methods can be used to get onto the RPA server, such as pass-the-hash or exploitation of web application vulnerabilities.
- On the robot host machine:
  - Some RPA tools have an option to store credentials in Windows Credential Manager on the robot's host machine. These passwords can be retrieved by anyone logging in to the host machine with the robot's account or with a local admin account.
  - Attackers can also use a robot's privileges without seeing its credentials: They can wait for the robot to log into a target system, and then gain entry into the session.
- In plain text files and emails:
  - Passwords might be found in tool configuration files, email archives, and RPA scripts. Developers in a hurry to get RPA running might embed credentials in scripts, then share their code with other team members and on GitHub.
- In transit:
  - Credentials used by robots are susceptible to man-in-the-middle attacks. RPA tools typically use SSL when transmitting credentials to robots, but can be misconfigured to allow self-signed certificates.

Figure 3: **Attacker steals credentials used by a robot**



Credential management is difficult and therefore lacking

RPA tools are not designed to be credential management systems. They don't have automated credential management features such as rotation and audit, etc. This can make good credential management practices difficult to implement and lead to poor practices including:

- Using the same credentials across multiple systems and not rotating them
  - RPA tools connect to hundreds if not thousands of devices and applications. It's not feasible, at that scale, to regularly change passwords and make them complex and unique through manual efforts.
- Not using strong authentication to connect to sensitive business applications
  - Accounts used by robots are typically set up to allow the robot to log in using a username and password only. Most RPA tools don't have built-in functionality for stronger authentication methods.

Credentials that are stored in RPA tools are isolated from centralized management. This runs contrary to enterprise security policies that require centralized privileged access management for all applications across the organization and means that the security team will not have an overall enterprise-wide view of "who has access to what."

Key Finding 3: Malicious use of robots can easily go undetected

Using the techniques described on the previous page, an attacker can gain privileged access to sensitive business applications without the organization knowing.

Monitoring robotic environments has distinct challenges

Achieving visibility and detecting threats in RPA systems present some inherent difficulties:

- Unlike humans, robots won't notice their account has been compromised, e.g. they won't see unusual logins using their credentials and report these suspicious activities.
- Attackers can hide in the noise: Robots work at high speeds. If a robot is copying files from one server to another 100 times per minute, a malicious actor might get the robot to install an infected file without being noticed.
- Some robots will be set up to work 24/7. This makes it difficult to use time of day to detect anomalous behavior.
- It's hard to see inherited privilege. For instance, if a robot has database administrator (DBA) privileges, the robot's name will appear in the DBA group—but not the name of its human operator.

> People tend to trust robots because robots lack intent. A common mistake is to think you can just turn a robot on and walk away since it will only do what it's supposed to do. But robotic processes can be compromised.

– TIM BENGSON
Vice President, Global Chief Information Security Officer, Kellogg Company

Native logging is hard to use effectively for security

Most RPA tools have audit logging, but it's not easy to use these logs for security purposes:

- The volume of logs generated by RPA systems can quickly become overwhelming to review.
- Out-of-the-box alerting focuses on cases where robots run into problems carrying out a task, not security issues.
- Logging can be turned off using RPA system admin-level credentials. An attacker could turn off logging to evade detection.
- Events that take place outside the RPA tool will not be logged, e.g. if an attacker steals a robot's username and password for a website and then uses it to access the website from a browser on his own desktop.
- Malicious behavior is difficult to trace if accounts are shared between robots and/or humans. It's hard to know which robot or human—robot operator or developer—is responsible for a problem.

RECOMMENDATIONS

The following recommendations summarize the practical guidance shared by the CISO View panelists for protecting privileged access in RPA.

Recommendation 1: Be proactive in setting security standards for RPA initiatives

The business, eager to adopt RPA, can jump into it without fully understanding the risks. It is key to get ahead of the curve. Building security into RPA projects will save costs in the long run.

