

# Unauthorized Access Attempts on Information Systems: The Role of Opportunity Contexts

## Challenge

89% of the organizations believed they are at risk from **insider attacks** / 55% suggested **privileged users** posed the biggest threat to corporate data (Vormetric 2015)

*Insider threats impose significant threats to organizations' digital assets*

- Studies in behavioral information security have revolved around **individual motivation**.
- It is unclear how **circumstances** impact insider threats.



## Solution:

- **Criminal opportunity** is created by the temporal and spatial convergence of **motivated offenders** and **suitable targets** in the absence of **capable guardians**.
- Scope of accessed applications, data value of accessed applications, temporal and spatial realization of ineffective guardianship, and department size.



## Scientific Impact:

- First study to examine the **predictive validity** of **multilevel criminal opportunity theory** in the context of information systems security
- Used **large-scale field data** along with quantitative methods and provided an **analytic tool** in identifying contributing factors.
- Incorporated both **individual-level** and **department-level** factors and examined the effects of opportunity contexts.

## Broader Impact:

- Help security managers better understand how employee activities (and vulnerabilities) may change along with their surroundings.
- Suggest risk profiles for adaptive authentication should consider time of user access, access location, the history of application access, and characteristics of the department the user is in.
- Inform the development of situational crime prevention techniques through changes in the conditions and circumstances that foster insider threat.