Enhancing Privacy and Security through Robust Access Management

Access management controls are a key part of data governance and cybersecurity. These controls determine who is able to access data and system resources (like specific software or computing capabilities). Effective access management has two complementary goals. It allows staff to work effectively by ensuring they have access to the tools and data they need, without relying on inefficient or insecure workarounds like account sharing. At the same time, limiting data and resource access to only those verified users who need it can lower the chances of an external data breach (because most data breaches involve human error, limiting access limits risk) or other forms of external cyber attacks and helps prevent internal unauthorized access to data and systems.

Forms of Access Management

There are a number of common forms or methods for managing access that bring with them a number of tradeoffs.

- **Role-Based Access Control (RBAC)** and **Attribute-Based Access Control (ABAC)**: RBAC and ABAC systems offer the ability to make access to documents or data contingent upon the role of an employee, or attribute of the employee or document or data, respectively. For instance, a role of "principal" could allow an individual to view all teacher evaluations on that school's system. Attributes can provide finer-grained controls, so for example a system could have a "teacher" role with a "3rd grade" attribute, which could enable them to view all student assignments with a "3rd grade" attribute. Attributes may also allow for things like time-limited access, so, for instance, a "substitute teacher" role could be supplemented with a date-range attribute to ensure the sub only has access to student information while they are currently teaching.

  True RBAC systems rely solely on roles, which makes them easier to maintain, but less flexible than ABAC systems. An RBAC approach can be well suited to contexts where several staff have the exact same level of access, such as registrar staff who all have access to, for instance, all student contact information and schedules. In contexts where more granularity is needed, ABAC systems can be useful. For example, it might be useful for a school to have a universal teacher role so that all teachers can see information like an employee handbook or grade submission schedules. However, the "teacher" role is not nuanced enough to ensure that teachers can only access assignments and grades for their own students. Adding grade or class attributes to the teacher role can allow for both generalized and specific access.

- **Access Control Lists (ACL)**: ACLs are simply lists of authorized users attached to each dataset and resource. This is a very flexible system as it allows essentially any access configuration; however, it is also complex to maintain and error-prone as each resource needs its own list, those lists need to be maintained individually, and it is easy for access lists to fall out of date.

Which approach an organization takes to access management depends on their structure and needs. Small organizations with limited data and staff may find that ACL is sufficient (though they may need to reevaluate if they expand), while large organizations with robust technical support may find that the benefits of ABAC are worth the time and expertise required. Many organizations end up using a combination of approaches to suit their needs, which can be useful but may also be difficult to maintain or introduce unexpected corner cases.

Best Practices for Access Management

There are a number of best practices that make access control systems easier to maintain and more effective from a security standpoint.

- **Implement a single sign-on (SSO) system**: SSO systems, which allow users to access different systems using the same account credentials, can be expensive to procure or deploy, but they provide a number of benefits for security and access management. For one, the central management can make the system easier to provision and maintain. Users only need to be assigned roles one time, which will carry over into every system that uses the SSO. For another, SSO can minimize user errors and workarounds. If users only need to remember one set of credentials, they may be able to use a stronger password without needing to regularly restore access (which can be an attack vector). Additionally, the central management offered by SSO systems can make auditing and maintenance of accounts simpler, as when staff leave or change emails, the information only needs to be updated in one place.

- **Clearly define and document roles and attributes**: Using clearly defined and well-documented roles and attributes helps to ensure that roles are consistent across different systems and, in larger organizations, across different departments or units. This makes the system easier to understand and maintain, which helps ensure that it is functioning as needed to secure data while still allowing users to do their jobs effectively. Additionally, documenting and defining roles is important when ensuring that systems are interoperable. For example, if a learning management system has an “experiencing homlessness” tag for records of unhoused students to allow a benefits coordinator to access those records, but the record archiving system does not have a comparable tag, it becomes unclear which records the coordinator should have access to, potentially leading to a breach or making it harder for the coordinator to do their job effectively. Clear definitions ensure that systems behave in consistent and expected ways.

- **Update and audit access**: It is important to regularly conduct checks to ensure the access management system is working as intended. This means reviewing access as a regular occurrence, and updating access as needed.

    - There are a number of events that should trigger an update to the access management system:

        - *Employee arrivals.* When new employees arrive, system administrators will need to provide them with the access they need. This may mean adding them to lists in an ACL system, or ensuring that their role is correct in RBAC or ABAC systems. Additionally, if another employee has been granted access to resources in order to fill the role temporarily, it may be necessary to revoke their access (though, depending on how the role transition is managed, it may make sense to keep this temporary access for a grace period to ensure proper handover).

        - *Employee departures.* When an employee leaves the organization, it is critical that their access be revoked as soon as possible, so this should be a standard part of any off-boarding process. If another employee will be covering the departing employee’s role, the covering employee should be granted access so that they do not have to rely on workarounds, which can be difficult to secure or document.

        - *Role transfers.* When employees transfer to new roles, their access should be updated to match. As with temporary role coverage though, it may make sense to allow a handover period before revoking access they will not need in their role, to ensure that the duties are passed over smoothly.

        - *Student class transfers.* When students transfer classes, any access to their materials should be reviewed to ensure that they are only available to those staff who are still involved in the student’s education.

  - In addition to updating access upon trigger events, organizations should also conduct regular audits of their access management system. This could mean reviewing access at the end of every semester or quarter to ensure that the roles and attributes are assigned as expected. Additionally, asking users to verify their account by logging in to ensure they are still active system users can avoid unnecessary risk in the form of dormant accounts. Reviewing email addresses to ensure that people are using their official accounts to access records rather than personal accounts can help ensure system compliance. These regular audits can help catch and remediate errors before they cause issues and ensure that any updates that were not captured by a trigger event are made.

Access management is a critical component of securing systems and data, and protecting an organization and the community it serves. By selecting an appropriate access management framework and following best practices, organizations can strengthen their cybersecurity and governance frameworks.

Further Reading

- https://nces.ed.gov/pubs98/safetech/chapter8.asp
- https://resources.infosecinstitute.com/certification/access-control-models-and-methods
- https://westoahu.hawaii.edu/cyber/best-practices/best-practices-weekly-summaries/access-control/
- https://csrc.nist.gov/publications/detail/nistir/7316/final
- https://csrc.nist.gov/projects/access-control-policy-tool
- https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/controls?version=5.1&family=AC

This is one in a series of information sheets designed to give practitioners clear, actionable guidance on how to most responsibly use technology in support of students. More info: cdt.org/student-privacy/.