## Access controls worksheet by Don Wickramanayake

Scenario

Review the scenario below. Then complete the step-by-step instructions.

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.

Supporting Resource: Accounting Exercise

|  |  |
| --- | --- |
|  | |
| 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 | | | |  |  | |  |  |  |  |  |  |
|  | |  | | | |  |  | |  |  |  |  |  |  |
|  |
| **me** | **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 |
|  |  | |  |  |  | | |  | | | | | | |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **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?*   *Robert Taylor Jr. Legal Attorney*   * *When did it occur?*   *Robert Taylor Jr. who was a contractor (no longer with the company) accessed the systems to do a money transfer (payroll activity) to an outside account. It occurred on 10/03/2024*   * *What device was used?*   *Device with the IP address 152.207.255.255. It was the assigned computer for Robert Taylor Jr.* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?*   *User had Admin level access.*   * *Should their account be active?*   *Their account should not be active as he was no longer working for the company. His contract with the company ended on 12/27/2019. Unauthorized money transfer happened on 10/03/2023 with the payroll system.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   *Should have been used the least privilege principle and separation of duties principle. As a contractor he should not have admin access to the system. And when he was leaving his account should have been deactivated.*  *There suppose to be MFA enabled for user access.*  *User accounts should be expire in certain time period.* |