Compliments of:

SailPoint | Accenture Security

The Ultimate Guide to Identity Governance:

How to Build a User-Centric Security Strategy

Jon Friedman

SailPoint: The Power of Identity™

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

About Accenture Security

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

The Ultimate Guide to Identity Governance:

How to Build a User-Centric Security Strategy

Jon Friedman, CyberEdge Group

Forewords by Kevin Cunningham and Rex Thexton

CYBEREDGE PRESS

The Ultimate Guide to Identity Governance

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

For general information on CyberEdge Group research and marketing consulting services, or to create a custom book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-0-9961827-6-8 (paperback); ISBN: 978-0-9961827-7-5 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Designer: Debbi Stocco
SailPoint Subject Matter Experts: Darran Rolls, Kevin Cunningham, and Erika Jarvi
Accenture Subject Matter Experts: Rex Thexton and Neha Joshi

Table of Contents

Forewords

Today's business world is constantly changing, and the identity industry continues to adjust to address evolving identity requirements.

Fifteen years ago, identity projects were focused on increasing business efficiency. When SailPoint entered the market, we added a governance layer to automate business processes and address a wave of regulatory mandates.

Now we're seeing another change. The network perimeter, which once protected our sensitive data and applications "behind closed doors," is no more. The use of cloud computing, mobile applications, and shadow IT is exploding. Hackers are taking an organization's identities and using them as the avenue to sensitive information.

It's time we think about security in a new way. We must put identity at the center of security, so enterprises can confidently empower their users with new technologies.

We want to help you understand how an identity strategy can give you confidence and security. In *The Ultimate Guide to Identity Governance,* we explain why identity is so critical to your IT operations and security strategy, as well as how to think about your best path forward.

Kevin Cunningham
President & Co-Founder
SailPoint Technologies

At Accenture, we are always looking ahead to help our clients leverage strategic technologies to deliver high performance.

Identity governance is one of those strategic technologies. Identity governance solutions help enterprises defend themselves against complex attacks that often start with stolen user credentials. They can also help enterprises protect unstructured data, use cloud-based resources more safely, streamline compliance activities, and simplify the "customer experience" of managers and employees who want fast, simple access to applications.

But identity governance has numerous moving parts, and is evolving rapidly. It can be challenging for managers and executives alike to understand and address new challenges as they appear in this kind of environment.

This guide is designed to give readers a solid grounding in the basics of identity governance today: what it is, why it is important, how it helps enterprises tackle cybersecurity and business problems, and how to build a strategic roadmap for implementation.

We hope the guide will encourage you to look more deeply into identity governance, and to consider how to strengthen and expand its use in your organization.

Rex Thexton
Managing Director and Global Practice Lead—Digital Identity
Accenture Security

Introduction

A few years ago, cybercriminals and hackers spent their time devising ingenious malware, finding vulnerabilities in popular software packages, and launching SQL injection attacks.

Today, they have found that it is easier to capture and exploit user access credentials.

At the same time, we have changed the way we work. We are embracing mobile and cloud computing, and using collaborative applications that make it very easy to share files and unstructured data. But we are finding it extremely difficult to answer seemingly basic questions about who has access to applications and systems, and if they are violating corporate access policies.

These developments have moved identity towards to the center of cybersecurity. Today, organizations need comprehensive identity governance solutions to ensure that people have appropriate access to computing resources, and to answer such critical questions as: "Who has access to what?", "How can they use that access?" and "Does that access conform to policy?"

This guide provides an overview of identity governance. We will discuss what it is, how it fits into today's IT environments, how it can prevent or mitigate data breaches, and how it can strengthen compliance and improve productivity. We will also explore how to develop a strategic roadmap for implementation, and how to select the right partners for that journey.

Chapters at a Glance

Chapter 1, "Identity Moves to the Center of Security," defines identity governance and describes the types of risks it addresses.

Chapter 2, **"The Power of Identity Governance,"** explains how identity governance solutions connect to everything, see everything, and empower everyone.

Chapter 3, "Identity Governance in Action," uses the Cyber Kill Chain® model to show how identity governance can prevent and mitigate data breaches.

Chapter 4, "Identity Governance and the Cloud," examines how enterprises can become more secure as they increase their use of cloud computing.

Chapter 5, "Building Your Strategic Roadmap," suggests how to assemble a steering group, build business cases, create a strategic roadmap for identity governance, and bolster training and communication.

Chapter 6, "Selecting the Right Partners," explores criteria for choosing the right strategy and technology partners.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

Identity Moves to the Center of Security

In this chapter

- Examine why the "human vector" is the new attack vector of choice for hackers
- Define identity governance
- Learn how changes in the workplace increase risks and how identity governance helps address those risks

"The use of stolen, weak or default credentials in breaches is not new, is not bleeding edge, is not glamorous, but boy howdy it works...It is used in highly targeted attacks as well as in opportunistic malware infections. It is in the standard toolkit of organized criminal groups and state-affiliated attackers alike."

— Verizon 2016 Data Breach Investigation Report (DBIR)

Today, everyone in information technology needs to be concerned about user access privileges related to employees, contractors, and partners – or simply, "identities."

Why? Because right now, compromised identities are arguably *the* most serious problem in cybersecurity. According to Verizon, *63 percent* of data breaches involve stolen, weak, or default user credentials (see *Numbers tell the story*, below).

Numbers tell the story

Most data breaches are linked to compromised or misused credentials:

63% of confirmed data breaches involve weak, default or stolen passwords.

66% of insider misuse involves privilege abuse.

60% of organizations cannot detect attacks that use compromised credentials.

Sources: Verizon *2016 DBIR*, Rapid7 *2015 Rapid Detection and Response*.

The Keys to the Kingdom

Why do attackers utilize user credentials so often in their activities? Because there is no need to smash windows if you have a key to the door.

At any given time in a large organization, thousands of employees, contractors, business partners, and customers are accessing hundreds, or even thousands, of applications. Each point of access for those thousands of users is a potential point of exposure.

Cybercriminals and hackers need to find only one weakness among millions of points of exposure. Once an attacker captures one valid set of user credentials, through a phishing attack, or malware, or a mistake by a single user, the door is open to plunder and disrupt the organization.

Because identities are the targets of so many cyberattacks, security efforts must focus on protecting them, and that starts with identity governance.

Compromised user credentials have played a major role in many of the most serious data breaches of the last few years. Captured credentials of a third-party vendor, a refrigeration contractor, led to the Target data breach and the loss of credit card information for 110 million customers. Personal information on 21.5 million government employees and job applicants was stolen when hackers used credentials from a contractor to penetrate systems at the United States Office of Personnel Management (OPM).

Defining Identity Governance

Identity governance helps enterprises prevent data breaches by protecting an organization's identities. But what is it, exactly?

A working definition

We define identity governance as:

Technology and processes to ensure that people have appropriate access to applications and systems, and that the organization always knows who has access to what, how that access can be used, and if that access conforms to policy.

All employees should be provided with exactly the access they need to do their work, and no more. For example:

- ☑ When James joins the company, on day one he obtains access to all the applications and systems he needs for his job – and no others.
- ☑ If Leila quits, all her access is terminated immediately.
- ☑ Sheila in accounts payable can pay invoices, but cannot initiate new vendors or invoices.
- ☑ Boris the email administrator can manage the email software, but not the customer service application.

Major processes

Identity governance solutions help organizations inventory, analyze, and understand the access privileges granted to employees, contractors, and partners. They automate processes related to identity information and access in ways that increase efficiency, strengthen security, and improve compliance with government regulations and industry standards.

