Activity details:

Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn't make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents.

To do this, you'll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

Table1

Name	Role	Email	IP address	Status	Authorization	Last access	Start date	End date
Lisa Lawrence	Office manager	l.lawrence@erems.net	118.119.20.150	Full-time	Admin	12:27:19 pm (0 minutes ago)	10/1/2019	N/A
Jesse Pena	Graphic designer	j.pena@erems.net	186.125.232.66	Part-time	Admin	4:55:05 pm (1 day ago)	11/16/2020	N/A
Catherine Martin	Sales associate	catherine_M@erems....	247.168.184.57	Full-time	Admin	12:17:34 am (10 minutes ago)	10/1/2019	N/A
Jyoti Patil	Account manager	j.patil@erems.net	159.250.146.63	Full-time	Admin	10:03:08 am (2 hours ago)	10/1/2019	N/A
Joanne Phelps	Sales associate	j_phelps123@erems....	249.57.94.27	Seasonal	Admin	1:24:57 pm (2 years ago)	11/16/2020	1/31/2020
Ariel Olson	Owner	a.olson@erems.net	19.7.235.151	Full-time	Admin	12:24:41 pm (4 minutes ago)	8/1/2019	N/A
Robert Taylor Jr.	Legal attorney	rt.jr@erems.net	152.207.255.255	Contractor	Admin	8:29:57 am (5 days ago)	9/4/2019	12/27/2019
Amanda Pearson	Manufacturer	amandap987@erems...	101.225.113.171	Contractor	Admin	6:24:19 pm (3 months ago)	8/5/2019	N/A
George Harris	Security analyst	georgeharris@erems....	70.188.129.105	Full-time	Admin	05:05:22 pm (1 day ago)	1/24/2022	N/A
Lei Chu	Marketing	lei.chu@erems.net	53.49.27.117	Part-time	Admin	3:05:00 pm (2 days ago)	11/16/2020	1/31/2020

Event Type: Information
Event Source: AdsmEmployeeService
Event Category: None
Event ID: 1227
Date: 10/03/2023
Time: 8:29:57 AM
User: Legal\Administrator
Computer: Up2-NoGud
IP: 152.207.255.255
Description:
Payroll event added. FAUX_BANK

Access controls worksheet

Authorization /authentication		
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?* • *When did it occur?* • *What device was used?*	**Objective:** Based on your notes, list 1-2 authorization issues: • *What level of access did the user have?* • *Should their account be active?*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: • *Which technical, operational, or managerial controls could help?*
Who caused the incident? Legal\Administrator Robert Taylor Jr. Legal attorney Contractor **When did it occur?** Date: 10/03/2023 Time: 8:29:57 AM	**Level of Access they had?** Admin **Should their account be active?** No, because they had left organisation	**Key Security Issues:** 1. All employees have access to the level of an admin. 2. Principle of least privilege is not followed 3. Destruction of account data and employee account is also important to make it difficult for ex employees to access their accounts an misuse them 4. Separation of duties looks weak since the legal department can access financial details from finance department **Mitigation Steps:** 1. Principle of least privilege must be implemented by providing access only on need basis.

Authorization /authentication		
What device was used? 152.207.255.255 Computer: Up2-NoGud		2. After employees leave their employee account must be deleted so as not to be misused. 3. Principle of Separation of duties must be implemented and sales team or legal team must not be able to access financial departments information 4. Audit logs can be maintained to detect unauthorised access sooner. 5. Multi Factor authentication - this helps anyone pretending to be someone else go through the process of verification through more than one before providing access to them 6. Role Based Access Control (RBAC) - to ensure users only have access to the systems and data necessary for their roles