Get involved well before robots are deployed

The security team is often called into RPA projects when scripts are ready to run. By then, the automation can already be lacking key controls such as separation of duties. At this stage, it will be difficult to retrofit a project. The security team may forced to stop the rollout.

By getting involved in the early stages of RPA adoption—when use cases are developed, roles established, standards set, and technologies selected—Security can be positioned as an enabler rather than an inhibitor.

> With RPA, it's critical to include security from the outset, because once that horse is out of the barn it will be much harder to bring it back under control. Create a governance structure for all RPA initiatives that includes security—to evaluate whether existing infrastructure, access roles, and process controls are sufficient to support each initiative.

– DAWN CAPPELLI
Vice President, Global Security and Chief Information Security Officer, Rockwell Automation

Understand the use cases

Have the security team work closely with the business to understand the use cases being proposed for automation. Then educate the RPA teams on best practices to ensure they:

- Consistently include security steps in the use cases
  - Security can provide templates to make it easy for robot developers to do it themselves.
- Retain checks and balances when implementing the workflow
  - Manual processes are often not fully documented. If the RPA team implements the workflow verbatim from the documentation, security steps may get left out.
- Reduce risk in the business logic for use cases
  - E.g. If a robot processes customer emails, have it read emails only from certain domains to avoid processing phishing emails.
- Plan additional controls to protect data
  - E.g. In a healthcare environment, humans naturally assess if the patient data they are reading is plausible. If a robot is programmed to read patient data, you might add data integrity checks.

Consider implementing RPA to automate IT and security processes such as configuring infrastructure or managing incidents. This can help the security and IT teams build RPA knowledge and skills.

Align RPA security standards to the enterprise-wide security framework

Securing RPA should not be a standalone strategy. RPA implementations should be subject to enterprise-level standards for protecting privileged access. This includes managing RPA credentials using a privileged access management (PAM) system to ensure:

- Credentials are safely stored in a purpose-built centralized vault with multiple layers of control
- Enforcement of policies such as password complexity and rotation
- Use of multi-factor authentication or device authentication to retrieve credentials
- Ability to meet audit and compliance requirements
- Enterprise view of who has access to what—including RPA human users and robots
- Consistent controls across all applications in the organization

Building security into RPA environments will require coordination with teams across the organization. Organizations often manage RPA initiatives through an RPA Steering Committee, RPA Center of Excellence, or Security Governance Committee. The security team should play a key role in RPA governance, driving the adoption of RPA security standards.

> While the business can program the robot and get it going, they don't always have the mindset around security. And if something goes wrong with what a robot is doing, it'll happen fast. Make sure your RPA security program is comprehensive enough and getting to all the business stakeholders.
>
> **– KATHY ORNER**
> Vice President,
> Chief Risk Officer, CWT

Participate in the RPA tool selection process

Make security requirements part of the evaluation criteria when an RPA tool is selected. A decisive factor will be whether the RPA tool can be easily integrated with enterprise security systems, such as the PAM system and the security incident and event management (SIEM) system. Another important consideration is whether the RPA tool provides audit logs with enough detail for security monitoring. Lack of essential functionality in the tool can lead to major delays in later phases or the need to abandon a tool and select a different one.

Include security costs in proof-of-value for RPA

The business often wants to get robots up and running as fast as possible in order to show value quickly. This can lead to requests for security exemptions. Avoid granting exemptions, as they often make it difficult to overlay security later.

Building the cost of security into the proof-of-value will more accurately reflect the actual costs involved in implementing RPA. Have security accounted for as a baseline cost, which allows the business to derive value from RPA, not as an overhead cost that can be cut.

Recommendation 2: Strictly limit access for reprogramming robots

Anyone with the right combination of permissions in the RPA tool has the ability to reprogram robots. Make sure that power is safeguarded and used appropriately.

