Consider this hypothetical scenario:
While inspecting a hotel construction site in London, Malcolm noticed that smaller, more expensive beams than what was originally identified in the blueprint were about to be installed. Pulling out his tablet, he quickly accessed engineering drawings from company headquarters in San Francisco to confirm the correct size. Malcolm then initiated a videoconference with the design team in Chicago to discuss the issue, looping in the structural steel provider in Jakarta to access financial information that detailed material costs. Within a matter of minutes, the potentially dangerous deviation from the plans was remedied and work resumed.

A few months earlier, such responsiveness would not have been possible, as the IT systems of Malcolm’s company lacked a holistic identity and data management (IDM) strategy. Malcolm would have been unable to access the project blueprints. In addition, he would not have been able to confirm the correct beam size and costs, due to disparate and disconnected identity directories across two companies. What’s worse, his inability to quickly access the needed information from the steel company would have likely resulted in a poorly constructed hotel—many thousands of dollars over budget.

In the era of digital transformation—where the number of IP addresses, users and data sets is expanding at a breakneck pace—IDM is essential to strategic security programs to protect and control continuously shifting assets needed in business enablement initiatives. IDM – encompasses the people, processes and technology for creating, managing, authenticating, controlling and removing a user’s permissions. It also defines the process by which data is classified, protected and accessed throughout an organization—by its employees, contractors, affiliates, partners and customers. IDM is the key to controlling and extending access to organizational resources and data to customers, partners, employees and other relevant parties.

Digital business initiatives, such as the one undertaken by Malcolm’s company, focus on improving partner and customer engagement by providing them access to online resources. Employees such as Malcolm must have rapid access to corporate data and applications to collaborate effectively. The use of mobile devices by customers, partners and employees is extending the perimeter, which must be defended. No longer limited to the physical confines of a building, the network edge is wherever users happen to be—in a coffee shop, hotel room, or airport—anywhere in the world.

The most successful IDM deployments integrate IDM infrastructure and tools with enterprise cybersecurity technologies. The ability to correctly identify users, their privileges and sensitive data across multiple security technologies enables the correct access levels to be granted in real time. Successful IDM deployments also encompass data classification and governance. The ability of an IDM systems to create detailed records of access history is critical not only to improve security but also to generate reports for regulatory compliance audits.

Challenges to IDM deployment
Despite the strategic importance of enterprise IDM, organizations face challenges in deploying comprehensive IDM implementations. Over time, many organizations have deployed Identity and Access Management on a tactical basis. Although beneficial in a limited context, a patchwork of ad hoc identity and access technologies can prove unwieldy to manage and can miss the bigger picture. The use of disparate and decentralized IDM products requires that each product be separately deployed, updated and managed, resulting in additional time and expense.
Many legacy tactical implementations are not only expensive to update and maintain but are also not designed to meet emerging requirements. Digital businesses, and their mobile users, require real-time access to online resources across hybrid cloud- and premises-based IT environments. These solutions often have difficult administrative interfaces and user interfaces that don’t meet the needs of today’s end users and customers.

A widespread skills shortage also creates significant obstacles for organizations seeking to strategically deploy IDM. Many organizations aiming to hire IT professionals with deep knowledge of the latest IDM technologies are simply unable to find them. If those skilled individuals can be found, corporate budget pressures may prevent them from being hired or retained through pay increases and bonuses. Other organizations attempt to build their own IDM resources by taking Java developers, database administrators, or individuals from the security field and repurposing them for IDM. This approach can have mixed results, depending on the support and formalized training provided to these people.

Together, these challenges often appear so daunting that implementation of a comprehensive IDM strategy is impeded. As a result, many organizations suffer from IDM implementations that are far from optimized, leaving them to bear the burden of unnecessary costs even as their sensitive data remains vulnerable, and their business users must jump through security hoops that may not be appropriate or risk-based.