Identity governance involves at least three sets of processes:

- ☑ **Policy modeling** to determine what permissions should be given to people based on their roles and responsibilities
- ☑ **User account provisioning** to manage and approve requests for access, provide access to multiple systems in an automated fashion, and revoke access when people change roles or leave the organization
- ☑ **Access certification** to verify and document on a regular basis that access is being provided and managed based on the organization's policies

Terminology in this field can be confusing. Broadly speaking, **identity management (IdM)** and **identity and access management (IAM)** are umbrella terms used to encompass two sets of technologies and processes. The first, **identity governance** (sometimes called identity governance and administration or IGA) relates to managing access policies, provisioning user access, and analyzing access rules, risks, and activities. The second, **access management**, consists of technologies that control access in real time, such as authentication, single sign-on, and password reset. **Identity-as-a-service (IDaaS)** refers to IdM technologies delivered from the cloud.

Challenges from the New Ways We Work

Legacy identity management tools and processes were designed for a relatively straightforward scenarios: full-time employees, sitting in corporate offices, on the corporate network, with a laptop or desktop computer, accessing structured applications running in the organization's data center. But changes in the way we work have made governing user access privileges more challenging – and much more important for security and compliance.

Many types of users

Over the past decade, contractors, suppliers, business partners, and customers have been given increasingly wider access to key business applications.

To maintain security, organizations need to enforce identity governance policies for these users that are typically more restrictive than for full-time employees. Because their "life-cycles" within the organization may be only weeks or months rather than years, their privileges need to be reviewed and revoked much more frequently.

BYOD and shadow IT

The bring-your-own-device (BYOD) phenomenon has created a situation where thousands of devices sourced by individual employees need to be managed safely. The challenges include registering unknown devices, provisioning them with required apps (including security apps), and ensuring that access from the devices to corporate applications is controlled in accordance with the organization's policies.

Another major issue is shadow IT, the tendency for employees and departments to use software-as-a-service (SaaS) applications without the knowledge of the IT organization. Often this behavior is caused by the perception that acquiring access to applications is difficult and takes too long. Security and compliance are both threatened when IT is unable to monitor or control access to those applications and the data they store. Organizations need to simplify access to authorized applications so it is easy for employees to "do the right thing."

Cloud computing

A recent study predicts that 92 percent of computing workloads will be processed in cloud data centers by 2020.[1] The migration of business applications to the cloud is a major challenge because enterprises typically have limited access to identity information and events within cloud platforms and SaaS applications.

In addition, because most organizations manage a hybrid environment, they need a single, consistent view into all identity data across on-premises and cloud applications. Further, they would like to be able to model, provision, monitor, and revoke permissions across environments that include both cloud platforms and traditional corporate data centers.

1. Forbes: With Internet Of Things And Big Data, 92% Of Everything We Do Will Be In The Cloud

Unstructured data

Most existing identity governance products are designed to work with structured data. However, the industry analyst firm IDC has estimated that 90 percent of digital information consists of unstructured data, including documents, videos, and other types of files, as well as email messages, blog posts, and messaging and chat sessions.

Today, some of the most serious security risks are created in situations like these:

- ☑ When Li in sales downloads a customer list from Salesforce, and attaches it to an email message.
- ☑ When Arnab in HR downloads employee information, including compensation and Social Security numbers, to a spreadsheet and saves it on a SharePoint server.
- ☑ When Sally in engineering uploads product design files to Dropbox, and invites a supplier to access them.

To manage these risks, organizations must be able to keep track of vast amounts of unstructured data, determine which files and folders contain sensitive information, and control who has access to that information.

The Benefits of Identity Governance

Reduced risk and improved security

Identity governance technologies and processes are designed to give people access to the computing resources they need, but no more. This “need to know” approach to access reduces the risk of security breaches. It also minimizes the damage that can be done if a hacker acquires user credentials or an insider goes rogue.

Identity governance processes help organizations eliminate common weak points that hackers exploit, such as:

- ☑ Weak passwords
- ☑ Orphaned accounts (dormant accounts of former employees)
- ☑ Entitlement creep (excessive access rights that employees accumulate as they change roles)
- ☑ Violations of separation-of-duties (SoD) policies (controls that divide responsibilities to prevent individuals from committing fraud)

Automated compliance

Numerous government standards and industry regulations, such as Sarbanes-Oxley, HIPAA, PCI DSS, and the EU GDPR, require enterprises to prove that they have policies and IT controls in place to ensure that only people with a need to know have access to sensitive information.

Organizations must not only implement appropriate policies and controls, they must also prove that these are in place and working. Documenting this can be extremely expensive and time-consuming.

Identity governance tools automate the process of certifying access, and provide a wealth of reporting capabilities required for audits.

A SailPoint white paper, *Get Compliant and Stay Compliant*, provides useful advice on using identity governance to improve compliance. You can find it at https://www.sailpoint.com/resources/get-compliant-and-stay-compliant/.

Empowerment of employees and increased productivity

Identity governance solutions empower employees by ensuring that they have access to the applications and systems they need, every time they need them.

The best identity governance tools can also:

- ☑ Increase the productivity of end users by providing self-service capabilities to reset forgotten passwords and request new access
- ☑ Increase the productivity of business managers by reducing time spent certifying access permissions
- ☑ Increase the productivity of IT staff by minimizing the volume of helpdesk calls related to password reset and access requests

In the next two chapters of this guide we look at how identity governance delivers these benefits.

Chapter 2

The Power of Identity Governance

In this chapter

- Understand how identity governance is addressing the challenges of complex threats, diverse workers, cloud computing, and unstructured data

"I know who I was when I got up this morning, but I think I must have been changed several times since then."

— Alice, in *Alice's Adventures in Wonderland*

In the previous chapter, we looked at how changes in the way we work have created major new challenges for identity governance. In this chapter, we examine how identity governance technologies and processes are meeting those challenges.

Adopt User-Centric Security

Most organizations employ a network-centric or an application-centric approach to cybersecurity. That is, they start by asking, "How can we defend each network segment," or "How can we defend each application?" They then rely on tools like firewalls, intrusion prevention systems (IPSs), and security information and event management (SIEM) systems to detect and block attacks on the individual network segments and applications.

Unfortunately, many of these organizations look at managing identities as an afterthought. They don't invest enough time and effort in critical tasks such as:

- ☑ Analyzing who actually needs to access each network segment or application, and who has permissions they don't need
- ☑ Identifying orphan accounts and SoD violations
- ☑ Providing business context to determine whether *jamesjones*, *jjones*, *jim.jones*, and *jjsalesmgr* are four different people, one person who accesses four resources, or something in between
- ☑ Deciding which identities are high risk (because they have access to sensitive information or applications covered by regulations and compliance standards)

Orphan accounts are accounts associated with people who have left the organization. SoD policies prevent one person from performing multiple acts to perpetrate a fraud (e.g., creating a phony vendor account and then issuing checks to it).

In contrast, organizations that use identity governance to take a user-centric approach to security are able to:

- ☑ Remove unnecessary permissions and accounts before they can be exploited by cybercriminals and hackers
- ☑ Ensure that SoD and other identity-related controls are in place and enforced
- ☑ Correlate identity information with identity attacks (e.g., notice that *jjones*, *jim.jones*, and *jjsalesmgr* tried to log on to different applications at the same time from three different locations)
- ☑ Provide extra monitoring and controls for high-risk identities

Organizations that take a user-centric approach to cybersecurity don't ignore firewalls, IPSs, SIEMs, and other proven security tools. However, they start by thinking about how to obtain and use accurate identity information, and how this information can strengthen all aspects of security.

To take a user-centric approach to security, start by answering three questions: (1) **Who has access today?** (catalog existing users and resources to determine who is currently using what to do their jobs), (2) **Who should have access?** (model who should have access to resources and data based on their needs and organizational policy), and (3) **How is that access being used?** (monitor and audit to identify suspicious activities and to continually improve the access model).

