Devolutions

Does Your Organization Have a Strategy for Employee Departures?

THE AVERAGE WORKER WILL EXPERIENCE 12 JOB CHANGES DURING THEIR CAREER

Until a few decades ago, it was common for people to spend their entire career working for a single employer — often starting from the bottom and working their way up through the ranks until retiring. How things have changed!

These days, the average worker will experience 12 job changes during their career. What's more, millions of workers are planning on switching employers in the aftermath of the pandemic, a mass turnover phenomenon that human resource experts have dubbed "turnover tsunami." However, this mass migration is not just a recruiting and retention risk. It is also a security threat.

1 in 4 Ex-Employees Have Access to Old Accounts

In a recent survey, 25 percent of workers said they could still access accounts from past jobs — including former IT staff and managers who had the proverbial "keys to the kingdom" (i.e., access to privileged accounts).

Granted, most of these former employees have not "gone rogue," and they do not intend to steal data, wreak havoc, or carry out any other illicit activities. But what if these individuals are attacked by hackers who, in the course of their snooping, discover these old accounts and their associated credentials? Then the consequences could be severe, if not catastrophic. According to IBM Security's 2021 Cost of a Data Breach Report, data breaches now cost organizations a whopping $4.24 million per incident on average — which is the highest cost in the 17-year history of the report.

The Solution: A Strategy for Employee Departures

In many organizations, when an employee leaves (voluntarily or involuntarily), the focus is on retrieving assets. For example, an employee is told to return their corporate-supplied laptop, smartphone, client files, building access card, and so on. Obviously, asset retrieval is a core part of the termination process — but it is not the full picture.

As part of a comprehensive strategy for dealing with employee departures, it is also extremely important to enforce an access deprovisioning process that should include the following:

1. Immediately Change the Employee's Password

The first and most important step is to change the employee's password, so that they (or someone on their behalf, operating with their permission or otherwise) cannot access their old account(s).

2. Disable Access to All Accounts

There are two options for removing employee access: deleting accounts and locking accounts. Deleting accounts is preferred, since this eliminates the possibility of future access. However, there may be situations where it is necessary to preserve accounts if they contain valuable data, such as important files, correspondence, etc. In that case, organizations should lock accounts until the data can be safely and properly archived elsewhere (after which the accounts can be deleted).

3. Change Passwords on Shared Privileged Accounts

Thycotic's State of Privileged Access Management Maturity report revealed that over 50% of organizations' privileged account passwords never get deprovisioned. This is an enormous vulnerability, since it means that ex-employees — or hackers who infiltrate them — could still access these shared accounts. To close this security gap, organizations should change the credentials for any privileged accounts that were shared with a former employee. These accounts include any that provide elevated user rights, as well as:

- Domain Administrator Accounts
- Local Administrator Accounts
- Emergency Access Accounts
- Application Accounts
- System Accounts
- Domain Service Accounts

How Devolutions Can Help

Devolutions helps organizations manage their strategy for employee departures in a few important ways:

- Both **Remote Desktop Manager** and **Devolutions Server** enable organizations to keep track of all employee accounts in a centralized location, so that it is clear which accounts need to be deleted and/or locked when an employee leaves.
- **Devolutions Server** and **Password Hub Business** feature built-in account brokering functionality. This enables employees to access accounts (including privileged accounts) without ever seeing passwords. As such, when an employee leaves the organization there is no risk that they will be able to access the old account(s) — because they never knew the password in the first place. Learn more about the advantages of account brokering here.
- In **Password Hub Business**, there is no need to chase down an ex-employee to get their login credentials for their user vault (i.e., the password and confidential data repository that was only accessible to that employee). Instead, authorized IT staff can access the user vault of any current or former employee — learn more about this process here.

The Bottom Line

There is nothing new about employees leaving organizations. However, what is going to change — and we are already seeing signs of this now — is the staggering volume of people in all sectors and industries who will be switching jobs in the coming months and years.

Organizations that have a robust strategy for handling employee departures that is supported by effective tools will reduce their exposure to data leaks and breaches — and increase their chances of surviving the oncoming "turnover tsunami."