THE RISKS OF USER ACCESS COMPLACENCY

COMMON PROBLEMS WITH ACCESS PROGRAMS AND HOW TO RESOLVE THEM

By Shane O'Donnell

((CENTRIC))

EXECUTIVE SUMMARY

Why should you as a CIO, CISO, CAE, or in any leadership role, care about the details of user access reviews?

"We do them, we're fine," most say.

From the outside, it may appear that user access is running smoothly, terminated employees are removed swiftly and new users receive the correct level of access to the correct system. But start peeling back the layers and you find there are many levels of user access that aren't being considered. In our experience, this is the case more than 75% of the time.

Can you confidently answer the question: Who has access to what? And can that question be answered for every critical system, database and device throughout your company? Is the appropriate person completing routine reviews of detailed access reports? As much as it hurts to admit it, reality must set in – the answer is likely no.

Critical assets and information often become vulnerable due to inaccurate access. User access is inherently risky due to frequent change and the human factor. People can unconsciously make a mistake or intentionally be malicious.

If given more access than required for their job duties, the risk is much higher than necessary. While the growing complexity of access management is contributing to that heightened risk, so is the widespread complacency in managing user access.

Consequently, if your company is not conducting proper access reviews on a consistent basis, risks increase, including a terminated employee or terminated employee of a contractor could gain access to the network remotely, send reputation-damaging emails, or process fraudulent transactions.

If an employee moves to a new department and previous access is not removed, the employee changing jobs could create segregation-of-duty conflicts. There's also the potential for abuse of dormant admin accounts.

> *"By limiting user access to what is needed for the job, you can reduce the amount of damage a single employee or disgruntled ex-employee can cause as well as how far an intruder can get if an employee is compromised."*
>
> *- SHANE O'DONNELL*

USER ACCESS REVIEWS

User access reviews are critical to safeguarding your organization – and should include reviews of every level. Start by gathering a list of critical systems and applications. Then, obtain a list of every user with access to each system and exactly what each user has access to see or perform. These reviews should be led by someone at a management level, but close enough to know who the users are and what type of access is appropriate for their specific job duties.

User access reviews should be performed on a routine basis, such as quarterly or monthly. The frequency depends on the size and complexity of your company along with the criticality of each system or application being reviewed.

Access reviews should include all types of users, including dormant and disabled accounts, accounts with passwords that do not expire or that have not been changed within the past year, remote access, system administrators, and "power users."

The process of obtaining all user access and security information in an understandable format can be difficult for some systems. The initial step to creating a proper user access review process is to ensure there exists a complete and accurate listing of every IT system or application used at the company.

USER ACCESS REVIEWS (CONTINUED)

Information technology professionals and developers are the user groups with the highest risk because these users typically have the most unrestricted access to more systems than any other user. Because of this, they can cause the most damage.

An employee who does not have a system administration role for each IT system should perform a review to ensure that excessive privileges are not assigned to users and that hidden accounts have not been created that could be used for illicit activities.

Another high-risk user group is third-party vendors. Vendors come and go from a business environment and often need access to the systems to do the job for which they were hired. There is a higher risk for this type of user not to be terminated at the end of the contractual relationship. Often vendors are given remote access, so even if they are not onsite, they can access the network.

Another often ignored, yet critical, topic is privileged access. Privileged access provides users with the keys to the castle, so to speak, since they can make behind-the-scenes system changes. Therefore, reviews of this type of access should occur more often. In fact, this type of access should be considered separately from typical users.

FALSE SENSE OF SECURITY

Your company may have a robust onboarding and offboarding policy, with procedures that look great on paper, but how are they being carried out? For example, when a new employee is hired and the hiring manager requests system access, do they simply ask for the access to be mirrored off another current employee, or are they forced to look at the details of the access they are requesting to ensure it is appropriate for a new employee?

Often, managers will request that the new employee be given the same access as another employee in the same department but, without a proper routine access review program, how can you be sure that the current employee doesn't have more access than required? What if that employee moved from another department and the old access was not removed? Not only do you have the original employee with too much access but, if that employee is being used as a guide for new employees, the problem will continue to grow. If an auditor found this, it could easily result in a significant deficiency for the company.

For employees who are involuntarily terminated, it is especially important to remove their access in a timely fashion. This situation creates a higher level of risk, as terminated employees may be more likely to act with malicious intent. Therefore, you should terminate as close as possible to the employment termination date.

CASE STUDIES

UPDATE TERMINATION CHECKLISTS

A large global public company had a false sense of security about terminated employee access because it routinely used a thorough termination checklist. However, once our auditors peeled away another layer of the onion, we found that while the checklist was helpful, it hadn't been reviewed or updated for many years.