**Strategic IDM**

**WHAT IT IS**

A strategic and holistic approach to IDM includes the following elements:

- **Identity data management**—The control and management of identity-related data, the systems that house the data and how the data is processed across the organization.
- **Identity management**—The core user life cycle and self-service management of end-user accounts, administration and entitlements.
- **Access management**—The support of authentication mechanisms, including single sign-on, multifactor authentication, federation and password management.
- **Access governance**—The policy-based activities that enable the definition, enforcement, review and auditing of IDM functions and policy compliance.
- **Privileged access management**—The support of processes and technology controls related to elevated permission accounts.
- **Data security and analytics**—The ability to manage unstructured data, providing data classification, identification and user analytics to support data security programs.

**WHAT IT DOES**

Strategic IDM delivers a host of benefits to organizations:

- **Enables digital transformation**—By providing for secure wired and wireless access to IT systems across hybrid on-premises and cloud environments, organizations can deploy applications that encourage more intimate customer engagement as well as richer collaboration among employees.
- **Streamlines authentication**—Centralized access management incorporates single sign-on and federated identity technologies, which eliminate the need for multiple user IDs and passwords.
- **Improves the ability to meet compliance requirements**—Promptly obtaining information and generating reports is essential to alleviating the burden of compliance. Centralized reporting enables rapid and stress-free compliance practices and audit performance.
- **Generates greater brand awareness and consumer loyalty**—Improving the customer experience by removing the hurdle of cumbersome IDM technology generates repeat customer visits and improves word-of-mouth reputation.

Standards and regulatory guidelines such as the Payment Card Industry Data Security Standard (PCI-DSS), in organizations storing or transmitting credit card information; Health Information Portability and Accountability Act (HIPAA), in healthcare; and the General Data Protection Regulation (GDPR), for organizations handling the data of European citizens, mandates significant penalties for noncompliance. In the face of these challenges, organizations must develop comprehensive and effective security strategies.
• **Supports zero-trust initiatives**—The strategy of treating everyone accessing corporate systems as untrusted is a proven approach to strengthening data security. Zero-trust is particularly effective in securing sensitive assets in organizations that have embraced workforce mobility, since mobile users might require access to online resources anywhere, anytime, from any device.

• **Enables organizations to gain operational efficiencies**—Centralized access management and user life cycle administration increase the efficiency of IT security staff. Eliminating a patchwork of legacy IDM implementations lowers costs by simplifying licensing and eliminating redundant management tasks.

**HOW TO DEPLOY IT**

The IT leaders responsible for IDM should deploy it with a structured approach, beginning with a detailed assessment of current environments, including pain points, challenges and red flags. Because the analysis, prioritization and scope of holistic IDM can be daunting, IT leaders should not hesitate to seek the assistance of skilled professionals who thoroughly understand IDM technologies and business requirements.

Working with an expert partner such as Optiv, IT leaders can develop a strategic IDM roadmap that clearly sets forth each step that is to be taken. Rather than replacing existing cybersecurity and IDM technologies entirely, organizations should develop an integration roadmap and implementation plan that aligns current goals with existing investments where possible. The roadmap should include both short- and long-term goals as well as iterative milestones along the path toward a fully mature IDM program. In this effort, the identity-centric framework developed by the Identity Defined Security Alliance (IDSA) is recommended.

**Conclusion**

As workloads are migrated to the cloud and the enterprise workforce becomes mobile worldwide, organizations face new challenges in protecting data. In this context, IDM is the key foundational technology for securing information assets.

Piecemeal IDM implementations, however, can leave security gaps and lead to unnecessary complexity and expense. Ad hoc and legacy implementations should be evaluated and optimized or replaced where necessary by technology built according to a holistic and strategic vision for identity governance and administration across the enterprise. Optiv recommends that a strategic IDM program include these key elements:

- Identity data management
- Identity management
- Access management
- Access governance
- Privileged access management
- Data security and analytics

To be assured of executive- and board-level support, strategic IDM should be aligned and integrated with other enterprise governance and security initiatives.

