Part 1.

Explain the security risks this behavior introduces.

* Tailgating creates a Security Risk due to non-employees walking in.
* Encourages backdoor access to confidential financial data & other countless potential risks.

Describe a method for finding out how many people encourage tailgating, and keeping track of those who do.

* At main access points and post a Security Guard to stand at the door and ensure one employee enters at a time and they have a Company ID badge and can be scanned in.

Set a goal for how many employees should engage in this behavior.

* No employees should be allowed to hold the door for anyone else. As this is an Accessibility, Integrity, & Confidentiality issue.

Identify three potential "high level" solutions to this problem—e.g., via training, hiring guards, etc. Document one advantage and disadvantage for each.

* Random monthly physical penetration testing, the pen-testing company hired threat actors having them hold the door for an outsider. Training and Evaluation for those who fail the test and get a write up/warning.
* Security rooms have to buzz you in after face ID authentication after scanning your badge, CCTV security rooms.
* Time-Limited/Timelocked - Rotating shift-based access policy to mitigate corporate espionage.
* 2fa/MFA high-level access to server rooms to protect confidential financial data.
* Skivs/RF - Proof/Insulated Rooms. Compartmentalized/Air-gapped Rooms.

Set an estimated timeline for each potential solution.

* Every month, there should be random checks for tailgating. Whoever fails has to do employee training and evaluation.

**If you finish early, get ahead by considering the following questions:**

All companies have leadership (CEO, etc.). Which common C-level officer titles do you know? Which do you think this company has?

* CEO, CFO, CISO, CSO. This company would have CEO, CFO, & CSO performing both positions (acting in place of CISO)

Which security functions/responsibilities would any security department have?

* The security department would have to control access points, high access areas monitored constantly (via cam and 30-minute passes.) (Security Guards)
* The System’s Analyst would be responsible for Pentesting, network mapping, data encryption, among others.

Which teams would fulfill these responsibilities?

* Pentesting & Training - CISO, CTO & CSO
* Implementation & Budgeting - CFO, HR, CEO, CISO & CSO

Part 2.

Involve the Right People:: Identify the teams and/or managers involved, and explain how the security department should collaborate with them.

* CIO, CTO & IT Director - Should check in with CISO & CSO that employees ran routinely hardware checks, door checks, cloud backups, file checks, and monitoring network traffic.
* CFO, HR, & CISO - Should manage security policies(employee training), project implementation, and budgeting, Write-ups/Strikes, and Decisions on which employees to let go should they not follow corporate security policies and employee training.

Make an Action Plan: Identify your "plan of attack". For example, you might propose running a training; implement stricter security controls; some combination of the two; etc.

* Run a training (Tailgating, screen lock desktops if you walk away from the computer for any amount of time (needs to be password locked), changing passwords every 30-45 days (explain the need for Num, Syb, Alpha. Passwords longer than 8 letters; no personal information used for password)
* Implement Stricter Security practices i.e. Access Points, No personal electronics at work stations, id badges worn at all times, Security Checks (door checks & random work station checks for unauthorized personal items), etc.

Schedule: Determine timelines for implementing your plan. Be specific: explain what will get done in terms of quarterly or annual goals.

* Implementing training sessions would take place within two weeks and we would train 25% of the staff the 1st week, the next 25% the following week, the next 25% the following week, and the remaining 25% the final week. In one month we will have trained the entire staff. (via Zoom, conference call) Failure to follow new security procedures; employee(s) will be asked to attend a special training session. Continue training every quarter for 25% of the staff.
* Implementing new stricter Security Security should be put into effect immediately. Ultimately this process would require on the job training instead of training before job official start. This would require assessments every month for up to 3 months.

Metrics and KPIs: Explain what you will measure to determine if your plan has been successful. Specify KPIs indicating what you want your plan to achieve. These are your planned goals.

* Plan: To implement an effective and sustainable company security policy based on monthly to yearly compliance and retention rate of employees, building trust with employees, and the hired pen-testing company/s, reducing HR having to hire new people.
* KPIs - Employee compliance rates, Trusted employee retention/satisfaction rates, Cyberattack, and Vulnerability rates monthly to yearly in detailed reports.

Measurements: Explain how you will measure the success of your plan. Specify both when and how you'll measure results. Be detailed: If you're going to contract an assessment to a pentesting company, explain exactly what you'll have them do.

* By measuring statistics and checking in with the pentesting company about failure-to-comply rates of employees based on monthly training analysis and employee retention rates.
* Measuring downtime of services, Cyberattacks, and vulnerabilities with the contracted pen-testing company/s.