Because it had been years since the checklist had been updated, some systems were not included. Therefore, terminated employees still could access these systems after leaving the company. They could share their login information with someone who still was employed at the company, so transactions could be conducted without knowing for certain who performed them.

REVISIT KEY CONTROLS

Another client, a rather large company, had been Sarbanes-Oxley (SOX) compliant for years with no significant deficiencies. Management assumed that SOX testing would find something as simple as user access issues. However, many key controls in place for SOX had not been revisited in years.

Once again, something that appeared fine on the outside revealed a problem once the layers were peeled away. The technology around user access and access reviews has changed so much, and automation has become such a constant process, that companies must revisit the controls related to that technology and make the necessary adjustments. Revisiting key controls every so often, especially those controls related to user access, should become routine.

IMPLEMENT ROUTINE USER ACCESS REVIEWS

This last example involves a multi-billion-dollar private U.S.-based firm that had a robust onboarding and offboarding process that was frequently tested for MAR requirements. However, the process didn't consider job changes. Employees would change jobs and receive new or additional access, but the access required to complete their prior role wasn't removed. This created many opportunities for fraud, as many employees ended up with access that created segregation-of-duties issues.

Once the proper level of management implemented and examined the results of routine access reviews, it was able to find and remove this additional inappropriate access. The company subsequently created appropriate procedures for job changes, but who knows when it would have found the problem if it hadn't conducted a thorough user access review.

HOW TO AVOID USER ACCESS COMPLACENCY

CRITICAL APPLICATIONS

Have you checked if the information is complete and correct? How do you know?

You will find that while SOX critical applications may have proper access and access reviews, what about other applications that may be critical to operations, but not necessarily appear on the financial statements? You should apply the same controls to those applications.

TRUSTED SOURCES OF INFORMATION

How do you know that the user listings used for the access reviews are complete and accurate? Where are these reports coming from?

It is not uncommon for companies to perform user access reviews with user listings that are not complete and accurate. If you're performing a review with a report that is not complete and accurate, then you are wasting your time. Ensure that user listings are complete, accurate and contain the necessary information for management to understand the distinct types of access.

HOW TO AVOID USER ACCESS COMPLACENCY
(CONTINUED)

ROLE DEFINITIONS

Do you know what each role in each system is allowing access to a user?

You should provide the person requesting access and the person doing the access review with a role definition. Most roles are either a few words or use a cryptic naming standard. By providing a definition with each role, you ensure the user knows what they are requesting and the reviewer knows what they are approving.

ACCESS REVIEWS

Who is performing the access reviews?

Those performing the reviews must be in a position of authority, and they must know enough about a user's job responsibilities to know what kind of access that user should or shouldn't have for a particular application. One departmental employee may require read/write access to all modules within an application, while another employee in the same department may only require access to one or two modules. It is important to provide only the access that is necessary to complete job duties. If a manager too high up the chain reviews the user listings, he or she may not have the knowledge at this level of detail to make the proper access determination. The same issue arises if someone in the IT department is performing these reviews.

ABOUT THE AUTHOR

Shane O'Donnell | Vice President
Cybersecurity Practice

Shane brings over 20 years of experience in audit and cyber risk. Most recently, he served as the Chief Audit Executive for The Mako Group, a cyber risk management firm acquired by Centric Consulting. There, he led projects with large healthcare, manufacturer and financial organizations. In previous roles, he worked extensively with Sarbanes-Oxley (SOX) testing and program development for Fortune 500 companies. Shane assisted organizations with streamlining internal audit processes, reducing redundant activities and identifying deficiencies.

Want to keep your brand reputation and financial impact safe? Our Cybersecurity team can help address your security concerns.

Talk to an expert

((CENTRIC))

ABOUT US

Centric Consulting is an international management consulting firm with unmatched expertise in business transformation, AI strategy, cyber risk management, technology implementation and adoption. Founded in 1999 with a remote workforce, the company has established a reputation for solving its clients' toughest problems, delivering tailored solutions, and bringing in deeply experienced consultants centered on what's best for your business. In every project, you get a trusted advisor averaging over 15 years of experience and the best talent from across the United States and India. Centric deliberately builds teams that can scale up or down quickly based on client needs, industry and desired outcome.

Headquartered in Ohio, with 1,400 employees and 14 locations, Centric has been honored over the years with over 100 awards for its commitment to employees, clients and communities. Most recently, it was recognized by Forbes, for the eighth consecutive year, as one of America's Best Management Consulting Firms.

Visit http://www.centricconsulting.com to learn more.