User Lifecycle Management Proves Costly to IT

IDG survey reveals that manual processes drain productivity and increase security risks

IT departments are struggling with time-intensive onboarding and offboarding processes, according to a recent survey of IT leaders at companies with more than 500 employees. This effort saps budgets and productivity while increasing security risks.

Managing access to enterprise applications is a manually intensive process for most IT organizations. Indeed, 100% of the U.S. respondents to an IDG Research Services survey on this topic said the user lifecycle process is very or somewhat time-intensive. On average, IT departments are committing more than 30 combined staff hours per week to managing user systems, devices, and application access. For companies with more than 2,500 workers, it takes 34 hours on average, with some respondents indicating that these tasks soak up 60 hours or more. With end user IT support salaries averaging more than $50,000 a year and HR-related onboarding expenses estimated at $4,000 per worker, the costs can add up quickly

Organizations rely largely on email, support tickets, and spreadsheets to manage user provisioning and deprovisioning. In the age of cloud-first IT, companies are quickly adding new applications, often hiring more workers, and dealing with employee churn, all of which adds up to a growing onboarding and offboarding burden. This further complicates the process of managing access needs, which can change as users are promoted, take on new roles, or adopt and drop various software tools.

Relying on manual processes can lead to prolonged project timelines. Furthermore, it may slow the enterprise's ability to adopt the best-of-breed cloud apps that end users need in order to do their best work.

Often IT is dealing with issues outside of its control. While IT is on the receiving end of requests from HR and end users to create accounts and assign permissions and licenses, a business app owner must grant access and create new employee accounts or notify IT that a departing or transferred user's access should be curtailed or modified. The result is frustration all around.

Risk factors

As a user's lifecycle state changes, it may trigger various necessary actions to ensure that access to resources stays compliant with business and security policies. When users leave an organization, failure to quickly offboard their identity and access can create significant security gaps and risks.

Survey respondents reported that it takes an average of two full days to deactivate a departing employee's access to relevant accounts. Respondents from companies with 2,500 or more workers said that it takes an average of 50 hours. Moreover, 42% indicated that they need more than two days, with some saying five or more.

During that period, disgruntled former employees could potentially duplicate intellectual property, tamper with records or systems, or compromise confidential customer or employee data. International Business Times reported in June 2017 that a Dutch web hosting company had suffered a catastrophic outage when an ex-administrator allegedly deleted customer data and wiped most of its services. Similarly, the publication reported that an ex-employee of Allegro Microsystems had accessed company systems to insert a "malware time bomb" in 2016 that deleted information from a financial database.

Besides facing risks of fraud and tampering, enterprises may increasingly find themselves out of compliance with government requirements involving identity management. "Regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley and HIPAA hold organizations accountable for controlling access to customer and employee information," observes CSO. The publication points out that State of New York Department of Financial Services regulations "prescribe many requirements for the security operations of financial services companies that operate in New York, including the need to monitor the activities of authorized users and maintain audit logs."

Further adding to compliance issues, U.S. companies that collect personally identifiable information (PII) in European Union countries will be subject to the new General Data Protection Regulation (GDPR), which takes effect in May 2018. Although the overall thrust of the regulation is protection of PII, it will have a vast impact on how companies manage access to that data by employees.

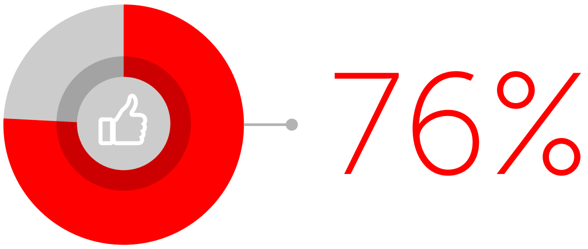
The full impact of GDPR won't be known until enforcement begins, but error-prone manual processes and lack of visibility into access rights could be costly. For example, it would be a compliance violation if employees who have access to PII in one role subsequently shift to another role in which there is no business need for such access. Such violations may result in hefty fines, which can be assessed at up to $20 million. Those fines could dwarf the costs of increasingly frequent data breaches, which the Ponemon Institute estimates costs U.S. companies $7.3 million on average per breach.

Automating the lifecycle

As companies grow, there are more manual tasks to perform throughout each employee's lifecycle. These tasks take time and are prone to error, delaying end user access to accounts and applications. The proliferation of part-time workers, contractors, vendors, and distributed partner networks—each with unique lifecycles—poses a huge hurdle for access management and compliance.

As workers join, move within, or leave a company, keeping everything in sync becomes a tedious ongoing task with multiple stakeholders. If every user has multiple profiles in multiple apps and directories, it can be challenging to manage user attributes and resolve issues when they arise.

It should be no surprise then that 76% of the survey respondents indicated that they would experience improved IT productivity by streamlining and automating lifecycle management. More than half indicated that automation would improve security.



of the survey respondents indicated that they would experience **improved IT productivity by streamlining and automating lifecycle management.**

Traditional identity governance and administration systems are complicated, taking too long to deploy. As a result, they tend to be implemented for only one or two critical applications and rarely deliver the ROI originally anticipated.

By centralizing and automating lifecycle management across all apps on-premises and in the cloud, IT can provide users and their devices instant access to the applications they need. Access can be shut off as soon as that need no longer exists. Meanwhile, the IT team can realize significant management cost improvements, along with greater productivity.

Managing identities

More than ever, enterprises must be in full control of the user lifecycle. Okta Lifecycle Management enables organizations to build an end-to-end map of who has access to which services and to understand how frequently they're being used. Based on group membership, role, and business need, it automatically removes access to applications containing PII.

Okta helps enterprises better manage user lifecycle management issues, with a cloud-based solution for provisioning and deprovisioning—for cloud as well as on-premises applications—with policies, workflows, and reporting for the members of an organization's ever-shifting workforce and their devices.

For more information, visit Okta's website.