Securely manage credentials for RPA tools

- Ensure that only those with a legitimate business reason get access to the RPA tool.
  - Establish processes to remove unnecessary access to the tool, e.g. if users change roles.
  - Keep a tight rein on all administrative-level access. Don't allow use of the default admin credentials.
- Store all credentials for accessing RPA tools in the PAM system's centralized enterprise vault.
  - Require multi-factor authentication to access RPA tool credentials. Consider time-of-day restrictions.
  - Recognize that even accounts with read-only access to scripts are powerful. Certain scripts might include sensitive information.
  - With administrator accounts for RPA tools that access highly sensitive systems, consider additional controls such as session recording to establish accountability, and using a proxy server to isolate sessions.

> The bottom line is to have secure script development. Have guidance and rules around what's acceptable. Possibly consider static and dynamic code testing, but for detecting well-written hazardous code, peer review as part of your process is a good control.
>
> **— PETER FIZELLE**
> Chief Information Security Officer, Asian Development Bank (ADB)

Ensure use of secure software development practices

All RPA projects should use the principles of secure software development.

- Train RPA teams on secure software development practices.
  - Robotic processes should go through rigorous code review and testing.
  - Have the security team do routine review and testing or provide training and tools and get involved by exception.
- Ensure script reviews and/or tests are triggered whenever significant changes are made.
  - RPA scripts will change with changes in business processes.
- Automate as much review and testing as possible.
  - Use tools to detect embedded credentials in RPA scripts.
  - Consider building or buying tools for automating RPA script inspection. Commercial tools began to emerge in 2019.

Controlling who runs a robot

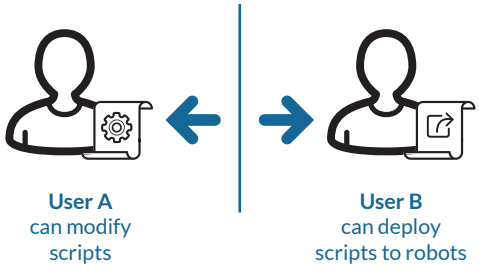
Many RPA tools don't let you control who can run a particular robot, but you can obtain this level of control through a PAM system. For instance, configure a PAM system to say, "Only these people can operate robot X."

You can also limit what a particular person can do when operating a particular robot. For instance, if a robot is designed to query a server and make a list of the services on it, configure the PAM system so that, "Person A can operate robot X to run queries only on servers Y and Z".

Segregate duties between RPA tool users

- If feasible, segregate duties between RPA tool users.
  - Reprogramming a robot should require at least two people—one to modify the script and another to deploy it. Consider having a third person to test the script before it is deployed.
  - Set up development, test, and production environments so that developers can't inadvertently change data in production or sabotage the production environment.
- Depending on the organization's operations and culture, it might not be feasible to segregate duties of RPA tool users.
  - If this is not feasible, consider setting up different accounts for different roles, having robust logging to trace all actions to a specific RPA tool user and/or strictly limiting robots' scope of duties (see section below).

Figure 4: **Separating duties between RPA tool users**



Establish policies around robots' scope of duties

When tasks are automated, organizations must decide how many duties each robot will be set up to handle. These decisions will affect how useful a compromised robot might be to an attacker.

If robots are allowed to perform a wide range of tasks, there will be fewer robots to manage. This approach minimizes account proliferation and license costs. However, each robot will have a lot of access, so keeping control over each robot is imperative.

If robots are given smaller mandates, there will be more robots to manage. This approach works best in organizations that are set up to manage accounts at large scale. It has several security benefits:

- An attacker would have to take over multiple robots and coordinate their activities to conduct an attack of real significance.
- Changes in a robot's behavior will be easier to detect.
- Monitoring of transactions that involve sensitive data is more manageable. For instance, a robot could be set up to work exclusively with human resources data, so that a data owner from the human resources department can monitor its logs.

To restrict the mandate of a robot, limit its access to credentials using a PAM system and set up monitoring to detect deviations from the robot's original set of tasks.

> If you limit the scope of what a robot can do, you won't end up having robots with pervasive access beyond the original intent. If you assign one robot one account for one business process, it will be hard for that robot to extend beyond that process.

