**Scenario:** You're the first cybersecurity professional hired by a growing business.

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.

Payment Info:

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

Employee Directory:

| 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.net | 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.net | 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.net | 101.225.113.171 | Contractor | Admin | 6:24:19 pm (3 months ago) | 8/5/2019 | N/A |
| George Harris | Security analyst | georgeharris@erems.net | 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 |

# Access controls worksheet

| | Note(s) | Issue(s) | Recommendation(s) |
|---|---|---|---|
| **Authorization /authentication** | **Objective:** Make 1-2 notes of information that can help identify the threat:<br>• *The event took place on 10/03/23.*<br>• *The user is Legal/Administrator.*<br>• *The IP address of the computer used to login is 152.207.255.255.* | **Objective:** Based on your notes, list 1-2 authorization issues:<br>• *Robert Taylor Jr is an admin.*<br>• *His contract ended in 2019, but his account accessed payroll systems in 2023.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:<br>• *User accounts should expire after 30 days.*<br>• *Contractors should have limited access to business resources.*<br>• *Enable 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.

This activity highlights how easy it can be to lose track of users, which can leave a business open to unnecessary risk if effective access controls are not in place. The activity also demonstrates the risk of operating a business with open, shared access to resources. Setting boundaries around who can access information and what they are allowed to do should be the starting point of any security plan.