Access Controls Assessment

Improving Authentication, Authorization, and Accounting for a Small Business

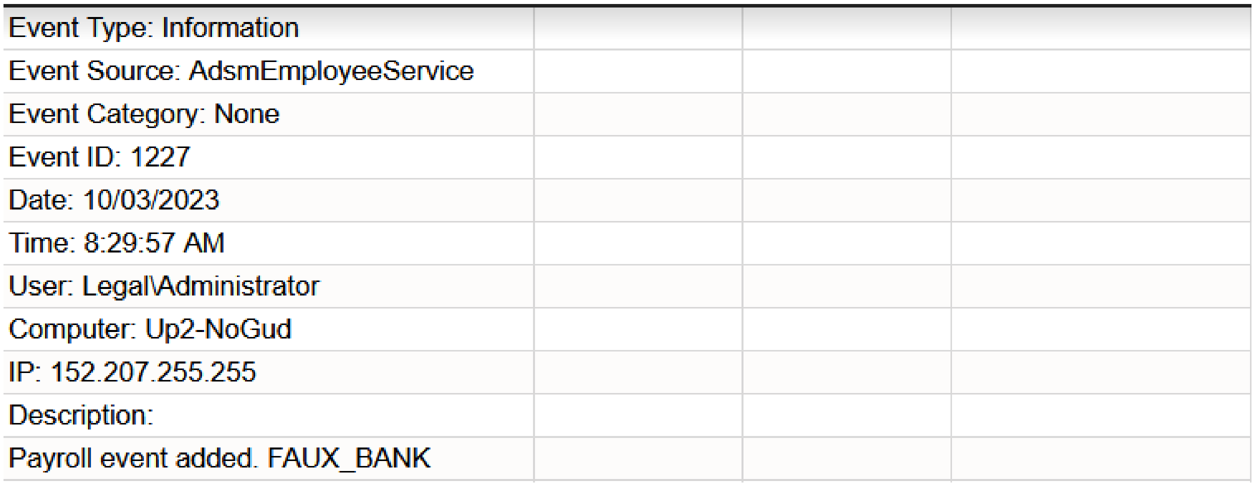
Wendy Alayon
03/07/2024 **@syszern**

Access controls assessment

Scenario

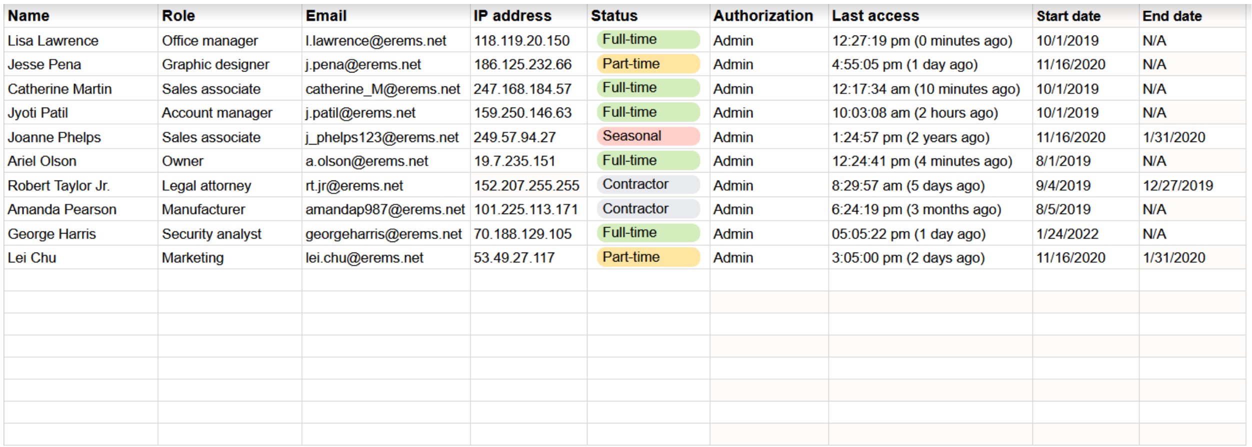
The newly hired cybersecurity professional at a growing business encountered a recent incident where a deposit was made from the business to an unknown bank account. The finance manager confirmed that no mistakes were made on their part. Fortunately, the payment was successfully stopped. The business owner requested an investigation to prevent any future incidents.

The cybersecurity professional commenced the investigation by conducting an accounting of the incident to gain a better understanding of the events. The initial step involved reviewing the access log related to the incident. This was followed by taking notes to help identify a possible threat actor. The professional then identified issues with the access controls that were exploited by the user. Finally, recommendations were made to improve the business's access controls and reduce the likelihood of a recurrence of such incidents.



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			

Fig. 1. *Event log*



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

Fig. 2. *Employee directory*

Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	• *The event took place on 10/03/23.* • *The user is Legal/Administrator.* • *The IP address of the computer used to login is 152.207.255.255.*	• *Robert Taylor Jr is an admin.* • *His contract ended in 2019, but his account accessed payroll systems in 2023.*	• *User accounts should expire after 30 days.* • *Contractors should have limited access to business resources.* • *Enable MFA.*