Connect to Everything

Identity-related information includes data about computer system users, accounts, groups, permissions, and entitlements. It also includes details about computing resources such as applications, network segments, databases, and sometimes documents and files.

An enterprise-grade identity governance solution connects to every application and system in the IT environment, both those in on-premises data centers and those hosted in the cloud.

Directories, applications, and other identity repositories

In most organizations, HR systems and enterprise directories like Microsoft Active Directory are the systems of record for employee identity information such as names, contact information, titles, roles, reporting relationships, organizational units, and major system accounts.

However, HR systems and directories contain only a subset of identity information within the organization. Most people have accounts, permissions, and credentials for multiple applications and devices. These might include email and collaborative tools, financial and other enterprise applications, professional and line-of-business applications, and computers and other devices owned by the business and by the individual.

An identity governance solution should be able to connect to *every* directory, application, and other repository of identity information so that it can create a complete, highly granular picture of the permissions available to each individual.

Cloud applications and platforms

As more corporate and collaborative applications move to the cloud, identity governance solutions are adding capabilities that allow them to connect to cloud-based applications, just as they have connected to on-premises applications. Key cloud applications include:

- ☑ Business applications provided by SaaS vendors (e.g., Salesforce, Workday, Atlassian JIRA)
- ☑ Email and collaboration solutions (e.g., Microsoft Office 365, Google G Suite, Slack, HipChat)
- ☑ Commercial and "home-grown" applications running on cloud platforms such as Amazon Web Services (AWS) and Google Cloud Platform.

Unstructured data

Some advanced identity governance solutions are now able to connect to applications and repositories that hold unstructured data, including:

- ☑ Local file servers and network attached storage (NAS) systems
- ☑ On-premises email and collaboration applications, such as Microsoft Exchange and SharePoint
- ☑ Online file storage applications, such as Microsoft OneDrive, Box, Dropbox, and Google Drive.

Figure 2-1: A user-centric identity governance solution connects to all on-premises and cloud-based applications and data repositories that users access.

There are several important standards in the identity management field that support interoperability. These include the Lightweight Directory Access Protocol (LDAP) for accessing and connecting directories, the Security Assertion Markup Language (SAML) for exchanging authentication and authorization data, and the System for Cross-domain Identity Management (SCIM) for sharing information about user attributes, group memberships, and provisioning actions.

See Everything

Identity governance solutions can give organizations a single view into all identity-related information in the IT environment.

Information about users and resources

An identity governance solution can provide comprehensive visibility into information about users, their devices, the accounts they use, the resources they access, and the permissions they have been granted.

If you can answer the question, "Who has access to what?" in a comprehensive way, you can perform tasks such as:

- ☑ Revoking entitlements that are rarely or never used
- ☑ Eliminating unnecessary entitlements by asking the administrators or "owners" of applications and resources to specify who actually needs access
- ☑ Comparing users with similar roles and responsibilities to pinpoint those who have excessive permissions

These activities will help you remove unnecessary entitlements that could be used by attackers, and also pass compliance audits.

Data about requesting access and creating accounts

Identity governance is also about processes. An effective identity governance solution will monitor events related to requesting, approving, revoking, and certifying access rights and creating user accounts.

If you have detailed data on events generated by these processes, you can:

- ☑ Analyze whether permissions are being requested, approved, and revoked by the right people
- ☑ Determine if users are granted permissions quickly, so they can become productive, and if unnecessary permissions and orphan accounts are being revoked promptly to reduce risks
- ☑ Flag suspicious activities, such as creating new admin accounts (a favorite tactic of hackers), or requesting access to systems a particular user shouldn't need
- ☑ Determine if entitlement certifications are being performed according to policy, and whether they are being performed conscientiously or in an inattentive, perfunctory manner
- ☑ Look for ways to streamline request, approval, and revocation processes

Make sure your identity governance solution has visibility into events that are generated outside approved processes. For example, it could create alerts when application owners create new user accounts without going through the normal request and approval process. But the system should also be able to manage exceptions. For instance, you might have a policy that only members of the HR department can access the payroll application. You might make an exception for a small office where the local administrator manages personnel. In that case, your identity governance solution should flag the exception, record why it was approved, and enforce reviews more often than typically required.

Empower Everyone

The best identity governance solutions empower employees and managers to perform identity-related activities quickly and easily. The key is replacing complex spreadsheets and confusing user interfaces with intuitive interfaces and workflows that match real business processes.

Business users

Employees want to minimize the wait time between requesting and receiving access to resources. Identity governance tools can automatically provision access to new employees, streamline request and approval workflows for existing employees, and in some cases eliminate wait times entirely by giving users access to self-service interfaces.

Identity governance products offer features to speed up workflows and avoid bottlenecks. Options can include allowing multiple approvers to be contacted in parallel (rather than serially), allowing approvers to delegate their role when they are busy, and flagging approvers who do not respond to requests within a pre-determined time. Have someone in your organization learn and configure these options, because they save a lot of employee time and avoid frustration.

Employee education is critical, including training on how to use the tools and workflows provided by your identity governance solution. It also includes education on security practices. For example, all employees should be trained on the importance of password hygiene such as creating strong, unique passwords and resetting them on a regular basis. You also need to plan how you are going to reinforce the education by offering refresher courses on the identity governance tools, and by routinely testing and enforcing compliance with password policies.

Business managers and resource owners

Businesses are complex. Jobs are complex. IT can't realistically be expected to understand all the details of organizational structures and roles, or all the resources and permissions needed to perform jobs. In contrast, business managers

and resource owners[2] should understand their organizations and how jobs are done.

Well-designed identity governance solutions empower business managers and resource owners to participate in the process of defining access policies and modeling roles. They enable this participation by providing interfaces that use non-technical terminology and common business concepts.

The same principle applies to certification processes, which have been a sore point for years in many organizations. Most managers, when presented with baffling technical questions, respond by approving 100 percent of existing entitlements ("How the heck should I know if Francis really needs access to \\Shares\Corp?"). Well-designed identity governance solutions provide intuitive interfaces that allow business managers to play an active role in pruning unnecessary permissions.

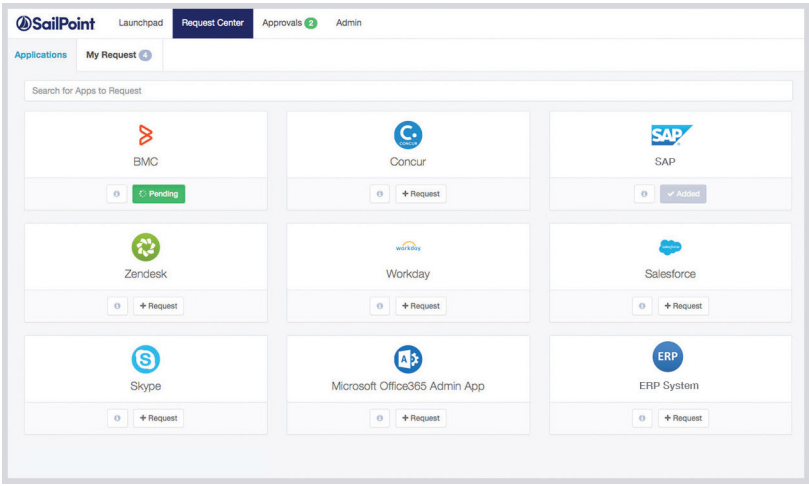

Figure 2-2: With the right interfaces, business managers can play an active part in defining policies and roles and in certifying permissions.

2 Resource owners are administrators and analysts responsible for configuring and managing specific applications, as well as computing services such as email, file shares and networks.