– DAVE ESTLICK
Chief Information Security Officer, Starbucks

Recommendation 3: Automate management of credentials used by robots

At the scale and speed of robotic processes, it is not feasible to rely on manual efforts to manage credentials. RPA tools are not purpose-built security tools and don't provide the necessary functionality to implement automated credential management.

Overview of key controls

Adequately managing the credentials that robots use to access business applications requires:

- Storage of credentials in a centralized, secure vault rather than in the RPA tools or scripts
- Complex and unique passwords
- Frequent rotation of credentials
- Strong authentication for retrieval of credentials
- Monitoring and auditing of credential usage

Automating these controls involves integrating RPA with your organization's PAM system. Once integrated, robots will retrieve the credentials they use to access Windows and/or business applications from the PAM system's vault.

> "Ultimately it goes back to avoiding anything that's got to do with manual management of credentials. That's number one. You've got to automate all your access processes and move as much as possible to automated rotations, just-in-time access, token rotation, short-lived access and all that."
>
> **– KHADIR FAYAZ**
> Vice President, Global Information Security, Pearson

Use automated selection and rotation of credentials

- Use machine-generated passwords
  - Configure the PAM system to generate complex passwords for the robots to use.
  - Ensure passwords are unique for every business application that robots access.
- Develop and enforce rotation policies
  - Set up the PAM system to automatically rotate the credentials that robots use.
  - Most organizations covered in this research are initially aiming for rotation every 24 hours. Many plan to increase the frequency to every 4 hours, or after every use. Ultimately, automated rotation can be set to any schedule.
  - Some organizations take the credential rotation policies they have in place for humans and apply the same policies to robots. However, more frequent rotation may be feasible for robots because, unlike humans, robots don't complain about password policies.
  - To meet operational requirements, some organizations use single sign-on: After a robot logs into Windows on its own virtual machine, it is automatically logged into the business applications it needs to access. In this case, the PAM system is set up to frequently rotate the single Windows credential.

Perform identity checks before releasing credentials

A way of implementing strong authentication for robots is to have the PAM system perform additional checks to verify the robot's identity before it releases the credentials. If the identity check fails, access to the credential is blocked and an alert is generated. For example, check that the robot's request for credentials is coming from:

- The robot's usual IP address and device type
- A machine with an appropriate certificate
- The robot's usual domain username (if logged into Windows)

Limit robots' ability to use credentials

Limits can include time-of-day restrictions and just-in-time access or time-limited access to credentials. To mitigate privilege escalation, robots deployed to support one department should not be able to access credentials from another department. For example, a PAM system can be configured so that a robot from customer service is unable to access credentials for critical R&D applications.

Safeguarding open sessions

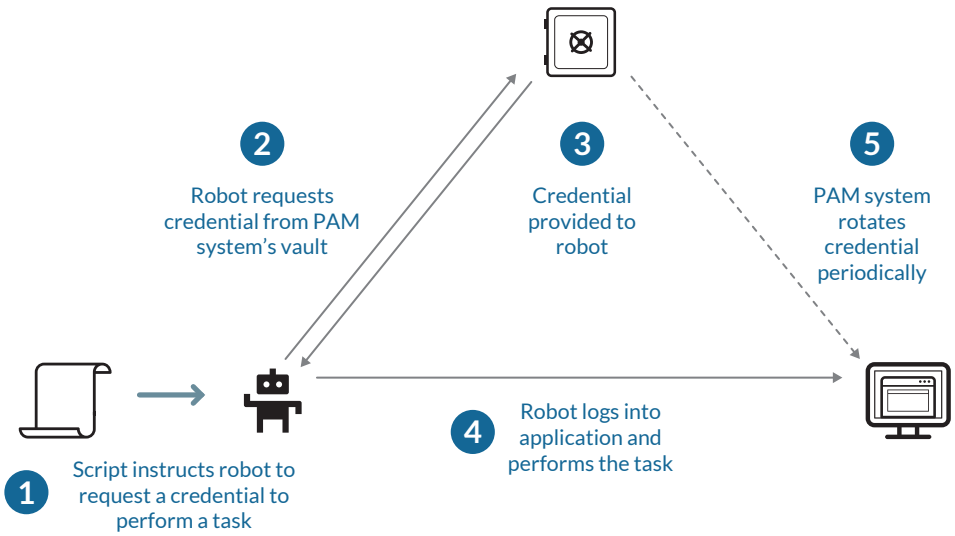
To ensure that a robot's open sessions are used only by the robot, consider the following controls:

