coresecurity
by HelpSystems

DOING IDENTITY ACCESS RIGHT

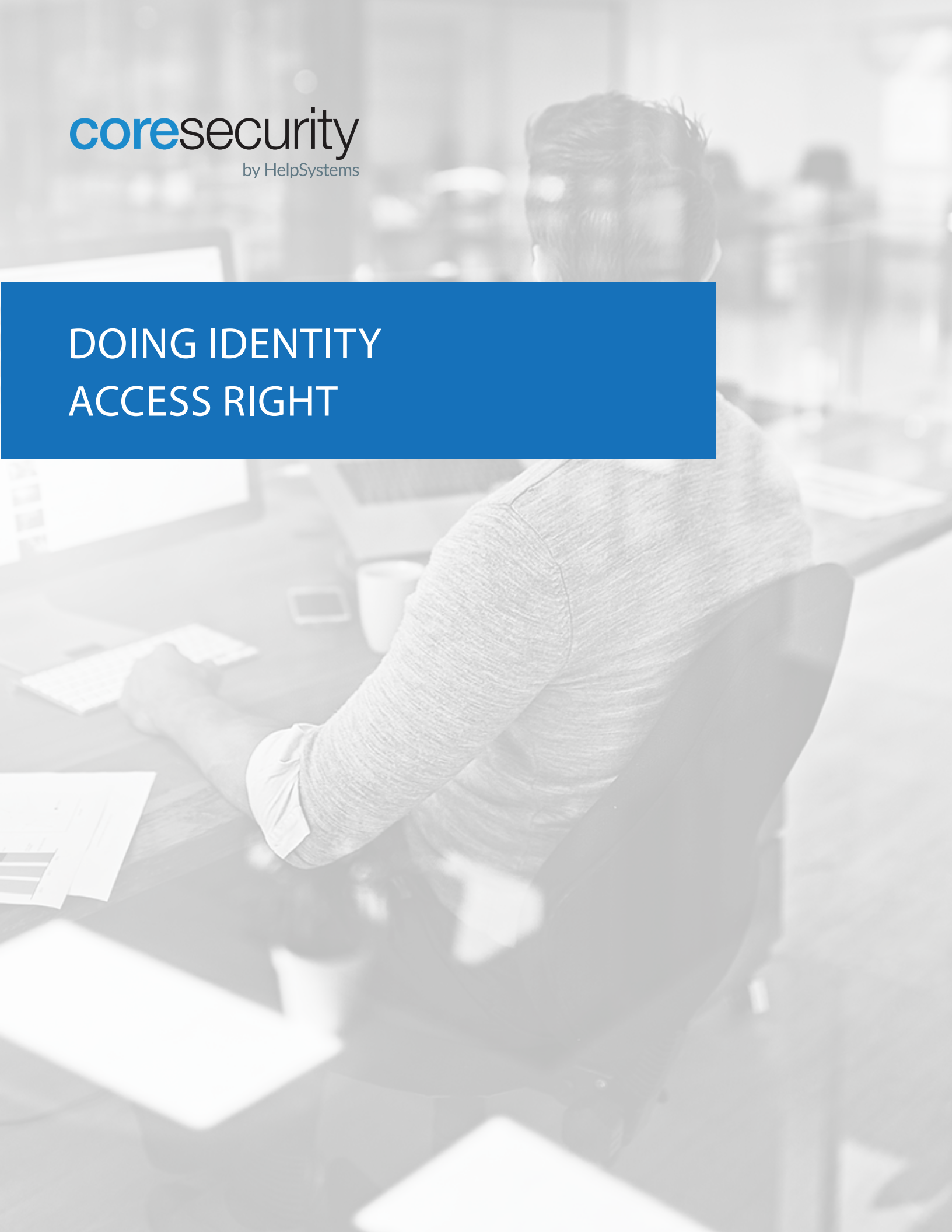

TABLE OF CONTENTS

3 Introduction

4 Most Common Access Risks

5 What is Identity Governance and Administration (IGA)?

6 How does IGA Combat the Top 3 Risks?

7 Issue of Compliance

8 Certification Fatigue

9 Next Step: Visualize IGA

INTRODUCTION

Caring for your company data as one of your most valuable assets can seem like a constant balancing act. In a world of corporate hacks and ransomware, keeping your data under digital lock and key is absolutely essential. But so is allowing your employees to use it to do their best work. Managing who has access—not to mention the what, where, why, and how—is an issue of identity access.

Here at Core Security, our mission is to help customers succeed in a world that demands open access but is also subject to increasing threats. We want to make sure that only the right people have the right access, to the right resources, and that they're doing the right things with them. And when this is not the case, we want to ensure that we are able to recognize and mitigate the threats that may result. With these goals in mind, the essential questions of identity access facing every organization become clear:

How can we assess threats and gauge the risk faced from both internal and external forces?

And how do we actively plan ahead with processes to help detect, identify, and manage the risk?

MOST COMMON ACCESS RISKS

Between the growing number of connected devices and the wide variety of locations from which they are accessed, monitoring and managing the complexity of user access rights becomes harder every day. The stresses and strains of access can come from all over, but the most common offenders are:

Routine changes such as hiring, promotions, or transfers

Business changes such as reorganizations, the addition of new products, or new partnerships

Infrastructure changes such as mobility, cloud adaptation, system upgrades, or new application rollouts

In addition to stresses from business change, the number of government regulations that influence how business is conducted across many industries continues to rise. From healthcare to banking, the number of regulations can climb into the hundreds, making full compliance more difficult and complex than it has ever been. This increase in regulations along with the increase in complexity of access rights (such as increased applications, devices, etc.) means that organizations must make standardized and closely managed identity access a top priority. These policies are known as Identity Governance and Administration (IGA).

