cloudbridge
uc_clearly;

EMPLOYEE EXITS…
3 MISTAKES THAT PUT YOUR DATA AT RISK

ABSTRACT
How to avoid data loss when employees leave. A review of the risks associated with an employee exit and the steps to prevent data loss.

KEVIN FOISY
kfoisy@ucclearly.com

QUICK FACTS

According to a Biscom survey:

- More than 1 in 4 respondents say they took data when leaving a company.
- 15% of respondents said they are more likely to take company data if they are forced out of their job (fired or laid off), rather than leaving on their own.
- Of those who take company data, 85% report they take material they have created themselves and don't feel this is wrong.
- While a majority take their own documents, 25% of respondents report taking data that they did not create.
- 95% of respondents said that this was possible because either their company did not have policies or technology to prevent data stealing, or that if companies did have policies in place, they ignored them.

EMPLOYEE EXIT = RISK

When people leave an organization, the organization incurs risk on multiple fronts. To mitigate that risk, organizations typically walk a person out the door. While this is a necessary precaution, few organizations do the equivalent for the digital identity.

Most business executives consider data to be their most important asset and loss of that data can lead to costly damages including:

- Risk of regulatory violation
- Legal actions
- Competitive disadvantages
- Revenue loss

CLOUD = NEW RISKS

In the pre-cloud era, this risk was somewhat mitigated by escorting the person to the door and disabling their primary login. While this left many potential risks, the corporate network perimeter offered a barrier. In the cloud era, this barrier is gone. Systems are completely exposed to anyone from anywhere. Consider for example, an employee that has shared OneDrive folders with their Gmail account for easy access. "This happens all the time" says, Jason Siegrest, VP of IT, Nuvolo. In cases like this, the physical person has exited but their digital identity is still authorized. With organizations adopting dozens of cloud applications, this becomes a very serious security risk.

BYOD CREATES ENTITLEMENT

To further complicate matters, the BYOD movement creates a sense of entitlement among employees, "It's my computer", where they feel they own the computer and hence the data on it.

MISTAKE #1 – YOU'RE DEPROVISIONING MANUALLY

Most small to medium sized organizations de-provision users manually. When HR sends the signal, IT begins disabling access to systems. This must be carefully orchestrated with each of the application owners. This process is manual, slow, and has a high risk of leaving doors open. Many employees report that they have access to systems long after they leave a company.

Larger organizations deprovision using identity systems. HR will either instruct IT of a person's departure, or in more automated systems, the HR software triggers the identity system to begin a deprovisioning. These systems cover many applications and lead to companies feeling that they have this problem resolved. However, a deeper dive reveals that this is not the case.

MISTAKE #2 – YOU'RE NOT LOOKING AT THE DATA

Whether it's a manual deprovisioning or an automated one, the process usually goes only as deep as the identity login. What happens when there's another way to access the data? With many applications, the employee can unlock the backdoor without the application owner's knowledge. An example is OneDrive or SharePoint where the user may have granted their personal email access to data.

DAG MEETS IDENTITY

Data Access Governance tools allow organizations to peer into unstructured data permissions. They can see where people have excessive permissions. This is used to help reduce the risk of over-exposed data. The challenge is that DAG systems go very wide with a goal of being able to identify all data that a person has access to. These large scans are slow.

Now consider the case where a person discovers that they are about to be let go. If they decide they want to take data, they simply enable access to an external account and access it after they leave. Timeliness is the problem here. The enablement and theft are too close in the timeline for DAG to help. This risk is compounded by any delays in deprovisioning user access.

Some organizations have policies that restrict this type of behavior, but cloud application disparity leads to a lack of centralized management; these policies are seldom enforceable.

MISTAKE #3 - YOU'RE NOT TERMINATING ACTIVE SESSIONS

Did you know that when an employee is terminated, they often retain access to their email for several hours? Even though you might have disabled their account, they retain cached access, and this often remains for up to 3 hours. It is possible to force-close their active sessions, but it requires a visit into the O365 admin portal or a PowerShell script. Since this is just another manual step, it's often overlooked and results in data risk.

CONCLUSION - A BETTER DEPROVISIONING PROCESS IS NEEDED

To protect an organizations data during an employee exit, IT staff must examine each application and the associated data.

- The user's primary corporate account should be disabled, and password reset
- Access should be disabled for all applications
- Current sessions should be terminated to prevent cached access
- All user devices should be wiped of any corporate data
- Any application that allows non-corporate account access should be reviewed for potential backdoor access
- Unstructured data permissions should be reviewed, and permissions removed
- Data ownership should be reassigned to a manager or replacement staff
- The user's calendar should be cleaned of any shared, owned meetings
- A litigation hold should be put on the owner's mailbox and as needed, converted to a shared mailbox
- Assigned licenses should be recovered
- An audit trail should be produced and shared with all relevant stakeholders

Following these guidelines will help ensure that an employee exit is a safe exit; the organization's data does not accompany the employee. The deprovisioning process can be a time consuming, labor intensive task. Since timeliness and accuracy is of great concern to prevent damage, automation of these tasks is highly recommended.

ABOUT CLOUDBRIDGE

Cloudbridge's solutions re-imagine IT management. By enabling true automation, we empower organizations to reduce their security exposure, reduce their operational costs and embrace new technologies in ways that empower their business.

cloudbridge
uc_clearly;

555 Legget Drive
Suite 304, Kanata, ON
K2K 2X3

info@ucclearly.com
+1 (613) 867 7177
www.cloudbridgeplatform.com