- Have each robot run in its own Virtual Machine (VM).
- Don't allow humans to interact with the VM. If they need access to the VM, have them use screen sharing technology.
- Do not allow remote access to the VM.

Integrate RPA with PAM

Integrating an RPA tool with a PAM system requires installing a connector between the tool and the PAM, and installing a credential management plugin for each business application the robots will access. Connectors and plugins are available off-the-shelf for commonly used RPA tools and applications. They can also be developed using APIs. RPA script developers will instruct robots to request credentials from the PAM system's vault by simply adding a parameter to the script, which is done through the RPA tool's user interface.

Figure 5: **Automated credential retrieval and rotation**



Recommendation 4: Establish robust processes for monitoring RPA activity

In discussions with the CISOs on our research panel, frequent themes included ensuring accountability, nonrepudiation, and the ability to detect anomalies.

Ensure humans are accountable for robot activities

Each robot should have a human manager who actively oversees the robot and is accountable for the robot's activities. A robot manager's responsibilities typically include:

- Requesting access rights for the robot
  - Consider having access requests reviewed by the robot manager's supervisor.
- Ensuring least privilege for the robot
  - Access rights should be reviewed periodically and removed if no longer needed.

Robot managers must clearly understand their responsibilities and acknowledge that they are accountable; some organizations require them to sign periodic attestations to this effect.

> The point is anomaly detection. In theory, a machine is going to be far more prescriptive so you can detect anomalies more easily than with humans. You might start with transaction monitoring and simple alerting.
>
> **– MIKE GORDON**
> Vice President and Chief Information Security Officer, Lockheed Martin Corporation (LMC)

Make every action traceable to a robot and human

Every action taken by a robot should be traceable to the robot and its developer, tester, and manager to ensure nonrepudiation.

- Assign every robot a unique account for each system that it accesses. Do not allow robots to share accounts with other robots.
- Avoid having a robot share an account with a human, unless absolutely needed for a workflow.
- Log all modifications to scripts so that making changes to robot actions is traceable.

Build capabilities to detect security issues in robotic processes

A compromised robot will be able to do lot of damage very quickly. Aim to be able to rapidly detect and respond to unauthorized or anomalous robot and human activities.

Plan to mature capabilities over time

RPA is still a relatively new technology, and the ability to integrate RPA with log analysis tools is evolving. To build detection capabilities, security teams are integrating RPA with tools such as security incident and event management (SIEM) and user behavior analytics (UBA). Analytics tools are also still maturing (see sidebar on next page on using UBA). Some organizations find that commercial tools do not yet meet their requirements and are building their own analytics tools in the interim. Others rely on custom scripts to generate alerts.

Identify the events that should trigger follow up

Work with the business to determine what events might warrant investigation. Some examples are:

- A script developer who normally doesn't deploy scripts tries to deploy a modified script.
- A robot manager tries to access a robot they don't manage.
- A robot that sends data to an external server suddenly starts sending it to another location.
- A robot attempts to pay a third party that's never been paid before.
- A robot tries to log into a business application that it doesn't usually use.
- A robot used for HR tasks requests credentials to a customer database.
- Activity during a time of day that is not usual for the robot or human operator.

Configure the RPA tool's native logging

RPA tools typically provide an audit trail feature. One of the main challenges to consider is the potential volume of logs generated by robot activity, and the corresponding volume of alerts.

- Ensure the tool is configured to collect data that will be useful for reviewing and alerting.
- Log actions throughout robot development, deployment, and operation, including changes to scripts.
- Determine the granularity of data to feed from the RPA tool to the SIEM and UBA systems.
- Decide who will review logs and receive alerts.

