REPORT Investigation of Unauthorized Payroll Access Incident

v1.2.0

Author:

Eldon Gabriel

July 10, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/12/2025	Eldon G.	Initial draft.
v1.0.1	02/15/2025	Eldon G.	Refined the report for clarity, added recommendations, and improved structure.
v1.1.0	02/16/2025	Eldon G.	Changed report title to "REPORT - Investigation of Unauthorized Payroll Access Incident", updated section title to "OBSERVATIONS", and added table blocks for section separation.
v1.2.0	07/10/2025	Eldon G.	Added full section headers, numbering, and conclusion.

SECTION 1.0: UNAUTHORIZED PAYROLL ACCESS INVESTIGATION

1.1 Project Description

As the company's first cybersecurity hire, I was tasked with investigating a serious incident involving an unauthorized payroll transaction. This incident put the company at financial risk and highlighted problems with how access and accounts were managed.

1.2 Incident Overview

A payroll deposit was initiated to an unknown bank account. The finance manager confirmed that no authorized action was taken. Fortunately, the transaction was halted before funds were released. An access log review revealed that the payroll system was accessed by a former legal contractor, **Robert Taylor Jr.**, whose **administrator account** was still active despite his contract ending in **2019**. This access occurred on **October 3, 2023, at 8:29:57 AM** from the IP address **152.207.255.255**.

SECTION 2.0: INVESTIGATION

2.1 Access Log Findings

- **User:** Robert Taylor Jr.
- **Role:** Former Legal Contractor (Administrator account)
- **Access Timestamp:** October 3, 2023 – 08:29:57 AM
- **IP Address:** 152.207.255.255
- **Device Name:** Up2-NoGud

The credentials of a former contractor were used to attempt the unauthorized payroll action. This incident was made possible due to the failure to deactivate user accounts post-contract termination.

SECTION 3.0 OBSERVATIONS

Category	**Observation**
Account Retention	*The contractor's admin account remained active years after contract expiration.*
Access Anomaly	*The login attempt originated from an unknown external IP and an unauthorized device.*
Policy Failure	*No automated or manual deactivation process was in place for offboarded users.*

SECTION 4.0: RECOMMENDATIONS

4.1 Access Control Improvements

- **Implement Automatic Account Expiration:** Set expiration dates for contractor accounts (e.g., 30 days post-termination).
- **Limit Contractor Access:** Apply the principle of least privilege. Avoid assigning administrative roles to temporary staff unless business-critical.
- **Enforce Multi-Factor Authentication (MFA):** Require MFA for all privileged accounts to stop unauthorized logins even if credentials leak.
- **Conduct Regular Account Audits:** Review user accounts every three months to identify and remove those that are no longer needed or belong to former workers.

SECTION 5.0: CONCLUSION

5.1 Key Takeaways

- A former contractor's active account enabled an unauthorized payroll access attempt.
- Lack of formal offboarding and access controls created a long-term security gap.
- The incident was mitigated without financial impact due to timely detection.

5.2 Security Implications and Recommendations

- Failure to enforce access expiration policies directly increases the risk of insider and residual threats.
- MFA, automated account lifecycle management, and regular audits are essential to maintaining secure identity access management.
- This case reinforces the need for strict enforcement of cybersecurity hygiene, especially during employee and contractor offboarding.