Take Actions

Identity governance solutions can help automate IT controls and give confidence to the IT organization that corporate policies are being enforced. For example, data supplied by an identity governance solution can be used to:

- ☑ Automate and accelerate time-consuming processes
- ☑ Eliminate orphan accounts and unnecessary permissions
- ☑ Find and resolve violations of SoD policies
- ☑ Implement extra controls and monitoring for high-risk accounts and users
- ☑ Streamline access requests and certification processes

Saving $1 million+ annually at Rockwell

Rockwell Automation faced a serious challenge when trying to improve its processes for requesting and granting access to computing resources. At least 25 different processes could trigger requests. In 20 core applications alone there were more than 8,000 requestable entitlements and more than 1,000 requestable roles. A staff of 23 contractors was needed to process 82,000 requests each year. Many new employees were unable to work while waiting for their requests to be fulfilled.

An advanced identity governance solution helped Rockwell Automation achieve its objectives of:

- Automating user provisioning
- Streamlining regulatory compliance
- Providing better visibility into the access assigned to identities

The results included handling 75 percent of the access requests automatically, many through self-service; reassigning most of the contractors to other tasks; and onboarding new employees faster. Savings exceeded $1 million annually. Additional benefits included improving the certification process and revoking permissions much faster when employees left the company.

Strengthen Other Security Technologies

Identity governance solutions can improve the effectiveness of other security technologies. For example:

- ☑ Integration with **privileged account management (PAM)** products improves your ability to monitor privileged user accounts and prevent insider attacks.
- ☑ Integration with **mobile device management (MDM)** products allows you to provision approved apps to mobile devices, control what software can be installed there, require employees to use multi-factor authentication when accessing corporate resources, and even protect data by locking or wiping devices when they are lost or stolen.
- ☑ Integration with **SIEM** systems helps analysts "connect the dots" and separate real attacks from false alerts by correlating identity data across devices and applications, as well as between cloud and on-premises environments.
- ☑ Integration with **data loss prevention (DLP)** software can allow you to enforce very granular policies about what information and documents can be disseminated outside the organization or uploaded to public cloud storage services.

Protecting project breakthrough

Consider this scenario.

Charlie is working on a three-month contract at CompanyX to document the new engineering design system. He finds *projectbreakthrough.docx*, a file describing a major innovation. Charlie thinks it might be nice to FTP this file to his server at home.

Before the file reaches the firewall, the DLP software at CompanyX detects the text string "breakthrough" and recognizes that the file may contain confidential intellectual property. Because the DLP software and the identity governance solution are integrated, the DLP system knows that (a) Charlie is a contractor, and (b) contractors do not have permission to send files containing confidential information outside of the corporate network.

Depending on CompanyX's policy, the DLP software and identity governance solution might take any or all of the following actions:

- Send a warning email to Charlie
- Send a warning email to the security operations center (SOC)
- Block the file transfer
- Suspend Charlie's accounts

Identity Analytics

One of the big pushes in the identity governance world is to add identity analytics capabilities to identity governance solutions. This means giving analysts and administrators tools to slice and dice identity data so they can answer questions like:

- ☑ Which employees and temporary insiders have the most access rights and the most privileged entitlements?
- ☑ Who has substantially more accounts and permissions than others with the same roles and responsibilities?
- ☑ Who has permissions that violate SoD policies?
- ☑ Are some people approving their own access requests, or bypassing approved provisioning processes (for example, administrators who create new accounts directly in applications)?
- ☑ Which business units have the most privileged accounts and the most orphan accounts?

- ☑ How long does it take to revoke permissions when an employee or contractor leaves the organization, and how comprehensive is that process (e.g., does it extend to mobile devices and cloud applications)?

This type of analysis highlights risks, such as individuals with excessive entitlements that they might someday abuse, or that could be used by a hacker who stole their credentials. It can also suggest where and how identity management processes need to be improved.

Chapter 3

Identity Governance in Action

In this chapter

- Learn how identity governance can detect data breaches at different stages of the Lockheed-Martin Cyber Kill Chain®
- Understand how identity governance can help prevent and mitigate data breaches

"It's not enough to know what someone is called. You have to know who they are."

— Gayle Forman

Our discussion so far about identity governance has been somewhat abstract. Now let's look at exactly how identity governance can derail external and internal attacks.

Anatomy of a Data Breach

Lockheed-Martin's Cyber Kill Chain® has provided a useful way of decomposing a complex cyberattack into stages. Although the original model included seven phases, from the perspective of identity governance we can concentrate on four main phases: reconnaissance, infiltration, exploitation, and exfiltration.

You can find the original Intrusion Kill Chain paper on the Lockheed-Martin website. Since the paper was published, experts have suggested a number of updates and revisions. You can see one example in a *Network World* article: Why the 'cyber kill chain' needs an upgrade. Another take on

the model, tailored for identity governance, is provided by Darran Rolls, chief technology officer of SailPoint, in a white paper: The Anatomy of a Data Breach.

Reconnaissance

During the reconnaissance stage, attackers look for vulnerabilities that might give them a beachhead inside the organization's network. They exploit technical weak points, such as web-facing servers with default administrative usernames and passwords, and software packages with known vulnerabilities. Reconnaissance also involves researching information that can be used in social engineering attacks: finding email addresses of employees and business partners, and scouring social media sites to find information about managers and executives for phishing and spear phishing campaigns.[3]

Infiltration

During the infiltration stage, attackers exploit the weaknesses they have discovered in order to penetrate the network. Infiltration involves tactics like gaining access to servers with default credentials, planting malware files on employee laptops and mobile devices, and scanning the organization's systems to locate valuable data.

Exploitation

During the exploitation stage, attackers secure their position inside the network, acquire credentials, and work their way through to high-value targets. A typical sequence of actions might be to:

- ☑ Use malware to download and install hacking tools on the devices
- ☑ Locate servers on the network and test to see if any have default account names and passwords
- ☑ Use malware on a hacked server to run brute force password attacks on Active Directory and on applications used by the organization

3 For a classic example of an attacker doing effective research, see: Omaha's Scoular Co. Loses $17 Million After Spearphishing Attack.

- ☑ Locate orphan accounts and acquire their credentials
- ☑ Acquire credentials from accounts belonging to system administrators and other users with extensive access, (privilege escalation)
- ☑ Create new administrative accounts with access to key systems, applications, databases, and document repositories

Exfiltration

During the exfiltration stage the attackers export the sensitive data and files they have located.

How Identity Governance Defends Against Data Breaches

In each phase of our attack model, identity governance can help mitigate the impact by detecting attacks early, impeding hackers' progress, or even preventing the breach from happening. Figure 3-1 shows how identity governance capabilities come into play at each phase.

Reconnaissance

Good identity governance tools and practices will detect and change default administrative usernames and passwords on web-facing servers, eliminating one major type of weakness that attackers locate during the reconnaissance stage.

Infiltration

Two-factor authentication can prevent attackers from gaining access to applications, even if they have obtained user credentials. While two-factor authentication products fall outside identity governance (as mentioned in Chapter 1), identity governance solutions make them more effective. For example, an identity governance solution can tell the authentication tool: "When executives log on from smartphones outside the network, 'step up' authentication by asking for both a PIN and a fingerprint."