Monitor robot credential usage

To detect anomalous use of credentials, organizations can use the PAM system to:

- Track all requests to retrieve credentials from the vault and detect anomalous requests.
- Monitor and record sessions in which particularly sensitive credentials are used.
- Integrate with SIEM and other analytics tools.

For Windows environments, Advanced Threat Analytics (ATA) can also be used to analyze credential usage and generate alerts.

Using UBA with RPA

The CISOs we spoke to for this research believe that detecting anomalies in robot behavior will be critical. Opinions vary on the feasibility of integrating RPA with UBA in the near term, given that RPA and UBA are both immature technologies. Most teams had already given a lot of thought to the challenges and possible solutions in using UBA with RPA including:

Baseline robot behavior

- What's normal for robots will be quite different from humans. Robots work with a faster cadence, e.g. log in more frequently. Separate baselines should be implemented for humans and robots.

Set tolerances for robot behavior

- With analytics, you can calculate risk scores and set tolerance levels for deviations from normal behavior, i.e. a certain level of change in behavior triggers investigation.

Keep pace with robotics technology

- Much of the potential of RPA is in the ability of a robot to learn new behavior. As robots become more intelligent and start to change behaviors on their own, detecting unusual behavior will become more challenging.

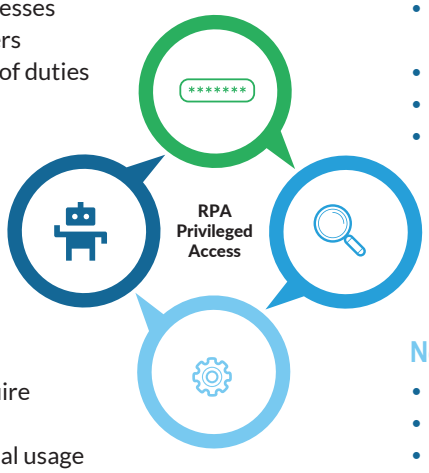
Key controls for protecting privileged access in RPA

Maintain Control Over Robots

- Store RPA tool credentials in the centralized vault
- Use secure software development processes
- Segregate duties between RPA tool users
- Establish policies around robots' scope of duties

Maintain Control Over Credentials Used by Robots

- Store robot credentials in the centralized vault
- Ensure there are no credentials in scripts
- Generate complex, unique passwords
- Rotate credentials automatically



Detect Unauthorized Robot Activity

- Identify types of robot events that require follow-up
- Detect anomalous behavior or credential usage
- Integrate with log analysis tools

Nonrepudiation and Oversight

- Assign a manager to every robot
- Ensure least privilege for robots
- Make every action traceable to an individual robot or human

Recommendation 5: Focus conversations with stakeholders on business opportunities and efficiency

Implementing the RPA security strategy will involve influencing stakeholders across the enterprise.

Make communications a priority

RPA will be used pervasively in many areas of business and the people implementing it may not be inclined to think about security or consult with the security team. Communications will be especially key with RPA initiatives.

- Implement a wide-reaching education program so that stakeholders know that RPA projects are expected to meet enterprise security standards.
- Encourage the security team to write policies and provide instructions without the use of jargon. RPA team members are relatively non-technical and often don't understand terms such as "privileged access management."

Lead with a positive message

To get the listener's attention at the start of a conversation, frame the initial message to focus on facilitating the business opportunities of RPA and providing a safe environment for the RPA teams to experiment with technology. Bring up specific risks later in the conversation, after the positive message has been established.

Highlight the efficiency benefits of the security strategy

Emphasize the benefits of aligning RPA to the enterprise privileged access management standard:

- Simplified script development
  - A single design pattern for developers to use for retrieving credentials, regardless of platform or application, provides a repeatable solution that can be quickly integrated.
  - Training and tools for secure software development enable developers to build secure scripts from the onset. Delays to fix software security issues are thus reduced.
- More efficient robot operation
  - Automated credential management removes the burden of doing this work manually.
  - Automated rotation means better performance; maintenance windows for rotation are minimized.
- Easier audits and better compliance
  - Robust access controls and monitoring help organizations avoid audit failures or regulatory compliance violations, reducing the need to shut down systems for remediation.