Because of the strategic nature of an enterprise IDM deployment and the difficulty of finding individuals with the required skills, a partner with expertise and experience in the full range of IDM technologies is necessary. The partner should provide people, processes and technology encompassing these areas:

- Strategic consulting services
- Implementation assistance
- Governance expertise
- Managed security services
- Certified expert advisors
- Best-of-breed technologies

Optiv engages with clients as a trusted cybersecurity advisor, providing expert consultants, advanced technology and key partnerships and applying deep knowledge of IDM technologies to the needs of organizations across all industries. Optiv strategic IDM implementations mitigate the risk of breaches, help meet expanding compliance mandates and enable digital transformation.

**CREDENTIALS: The Weakest Link**

Control of user permissions and access to data are of the utmost importance in keeping data secure. Research has found that loss, theft, and weakness of credentials are the leading causes of breaches. Consider:

- **81%** of hacking-related breaches have leveraged stolen and/or weak passwords.¹
- **60%** of internal data breaches are caused by privilege abuse, where internal actors misuse their level of granted access.²
- **76%** of IT professionals say their organization experienced the loss or theft of company data over the past two years—and the leading cause was insider negligence.³

¹Verizon’s “2017 Data Breach Investigations Report (DBIR).”
²Ibid.
Optiv Empowers Enterprises to Achieve Strategic IDM Programs

Optiv takes a strategic and holistic approach to IDM. Clients gain the comprehensive expertise of more than 1,000 Optiv IDM advisors and delivery experts, plus the capabilities of Optiv partners in multiple areas.

**Workshops and assessments.** The first step in developing both short- and long-term road maps for IDM is to fully understand the current environment, including security challenges. Optiv offers one- and two-day workshops that enable participants to align IDM initiatives with business goals and implement best practices that incorporate people, processes, and technology.

**Implementation.** Through partnerships with leading IDM vendors, Optiv assists organizations with deployment of single sign-on, federation, password management, life cycle management, identity governance, data access governance, and privileged access management. Partners include:

- Cyberark
- BeyondTrust
- Bomgar Lieberman Software
- Saviynt
- SailPoint
- SecureAuth
- Ping Identity
- Okta
- Varonis
- STEALTHbits

**Governance.** Optiv provides oversight of the entire IDM program, from implementation through optimization, growth, and the transition to next-generation IDM.

**Managed IDM.** Optiv extends the security team with IDM experts to manage and monitor critical IDM infrastructure.

**Optiv technology**

**Point solutions and integrations** that create one cybersecurity fabric

- Ping Identity Integration Kits: SiteMinder, Axiomatics, HitachiID, Netskope
- RSA SecureID Suite Integration Kits: CyberArk, Microsoft Office 365

**Tools and technologies** that help migrate legacy IDM technologies to next-gen environments, protecting existing investments

- Legacy web access management migration to PingAccess (including Oracle Access Manager and SiteMinder)

**Extensions and enhancements** of commercial off-the-shelf technologies to meet unique needs

- RSA SecureID Access Manager and L6G Custom Integration and Extensions
- Unix Access Governance Tool

**Advanced technologies.** User and entity behavior analytics (UEBA), machine learning, and AI technologies observe and learn from everyday user conduct to spot anomalies in normal behavior patterns that could signal hacker intrusions or other illegal activity.

**New approaches.** The Identity Defined Security Alliance (IDSA), founded by Ping Identity in conjunction with Optiv, takes an identity-centric approach to security. This proactive strategy leverages the intelligence relating to users and their transactions that is inherent in IT infrastructure to improve the processes of authenticating, authorizing, and managing users.

The Optiv Identity Centric Security Strategy Workshop and Identity Centric Security Integration solutions are designed for organizations that are ready to extend their IDM investments through integration with existing cybersecurity technologies, based on the work of the IDSA.

**Post-implementation services.** Access to expert solutions advisors and staff augmentation are available wherever needed.

For more information, visit [www.optiv.com](http://www.optiv.com).