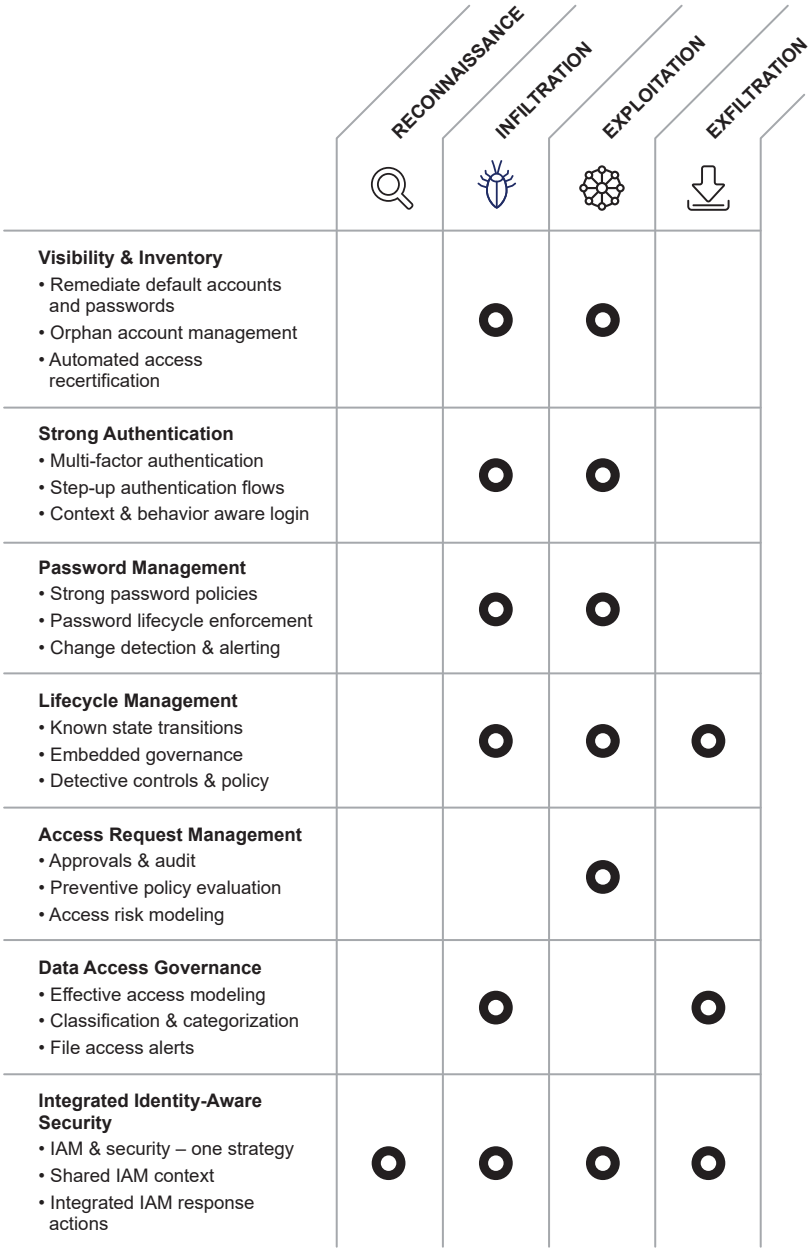

Figure 3-1: How identity governance capabilities map to activities on the kill chain.

Identity governance solutions can also feed identity and policy data to SIEMs and security analytics products to help them detect and block suspicious access requests. This cooperation might generate alerts when, say, someone using a customer service rep's credentials tries to access the engineering design database, or it appears that a sales manager based in Texas is trying to log on from Moldova.

Exploitation

Identity governance solutions can play a major role in preventing lateral movement by attackers during the exploitation stage of a complex attack.

One way is by detecting default usernames and passwords, as well as weak passwords, and helping to enforce strong password policies. These methods make it much harder for attackers to crack passwords using lists of common passwords, dictionaries, and brute force attacks. This reduces the ability of attackers to expand their reach within the network. Also, forcing users to change passwords frequently shortens the window during which attackers can use passwords that have been compromised or purchased on the dark web.

Identity governance solutions can identify existing orphan accounts, and can prevent new ones from being created by revoking access for employees and contractors as soon as they leave the organization.

Certification processes and analyses can remove extraneous permissions, reducing the potential impact of a compromised account. This is particularly important for privileged users, because it can prevent the compromise of one system administrator from giving an attacker direct access to all the systems in the data center.

Identity governance solutions can also detect ongoing attacks by flagging anomalies such as logon attempts from orphan accounts, users who suddenly start creating new administrative accounts, and unusual spikes in activities like creating new accounts and changing passwords.

Exfiltration

Identity governance solutions can also help SIEM, network monitoring, and security analytics products assess whether attackers are trying to exfiltrate data (e.g., by pinpointing large or frequent file exports that are out of character for a person in a given role or location).

Managing Identities Securely and Effectively

In Chapter 1, we referred to statistics from a Verizon report indicating that hackers often exploit legitimate credentials. Identity governance can reduce this risk by eliminating the most common vulnerabilities associated with user access.

Stopping entitlement creep

Identity governance can counteract entitlement creep, a phenomenon caused by practices such as:

- ☑ Giving users more permissions than they need "just in case"
- ☑ Failing to revoke permissions when users change roles
- ☑ Giving everyone in a role new permissions when only one person requests them (i.e., treating one-off access requests as a norm rather than an exception)
- ☑ Giving IT administrators and other privileged users access to all types of applications and servers, in all regions, even though they are responsible only for specific applications or servers in specific locations

Reducing the number of entitlements limits the opportunities of insiders to go rogue, and of cybercriminals and hackers to move laterally inside the data center.

Configure your provisioning system to revoke (or at least flag) orphan accounts when people change roles, as well as when they leave the organization. You can analyze accounts and users to find outliers who have more permissions than others with similar roles and responsibilities. You can also compare different departments, and different locations, to highlight groups that are granting privileges at higher rates than their peers.

Identifying SoD and other policy violations

SoD and other policy violations can very difficult to detect. Identity governance solutions can help find subtle violations that involve:

- ☑ Activities across multiple applications
- ☑ Users who accumulate unusual combinations of privileges by belonging to many account groups or roles
- ☑ Access rights obtained through nested groups (e.g., sales managers automatically obtain the access rights of "corporate managers" as well as of "sales department members")

Controlling temporary insiders

Organizations are giving increasing amounts of access to temporary insiders: contractors, project workers on virtual teams, suppliers, and other types of business partners.

Unfortunately, access for these groups is often managed in a haphazard way. The IT press is full of reports of contractors who access internal systems months or years after ending their engagement, as well as attackers who use suppliers and business partners as an avenue into the networks of major enterprises.

Identity governance solutions can help model the permissions appropriate to different classes of temporary insiders, and also enforce the granting and revocation of accounts through authorized and monitored processes.

In addition, identity governance solutions can enforce mandatory access reviews for contractors every 60 or 90 days, and force re-certifications when contractors leave, to ensure that access is completely revoked.

Monitoring privileged users

Privileged users, particularly IT administrators, have extremely broad powers to perform acts such as creating user accounts and changing system configurations. Identity governance solutions can monitor these actions and flag indicators that privileged users are abusing their positions, or that their credentials have been captured and are being used as part of an attack.

Strengthening Security with Audits and Risk Modeling

We should also note that identity governance audits and risk modeling can play a role in preventing data breaches and ensuring ongoing compliance with regulations. They can:

- ☑ Flag actions taken out of band (outside of authorized processes)
- ☑ Identify trends and spikes in activity that might indicate malicious activity, such as increases in account creations, password changes, and use of privileged accounts
- ☑ Highlight the areas of highest risk, such as users with the most access, so they can be monitored more intensively
- ☑ Strengthen processes for requesting, approving, and certifying permissions, and for modeling roles and policies, thereby helping to eliminate weaknesses that can be exploited by attackers and rogue insiders

Chapter 4

Identity Governance and the Cloud

In this chapter

- Review how identity governance can help enterprises be more secure as they move to the cloud
- Explore the advantages of deploying identity governance solutions in the cloud

"They must often change, who would be constant in happiness or wisdom."

— Confucius

The Cloud-first Enterprise

In Chapter 1 we referenced an estimate that 92 percent of computing workloads will be processed in cloud data centers by 2020. In fact, a growing number of enterprises have adopted a "cloud-first" policy, where they give preference to cloud-based solutions when they are available (although almost all plan to keep at least some infrastructure on the premises for the foreseeable future).

