Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *Who caused this incident? A user called Legal\Administrator (Robert Taylor Jr.)* ● *When did it occur? 10/03/2023 at 8:29:57 AM* ● *What device was used? A computer called Up2-NoGud with IP address 152.207.255.255*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have? Admin* ● *Should their account be active? No* ● *The organization failed to revoke admin access from employees who are no longer employed by the company: Lei Chu, Robert Taylor Jr., and Joanne Phelps. Additionally, employees with different roles are all given admin level access. By the principle of least privilege, each*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help? The organization should implement managerial controls such as policies that require user deprovisioning upon separation of employment and policies that limit administrator level access to full-time employees with a business need for that level of access. Contractors should not be granted admin*

		employee should only have the level of access necessary to perform their role, and by the principle of separation of duties, no employee should have been given a level of access that would enable them to misuse the system, which administrator access does allow them all to do.	*access. Technical controls that the company could implement include automated audits of login attempts that deactivate access for users who have not accessed the system within a certain time period, preventing individuals who no longer need access to systems from continuing to have access. Role-based access control should be implemented.*

Access control issue(s):

- Robert Taylor, Jr. is a contractor with admin access.
- His contract ended in 2019, but his account accessed payroll systems in 2023.

Oftentimes, incidents like this occur because systems are misconfigured or misused. That is the case with how this business is sharing information among its employees.

Recommendations:

- User accounts should expire after 30 days.
- Contractors should have limited access to business resources.
- Enable multi-factor authentication (MFA).

It appears as though a former employee is potentially the threat actor. However, it's possible that they were not the person responsible for this security incident.

It is common for people to reuse login credentials across many services. And if those credentials are compromised on one platform then an attacker can use them to gain access to others. In this case, implementing access controls, like password policies, limited file permissions, and MFA can protect the business from incidents like this.