WHAT IS IDENTITY GOVERNANCE AND ADMINISTRATION (IGA)?

Identity Governance and Administration is commonly defined as a policy-based, centralized composition of access control and identity management practices usually put in place to help support efforts to remain compliant with government or industry regulations.

Wondering what this official language actually looks like in practice for your organization? Implementing IGA should include the following steps:

- Properly designed and governed roles that help define "least privileged" access for users
- Streamlined provisioning based on these roles designed for your organization
- Continuous monitoring of all access and entitlements to stay on top of changes
- Full visibility of all access and entitlements allowing for better informed decisions

HOW DOES IGA COMBAT THE TOP ˜ RISKS?

With an increasing number of computers and other devices and an increase in the ways in which users access resources, access rights and the monitoring and managing of complex user access rights becomes harder every day. The stresses and strains of access can come from all over but the most common offenders are:

Risk from Routine Changes – Faster, more accurate onboarding of new employees, contractors, and business partners by using roles, business friendly user interfaces, and policy-driven approval workflows. These help to ensure least privileged access during

day-to-day operations such as on/off boarding users and performing access reviews.

Risk from Business Changes – With roles based access control you can build out new roles faster and more accurately for employees impacted by business changes to prepare for a reorganization or merger or acquisition. It is also possible to easily view directly assigned and hidden access and quickly identify outlier access both before and following business changes such as a reorganization or M&A activity.

Risk from Infrastructure Changes – New application roll out? No problem. By adding in the new application using your IGA solution, you can quickly provision whole teams at once and get them started within minutes with the correct, least privileged, access required to be effective from day one.

These are only a few examples of ways that IGA can support and enable the business as well as help ensure proper access based on your policies or on industry regulations to remain compliant.

ISSUE OF COMPLIANCE

What once was just an issue for highly regulated industries—like healthcare and financial services—is now starting to affect everyone. The new GDPR regulation in Europe is an example of a regulation that touches all industries and impacts privacy and cybersecurity efforts. Going forward, you have to be very specific and diligent in the type of information that is known and stored about an individual in order to be compliant. Cybersecurity efforts that require information about an individual must be reviewed with this requirement in mind. Solutions that provide visibility into who has access to personal information will become more valuable to you when working to become complaint.

Under the GDPR, organizations are required to take these new measures related to identity access:

Protect the personal information of users and customers including name, location, online identifier (like email address), and any ID number.

Obtain the explicit consent of data subjects on what data is gathered, stored, and shared and for what purposes in clear terms.

Inform all data subjects of any data breaches, and pay hefty penalties for data breaches and instances of noncompliance.

Time and Efficiency

In order to be fully compliant with most regulations, you must certify access on at least a yearly basis.

In the past, certifications were done on spreadsheets, and completed only once a year due to the amount of time it took to manage the project. The problem was that as soon as the data was gathered—which could take weeks—it was already out of date. However, with a well-defined and implemented process as well as a user-friendly means to review and attest to required access, you will save time on audits and save money by avoiding fees or fines for being non-compliant. You will also have a log of all of the certifications and access points that have been either granted or revoked so that if you are audited, you will have proof of your continuous efforts to remain compliant with whatever regulations you have in place.

CERTIFICATION FATIGUE

When you have a large organization and are manually provisioning or certifying access, it can quickly lead to fatigue—which turns certification into a rubber stamping process. Of course, you want to make sure that everyone has access to the applications that they need, but you also need to ensure least privileged access to remain compliant and, more importantly, secure. But, what if you don't know if your employee needs access? The spreadsheet, or other types of solutions that present lists of people and entitlements for review, rely on repetitive tasks to

"approve/deny" and offers little in the way of information about the context of the user, the user's peers, their access, and what the access actually means. You need more information and more visibility.

With a visual-first approach to IGA, you can see all of your employees' entitlements at once and can quickly see any outliers in the organization. This makes it easy to spot when someone may have too much access and gives you the option to approve, deny, or send back to ask more questions around why that person needs access to that application or infrastructure. For example, everyone on the marketing team has access to the mail server and marketing automation software, but why does the one person also have access to payroll? It could be a mistake or a nested entitlement that you are seeing for the first time, or it could be an attacker using that identity to steal valuable information.

NEXT STEP: VISUALIZE IGA

So how do we make it easier to see all users' access and entitlements and start working toward least privileged access for all? Clearly the years of using spreadsheets, including online webpage functional equivalents, isn't working. It's time for a new approach where you can finally visualize IGA. Think about if you had the ability to:

Protect the personal information of users and customers including name, location, online identifier (like email address), and any ID number.

Obtain the explicit consent of data subjects on what data is gathered, stored, and shared and for what purposes in clear terms.

Inform all data subjects of any data breaches, and pay hefty penalties for data breaches and instances of noncompliance.

Initial observations show that when users are given the ability to literally "see" role design and certifications, they had twice as much accuracy and reduced time spent reviewing by 50%. Can you say that about the other solutions you are using?

Identity access management is not going to get any easier in the future. However, with a strong plan, governance rules in place to ensure least privileged access, and a solution to help you visualize access, you can make it easier for your organization.

Core Security Visual Identity Suite (VIS) offers the simplest most intuitive way to manage roles and certify users. Find out how VIS can help you at:

www.coresecurity.com

coresecurity
by HelpSystems

www.coresecurity.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.