In this chapter we consider how this trend, together with changes in the way we work and emerging technologies, have altered what organizations are seeking in identity governance solutions. We will also examine the option of deploying identity governance solutions as cloud services.

New challenges

Mobile computing, SaaS applications, and cloud storage services create many new challenges for cybersecurity:

- ☑ Managing more types of users including employees, contractors, business partners, and customers
- ☑ Associating multiple devices with each user
- ☑ Provisioning mobile apps when employees join the organization or assume new roles
- ☑ Providing visibility into cloud-based applications and platforms outside of the organization's control
- ☑ Providing information about unstructured data in collaborative apps and storage services such Microsoft Office 365, Google G Suite, Box, and Dropbox.

Provide a single view

Identity governance solutions can provide a single view of identity- and access-related data across all applications and environments, including HR, financial, and other legacy applications in corporate data centers, as well as SaaS and collaborative applications in the cloud. A unified view means that you get a complete picture of the access permissions of each user, and how and when those permissions were granted.

You can also look at the data and determine for each application, and potentially for each document, exactly who has what level of access, and how those rights were granted. Finally, you may be able to reduce software costs by discovering how many people are using specific applications and comparing that number with your licenses.

Create unified processes

Identity governance solutions can ensure that one process is used to request and approve access to both data center and cloud-based applications, ideally through an intuitive online portal. With the right connectors and interfaces, that process can manage the provisioning of access to cloud applications and services, and even to mobile apps for smartphones. A uni-

fied approach is far more efficient and reliable than separate processes for managing access to on-premises and cloud applications.

Enforce policies

Identity governance makes it possible to create and enforce a single set of policies that span legacy and cloud applications. That unification allows you to define policies centrally and to apply them across the enterprise.

An identity governance solution can be especially valuable if it works with MDM products and cloud applications to enforce policies. Working together, these tools can mandate the use of multi-factor authentication on mobile devices, prevent users from granting access to files to anyone outside of the organization, and even suspend user accounts when people violate policies.

Support security analytics

By combining identity data from cloud-based and on-premises applications and data stores, an identity governance solution can do a much better job of detecting risk factors such as orphan accounts in cloud apps, employees with excessive access rights, employees who share documents too widely, and violations of SoD policies. It can also speed up the work of SIEM and security analytics products, for example by establishing that the *jamesjones* storing documents on Google Drive is the same person as *jim.jones* generating events on cloud-based email server and *jjsalesmgr* creating alerts on the main financial system in the data center.

Cloud-based Identity Governance

Advantages

Several cloud-based identity governance offerings (also known as identity-as-a-service solutions) are now available. There are many advantages to subscribing to these services.

These include:

- ☑ Faster time to value, because you don't need to install, configure, and test hardware and software
- ☑ Lower capital expenditures, since you don't have to invest in servers and data center operations
- ☑ Simplified management, because you don't need to manage and upgrade the hardware and software

This model allows enterprises to devote their technical staff to tasks that are more strategic than installing and administering servers and identity governance software.

Customization vs. configuration

IDaaS offerings, like most SaaS products, are not architected to allow extensive customization by individual customers. This can be an issue for organizations that have specialized processes.

On the other hand, cloud-based solutions tend to have easy-to-use interfaces and workflows that reflect industry best practices. Most also provide parameter-based configuration, which allows organizations to tailor processes without the burden of writing and maintaining software code.

Results in two months at Orrstown Bank

Orrstown Bank has almost $1.3 billion in assets and does business through 22 branches in Pennsylvania. It wanted to move quickly on a project to improve regulatory compliance and mitigate risk.

By leveraging a cloud-based identity governance solution, in under two months the bank was able to automate access certifications, password management, and single sign-on for most of their primary applications.

The solution has since been expanded to include over 100 applications. Not only have compliance and security been improved, but the time required to certify access has been reduced by 2,000 hours a year. In addition, users can now change passwords and unlock accounts in self-service mode from mobile devices.

Chapter 5

Building Your Strategic Roadmap

In this chapter

- Learn why it is important to have a strategic roadmap
- Review suggestions about how to assemble a steering group and develop the roadmap
- Explore ideas for training, communication, implementation, and measurement

"People make their own luck by great preparation and good strategy."

— Jack Canfield

A strategic roadmap can help you present to the organization your vision and goals for identity governance. It gives you a vehicle to identify needs and prioritize projects. It can guide you through the initial implementation, and provide a basis for adjusting plans when new opportunities and challenges arise.

In this chapter we give you advice on developing a strategic roadmap. We also explain why activities like training, communication, and measurement should be continued over time.

Assemble the Team(s)

The steering group

Identity governance cuts across every function and every business unit in an enterprise. It is also constantly evolving to support new business initiatives and to respond to new cybersecurity threats. For these reasons, most organizations need a core group that works as a long-term steering committee to assess business needs for identity governance, set priorities, develop a roadmap, build support throughout the organization, measure progress, and periodically update the roadmap.

The steering group should include representatives from:

- ☑ Top management (an executive sponsor)
- ☑ IT management (ideally a CIO or CISO)
- ☑ Security and IT operations teams
- ☑ Legal and audit or compliance staffs
- ☑ Major business units (senior executives)

The steering group needs business knowledge to set priorities and justify programs, as well as technical expertise to understand how identity governance can support various business initiatives and security needs.

The steering group must include an executive sponsor and senior executives who have credibility and clout. These business leaders will play an indispensable role in explaining to managers, supervisors, and employees why their active participation in identity management processes is so important for security and productivity.

The European Union's General Data Protection Regulation (GDPR), which takes effect in 2018, requires enterprises to designate a data protection officer (DPO). The DPO is responsible for ensuring compliance with rules related to privacy and controlled access to personal information. If your organization already has a DPO, you should have that person participate in, or possibly lead, your identity governance steering group.

Project teams

Individual identity governance projects should have their own project teams. In addition to selected members of the steering group, these teams should include:

- ☑ Business managers from the groups directly affected by the project
- ☑ IT administrators and application owners
- ☑ HR managers
- ☑ Helpdesk staffers

People in these roles understand how employees work, what computing resources they need to do their jobs, where they are struggling with identity processes, and the potential impact of the program on security and productivity.

If you have only one identity governance project going at a time, instead of creating separate project teams, you can expand the steering group with appropriate temporary members during the life of each project.

Business accountability

Another reason for having business managers play a major role in the steering group and on project teams is to promote business accountability.

Most managers assume that the IT staff "owns" identity management. Working on identity governance teams exposes them to the reality that only business users and application owners can fully understand what access employees need to do their jobs, and what policies and controls are needed to minimize risk. Help them understand that identity governance will only succeed when business people assume responsibility for managing user privileges and ensuring effective access control in their areas.

Assess Capabilities and Perform a Gap Analysis

To begin developing a strategic roadmap, you should assess your current identity governance solutions and processes, and measure them against desired capabilities.

Weaknesses in identity governance processes

Identify weaknesses in your current identity governance processes. Clues include:

- ☑ Processes that are manual, error-prone, and costly to administer
- ☑ Long wait times to provision and de-provision employees and contractors
- ☑ High volumes of service requests to technical support to provide access to resources and reset passwords
- ☑ High costs to prepare for audits, and failed audits
- ☑ Large numbers of orphan accounts, evidence of overentitled users, and accounts created outside of authorized processes
- ☑ Managers "rubber stamping" access and certification requests without considering real access requirements
- ☑ Inconsistencies across business units and geographies, indicating inadequate tools or poor training in some of them

Business initiatives

Determine if upcoming business initiatives will place demands on identity governance solutions. Is the enterprise integrating its supply chain? Making greater use of contractors and virtual teams? Expanding into new product markets or geographies? Making acquisitions and integrating the acquired companies into existing processes? Will existing identity governance tools and processes slow down any of these initiatives, and can they ensure adequate security?