> "Businesspeople want to hear about business opportunities. It will be easier to attract their attention if you start by saying, 'I'm here to help you create even better opportunities by using security to safeguard your transactions.' It's more a difference in attitude than methodology."
>
> **– THOMAS TSCHERSICH**
> Senior Vice President, Internal Security & Cyber Defense, T-Systems International

Help individual stakeholders relate to the risks

Business users are seldom interested in descriptions of attack pathways or security technologies. What works is helping them understand the risks and the extent to which their actions will offset risks:

- Help them relate to the risks by describing the business impact of compromised robots and how they benefit personally from security (see table on page 20).
- If possible, quantify the business impact of a security incident in dollars.
- Demonstrate risks rather than describing them. For example, use red teaming or a discovery tool to show insecure credentials in RPA and how they can be exploited.

Examples of describing business risks to stakeholders

Stakeholders	Business Impact of Risk	Personal Benefit of Security
Business leaders of an RPA initiative in manufacturing	If we don't adequately protect access, attackers could take over the process and bring down one of our manufacturing plants, translating to a million dollars per hour of lost time as we try to regain control.	Conforming to the enterprise security standard reduces your risk of being responsible for a plant going down.
Developers of a customer service robot	The robot's credentials provide access to multiple customer databases. If attackers get these credentials, they could breach millions of customer records containing personally identifiable information. We'd be required by regulations to disclose the breach, and the company could be fined up to 4% of our annual revenue.	Designing the robot to retrieve credentials from the enterprise vault reduces the risk of your work being a factor in a data breach.
Owner of a robot that reconciles purchase orders to invoices	If the robot's privileges allow it not only to "read" invoices but also to "write," an attacker who steals the robot's credential could modify invoices to send payment to themselves. We would lose money to fraudsters.	Since you are accountable for the robot's actions, it's in your best interest to limit its privileges. Make it hard for fraudsters to have your robot work for them.
RPA tool system administrator	If attackers obtain your credentials, they can reprogram robots to harm us. For example, they could train a robot to destroy data in the customer order system and we could lose millions of dollars' worth of orders.	Using MFA and session recording brings down the risk of your credentials being used for sabotage. And if your password is stolen, we'll have a complete record of what was done with it and when, reducing the burden on you during the investigation.

CONCLUSION

The CISOs involved in this research know that the risks of privileged access in robotic processes can often be underestimated by the business. They also recognize that the security team can offer tremendous value to an organization's RPA strategy. If involved early on, the security team can contribute to the formation of repeatable processes that will enable RPA to be scaled up securely. They can prevent costly pitfalls such as inappropriate tool selection and can enable security standards to be met through automation rather than through manual efforts.

The principles of securing privileged access are not new, but with RPA comes a window of opportunity to apply those principles from the ground up in a new environment. Along with advances in security technology and processes in the past several years, many security teams have made great strides in building strong positive relationships with the business. Leading CISOs see RPA as a chance to build security into a key business innovation and are well placed to achieve it.

> A lot of these best practices are things that organizations should have been doing for years with any non-human account. Let's not continue bad habits like hardcoding passwords into scripts. With RPA, we can formulate the right habits to begin with.

– OMAR KHAWAJA
Vice President and Chief Information Security Officer, Highmark Health

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

APPENDIX **BIOGRAPHIES OF CISO VIEW PANELISTS**

Top information security executives from Global 1000 enterprises

Tim Bengson

Vice President, Global Chief Information Security Officer, Kellogg Company

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

Dawn Cappelli

Vice President, Global Security and Chief Information Security Officer, Rockwell Automation

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

Melissa Carvalho

Vice President, Enterprise and Customer Identity and Access Management, Royal Bank of Canada (RBC)

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

Dave Estlick

Chief Information Security Officer, 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's global technology infrastructure. He was responsible for strategy and execution in technology standardization, infrastructure convergence, and the establishment of the Starbucks private cloud. Previously, 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.