IT projects

What requirements will be placed on identity governance solutions by planned IT projects, such as deploying mobile applications and making increased use of SaaS applications? Do new security analytics or incident response tools require identity information, and if so, are current systems able to provide complete, accurate data?

Build Business Cases

After you assess the weaknesses in your current identity governance solutions and determine requirements for upcoming business initiatives and IT projects, you are in a position to build business cases for individual projects. This boils down to estimating the value of each project, minus the cost of implementing and managing the solution.

In identity governance, most of the justification will come from four areas.

Reduced operational costs

Estimate the value of improvements such as:

- ☑ Automating processes for requesting, approving, and provisioning access rights
- ☑ Reducing technical support calls related to access issues and password resets
- ☑ Speeding up and simplifying certification processes
- ☑ Speeding up and simplifying audits

Improved employee productivity

Calculate the time savings for employees related to:

- ☑ Streamlining onboarding and provisioning
- ☑ Accelerating approval of new access requests
- ☑ Enabling employees to use self-service portals to request changes and resolve issues themselves

Reduced security risk

Project the probable decrease in the annualized loss expectancy (ALE)[4] from data breaches resulting from:

- ☑ Fewer orphan accounts, overentitled users, and accounts created outside of authorized processes
- ☑ Faster deprovisioning of terminated employees and contractors
- ☑ Stronger and better-protected passwords
- ☑ Accurate and granular enforcement of security policies by MDM, DLP, and other security tools
- ☑ Faster detection and more accurate analysis of attacks by SIEMs and security analytics products
- ☑ Consistent operation of identity governance processes across business units and geographies

Faster delivery of value from business initiatives

Solid identity governance solutions can accelerate the roll out of business initiatives and IT projects. For example, they can make management more confident that it is safe to integrate business partners and virtual team members into corporate processes, and to allow employees to use more cloud-based services. You can approximate this benefit using cost of delay methodologies.

A SailPoint white paper offers detailed advice on justifying identity governance projects. You can obtain a copy at: Building a Business Case for Identity & Access Management. This note from industry analyst firm Gartner is a bit dated, but it includes useful suggestions on how to relate identity management to top business and technology priorities.

4 The ALE is the probability of a breach during one year multiplied by the likely cost of the breach.

Create the Roadmap

Communicate your vision

Your roadmap should show when major identity governance projects will be started and completed, looking out 18 to 24 months. It should communicate your vision and business direction for identity management, and inform the organization when new capabilities will be available.

Plan to deliver value early and often

The project business cases you have built are important input for your roadmap, because they show which projects have the greatest potential benefits. However, when it comes to sequencing projects, you should consider applying Agile principles. In particular:

- ☑ Break projects down into increments that allow you to deliver value early, demonstrate initial successes, and build momentum (see the *How to avoid big bang projects* text box, below).
- ☑ Inspect and adapt: at regular intervals, solicit feedback, evaluate progress, and adjust the roadmap based on lessons learned and changed business needs.

How to avoid "big bang" projects

Many IT projects fail when organizations take a "big bang" approach, trying to roll out comprehensive, feature-rich solutions across the entire enterprise in one long process. It can take months or years to add features, configure workflows, set up accounts, and train hundreds of users. During that time the organization receives little or no value from the project, raising the risk that it will be cancelled due to lack of results.

There are several ways to break up mega-projects so they can begin producing value early, and so that organizations can learn from and build on the initial iterations:

- Launch a project in one business unit or geographical area, and gradually roll it out to additional locations
- Begin with a base set of features, and gradually add functionality that users need (but not bells and whistles that may have been available in the past but don't produce real value)
- At first integrate with a limited number of data sources and applications, and then gradually add new connectors

Train and Communicate

Identity governance solutions affect managers on a regular basis, and touch almost every employee. Yet in most organizations, very few people outside of IT have any appreciation for the importance of identity governance. Not surprisingly, they also have little patience for using identity governance tools the way they were designed. For these reasons, training and communications need to be a central part of your organization's identity governance strategy.

Training

Consider providing training at three levels:

- ☑ Everyone in your organization needs to understand its policies related to identity governance, their own responsibilities for following approved procedures, and the possible consequences of ignoring or circumventing the rules.
- ☑ Managers and supervisors need to be trained on how to use the organization's tools for requesting and approving access, and for reviewing and certifying entitlements.
- ☑ Security and IT operations staff need training on identity governance tools, and how to work with managers and employees to ensure that policies and procedures are followed.

Do not focus identity governance training only on "*how to*." It must give equal emphasis to "*why*." Employees, managers, and even IT staff should understand why it is important to use strong passwords, resist the temptation to approve access rights "just in case they might be needed someday," pay close attention to certifications, and refrain from circumventing standard processes and creating unneeded superuser accounts.

Training is available from identity governance solutions vendors and consultants. There is even an organization that offers courses for a security professional to become a Certified Identity and Access Manager (CIAM)®. However, for employee training, you should consider developing your own instructors, or creating custom online courses.

Communication

Build a communication plan into your roadmap. Communication serves to:

- ☑ Let people know what to expect
- ☑ Reinforce training
- ☑ Increase acceptance and enthusiasm by promoting identity governance successes inside the organization and at peer enterprises

Don't think of communication as a one-time task to announce your identity governance strategy. It should be an ongoing program to build awareness and active participation over the long haul.

Consider communication in broad terms. It's fine to start with an official announcement and an article in the company newsletter. But how about creating a message forum on your internal portal to keep people informed? Could you send e-postcards or start a blog to give advice and communicate progress? Is there a file share or wiki where you could post materials so employees and managers can educate themselves and find success stories? Why not be creative and produce videos that dramatize the need for data security and identity governance?

Implement and Measure

We mentioned earlier that you should break projects down into segments so you can deliver value early, demonstrate initial successes, build momentum, and adjust the roadmap based on lessons learned from the initial efforts. To do this successfully, you need to measure progress and solicit feedback.

Measurement should be tied to the business cases you developed as part of the strategic roadmap. For example:

- ☑ If you justified projects based on reduced operational costs, then measure savings from automating processes, reducing technical support calls, speeding up certifications, and simplifying audits.
- ☑ If you justified projects based on employee productivity, then measure times required to onboard new employees and approve access requests, and track the percentage of requests handled through self-service.
- ☑ If you justified projects based on security, then measure the reduction in orphan accounts, the speed and completeness of deprovisioning, and the reduction in security events detected.

You can also track employee and manager satisfaction with identity-related processes. This exercise will give you early warning signals if user confusion or apathy are threatening the success of your programs. It will also give you valuable information on how to refine and improve your identity governance solutions and processes.

To optimize the value of user input, combine online surveys, which are fast, inexpensive ways to reach large audiences, with selective one-on-one interviews that go into depth. Another technique is to create "user councils" so you can obtain employee feedback throughout a project.

Maintain the Momentum

An identity governance strategic roadmap should plan explicitly for the long term by allocating resources for:

- ☑ Ongoing planning, training, communication, and measurement
- ☑ Upgrades to the software tools and integration with new applications
- ☑ Support for new business initiatives and IT projects currently on the horizon, or as yet unknown

Chapter 6

Selecting the Right Partners

In this chapter

- Explore criteria for selecting strategy and technology partners

"In the long history of humankind…those who learned to collaborate and improvise most effectively have prevailed."

— Charles Darwin

Throughout this guide we have emphasized how identity governance processes touch every employee and every part of the organization. They have major impacts on security, operational costs, and employee productivity. They also need to evolve to support new business and technology initiatives: mobile applications, cloud computing, and unstructured data today; the Internet of Things and advanced analytics very soon; and as-yet-unknown projects coming down the pike.