Khadir Fayaz

Vice President, Global Information Security, Pearson

Khadir Fayaz leads Pearson's enterprise's digital security transformation programs, owns the cybersecurity blueprint and capability portfolio, and manages a global workforce. He has 17+ years of experience driving large-scale technology security initiatives, cyber resiliency and risk management programs, and global transformation programs in cloud enablement and DevSecOps. Prior to Pearson, Khadir was Global Security Architecture head at Carlson Wagonlit Travel and held senior security and IT roles at Agilent, British American Tobacco, Cognizant, and Capgemini.

Peter Fizelle

Chief Information Security Officer, Asian Development Bank (ADB)

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

Top Information Security Executives From Global 1000 Enterprises (CONTINUED)

Mike Gordon

Vice President and Chief Information Security Officer, Lockheed Martin Corporation (LMC)

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

Omar Khawaja

Vice President and Chief Information Security Officer, Highmark Health

Omar Khawaja oversees information security and risk management for the Highmark Health portfolio of health care businesses, which employ more than 40,000 people and serve millions of customers across the U.S. He has spent over 15+ years delivering, developing and managing security solutions for startups, service providers, consulting firms and enterprises. Omar serves on the board of the Health Information Trust Alliance (HITRUST) and as an adjunct faculty member for the CISO program at Carnegie Mellon University.

Kathy Orner

Vice President, Chief Risk Officer, CWT

As Chief Risk Officer, in addition to overseeing global information security strategies operations and programs, Kathy Orner is responsible for global business resiliency, global insurance portfolio, trade sanction and embargo business operations, and enterprise risk management. In her previous role as CISO at CWT (formerly Carlson Wagonlit Travel), Kathy built the global information security organization. Other previous roles include VP & CISO at Carlson, CISO at United Health Group and CISO at Blue Cross Blue Shield of Minnesota.

Olivier Perrault

Chief Information Security Officer, Orange Business Services

Olivier Perrault is CISO at Orange Business Services, a global IT and communications services provider. He leads the department which defines, builds and runs the security of Orange Cloud Services. As companies migrate to the cloud, Olivier's mission is to ensure it will enable not only cost-efficiency and flexibility but also better security and business continuity. His 20+ years at Orange includes several director roles in R&D and wholesale divisions and Cloud Technical Director.

Thomas Tschersich

Senior Vice President, Internal Security & Cyber Defense, T-Systems International

Thomas Tschersich is Chief Security Officer for Deutsche Telekom Group and Senior Vice President Internal Security and Cyber Defense such as CTO of Telekom Security. Thomas is a member of the German national Cyber Security Council, of the UP-KRITIS Council and Chairman of the BITKOM Security steering committee. He has been with the Deutsche Telekom security team since 2001, including leading security strategy and establishing Technical Security Services and Group IT Security. He has a degree in electrical engineering.

Daniel Tse

Head, Cyber Security, Information & Technology Risk (CSITR), GIC Private Limited

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

ABOUT THE CISO VIEW INDUSTRY INITIATIVE

Sharing information on good security practices is more important than ever as organizations face increasing cyber security risks. At CyberArk, we believe if security teams are armed with the leading wisdom of the CISO community, it will help strengthen security strategies and lead to better-protected organizations. Therefore, CyberArk has commissioned an independent research firm, Robinson Insight, to facilitate an industry initiative to explore CISO views on topics related to improving privileged access controls. The initiative brings together top CISOs who share their insights into critical issues facing practitioners today. By developing CISO reports, studies and roundtables, the initiative generates valuable peer-to-peer guidance and dialogue. For more information on this initiative, go to www.cyberark.com/cisoview.

- **CyberArk** (NASDAQ: CYBR) is a global company providing 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.