To meet these challenges, you want to work with strategy and technology partners that not only satisfy your requirements today, but can be allies over the long haul. In this chapter we outline some of the criteria for selecting those partners.

Relevant Experience

Strategy partners

A strategy partner can help you:

- ☑ Assess current capabilities and weaknesses
- ☑ Develop a strategic plan and roadmap
- ☑ Build acceptance for identity governance projects at managerial and lower levels
- ☑ Update the roadmap as new opportunities and challenges emerge

The ideal strategy partner will have experience helping organizations in your industry that are operating at the same scale as yours and facing the same challenges. You should also look for firms that have demonstrated both strategic vision in identity governance and skills to guide the implementation of individual projects.

Technology partners

When you evaluate technology partners such as software vendors, you obviously want to find solutions that meet your immediate requirements for features and functions. But also keep these considerations in mind:

- ☑ Does the vendor have experience with organizations in your industry, operating at the same scale as you do?
- ☑ Can you single-source multiple elements of identity governance from one vendor (so you don't need to integrate solutions from several parties)?
- ☑ Does the vendor have a good track record of upgrading technologies and extending identity governance to new areas?
- ☑ Does the vendor offer strong support and professional services that you can call upon when you need help or short-term resources?

See if the vendor has an active users group. A vibrant customer community is a sign of long-term viability, as well as a source of information and support for new customers.

An Open Identity Platform

In Chapters 2 and 4 we discussed how identity governance solutions need to acquire data from all of the organization's directories, applications, and repositories of unstructured data, as well as cloud platforms, so they can create a comprehensive view of users and permissions.

Because integration provides so much value, identity governance solutions should be built on an "open identity platform"; that is, a structure that facilitates connecting to systems that contain identity information and interface with cybersecurity technologies. Attributes include:

- ☑ Out-of-the-box connectors to directories and applications
- ☑ Interfaces to file shares, on-premises storage networks, cloud-based file storage services, and other repositories of unstructured data
- ☑ Integration with other identity management tools, such as authentication, single sign-on, PAM, and GRC products
- ☑ Integration with MDM, DLP, SIEM, and security analytics tools you have in your organization today or might want to work with in the future
- ☑ Integration with service management and technical support ticketing systems you use to handle access requests and issues

Also, because new applications and security technologies come along every year, the open identity platform should include a framework and tools for creating new connectors. The platform should offer the ability to leverage APIs and identity-related standards such as LDAP, SAML, and SCIM. It might also provide agents that can be configured quickly for new data sources, or agentless technology that makes it easier to deploy new connectors.

Consistency Across Environments

You may have noticed that:

- ☑ Employees expect the same access to computing resources, regardless of where applications run.
- ☑ Auditors demand that all data access meets corporate policies, regardless of where the data is stored.
- ☑ Managers want a single system for requesting and approving access.
- ☑ Administrators prefer one tool to provision access to data center, cloud, and mobile applications.
- ☑ Analysts need to correlate identity and event data from all directories, applications, and systems in the enterprise.

To satisfy all these audiences, look for identity governance solutions that use one set of interfaces, processes, enforcement mechanisms, and analytics tools across data center, cloud, and mobile environments.

Coverage of Unstructured Data

Today, many cybercriminals and rogue insiders target unstructured data, including documents, spreadsheets, slide presentations, software and product design files, email and text messages, and social media posts. These can contain credit card and Social Security numbers, business secrets and intellectual property, and sensitive personal information.

Look for identity governance solutions that can extend monitoring and policy enforcement to repositories of unstructured data, including:

- ☑ Cloud storage services
- ☑ Email servers and online collaboration portals
- ☑ File shares and storage networks

Through connectors and APIs, the system might track:

- ☑ Who created and owns files and folders
- ☑ Who has permissions to access each file and folder

- ☑ What sharing is enabled for each (e.g., "private," "share with people you invite," "anyone with the link can view," "anyone with the link can edit")
- ☑ Who has accessed each file and folder

This data can alert you to risks and policy violations, identify files and folders that require special monitoring, and help you improve policies and processes for storing and accessing unstructured data.

Business-friendly Interfaces

We have mentioned several times how critical it is to gain the active participation of non-technical business people in identity governance activities. Only business users and application owners can fully understand both access requirements and access-related risks. You are going to rely on business managers to certify access rights and rigorously reduce unnecessary permissions.

To encourage the participation of business people, you should find identity governance solutions that:

- ☑ Have intuitive and easy-to-use interfaces suitable for non-technical users
- ☑ Use business-friendly terminology and concepts, without jargon or cryptic system and network names
- ☑ Provide features that address real-world conditions (e.g., allow managers to delegate approval authority if they are busy, and send email reminders when managers fail to respond within a specified period)

Analytics and Risk Management

Security analytics and risk management can improve incident response and help organizations detect weaknesses in their security infrastructure and practices. You should seek identity governance solutions that capture comprehensive identity-related data from across the enterprise, then correlate the data to identify policy violations and reveal vulnerabilities, such as employees with too many permissions, and access rights created outside of authorized processes.

Some vendors are working on identity governance solutions that capture and correlate event data (log-on attempts, file downloads), calculate baseline levels for these events, and flag departures from the baselines. They will also be able to feed risk scores for users and transactions to risk management and fraud detection platforms.

A Cloud Strategy

As we discussed in Chapter 4, identity governance solutions should help you migrate applications to the cloud safely. Your technology partners should have a strategy for integrating with a wide range of cloud-based applications and services. Also, you might want to give preference to vendors that offer some or all components of identity management as cloud-based services (IDaaS), or better yet, provide options for hybrid solutions with some elements deployed on premises and others in the cloud.

Final Thoughts

We started this guide by pointing out that most data breaches and unauthorized insider activities involve the misuse of user credentials. Identity governance solutions are designed to minimize these abuses by ensuring that permissions to access computing resources are assigned and controlled based on explicit organizational policies.

To achieve these goals you need sophisticated technology and the active participation of business managers, employees, and technologists. We have highlighted the importance of developing an identity strategy and roadmap that pull in resources from many parts of the business to generate early wins, build momentum, and evolve to meet changing business and technical needs. We have also made suggestions about criteria to use in selecting strategy and technology partners to help you move forward.

Please share these ideas (and this guide) with your colleagues as a basis for discussion about how identity governance principles and practices can be applied in your environment. Then, when you have started to implement your strategy, share the results with your professional community, so we can learn from one another.

Organizations today face greater challenges and risks than ever before.

Do you know the path forward?

Hackers today are choosing a new attack vector of choice – enterprise users. With potentially millions of exposure points from thousands of users and hundreds of apps, putting identity at the center ensures that your users have the right access to the right applications and data at the right time – and nothing more. In this book, learn how identity governance can mitigate, and even prevent, data breaches, improve productivity, increase security and compliance, and then how your organization can continue down the path in the right way:

- **Review the basics of identity governance and why it is central to enterprises today.**
- **Discover the capabilities of identity governance solutions today and how they provide visibility and control over structured and unstructured data.**
- **Examine how identity governance helps enterprises mitigate data breaches, adopt new technologies like the cloud and be empowered to chase opportunities.**
- **Explore how enterprises can be more agile, while also meeting compliance needs in an efficient – and provable – way with identity governance.**
- **Learn how to build a strategic roadmap that captures your organization's vision and goals for identity governance.**
- **Find out how to choose the right strategy and technology partners to make your identity governance program a success.**

About the Author

Jon Friedman is a managing consultant at CyberEdge Group, a premier research and marketing consulting firm serving the needs of high-tech vendors and service providers. Jon has more than 20 years' experience in industry analysis and marketing, working with more than 40 software, computer, and IT services companies. He has a BA from Yale and an MBA from Harvard.

CYBEREDGE PRESS

Not for resale

ISBN 978-0-9961827-7-5