# Managing Cybersecurity: Data Access Protection

RUSLAN MOMOT, Ross School of Business, University of Michigan, USA
MARAT SALIKHOV, New Economic School and Moscow School of Management Skolkovo, Russia
OLEH STUPAK, University of Cambridge, UK
GEORGE CHARLSON, Keystone Strategy, UK

Digital businesses are increasingly adopting data-sharing practices, granting employees broader access to internal datasets to improve operational efficiency. Yet, many organizations may be sharing too much: a recent survey found that 33% of firms give employees access to all company data, and another 35% grant more access than is strictly necessary for their roles. Such overexposure increases cybersecurity risk, particularly when adversaries exploit employee access (e.g., through phishing attacks). Such overexposure exposes firms to cybersecurity risks such as data breaches

We study this problem using a game-theoretic model featuring a firm and an adversary. The firm (i) chooses a data access allocation—specifying which employees have access to which datasets—and (ii) sets a global cybersecurity protection level. While granting access generates economic value, it also increases the potential damage if an adversary succeeds. The attacker may be either opportunistic (random) or strategic (targeting the most valuable employees). The firm does not observe the attacker's type but knows the probability of each.

Our analysis shows that giving full access to all employees is only optimal when the adversary's attack strength is sufficiently low. As the threat intensifies, the firm must restrict access—either selectively or uniformly—depending on its underlying technology. With vertical differentiation (i.e., some employees and datasets are more valuable), the firm adopts a hierarchical structure. With horizontal differentiation (i.e., employees specialize in certain datasets), the firm compartmentalizes access, choosing a structure aligned with Zero-Trust principles.

To characterize access structures, we define two summary statistics: the *average access level*—the expected number of datasets per employee—and the *access inequality*—a measure of how unevenly access is distributed across employees. As the adversary's strength increases, the average access level declines, while access inequality follows an inverse U-shape: it initially rises as the firm concentrates access among a small subset of employees, then declines as restrictions are applied more uniformly. Protection investment may decrease once access is sufficiently limited. As the probability of facing a strategic (rather than opportunistic) adversary increases—that is, as adversarial sophistication rises—firms reduce access inequality and may even expand overall access. Finally, when employee productivity is highly concentrated, the firm benefits from allocating more data to top performers while relying less on protection.

Our results highlight how firms should coordinate data access and protection decisions in response to both external and internal factors. We show when hierarchical, compartmentalized, or mixed access structures emerge, and how these structures adapt to changes in adversarial strength and sophistication, as well as in the distribution of employee productivity.

*Full paper available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4293509

CCS Concepts: • **Security and privacy → Access control**; **Economics of security and privacy**.

Authors' addresses: Ruslan Momot, momot@umich.edu, Ross School of Business, University of Michigan, Ann Arbor, MI, USA; Marat Salikhov, msalikhov@nes.ru, New Economic School and Moscow School of Management Skolkovo, Russia; Oleh Stupak, os446@cam.ac.uk, University of Cambridge, UK; George Charlson, gcharlson@keystone.ai, Keystone Strategy, UK.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

*EC '25, July 7–10, 2025, Stanford, CA, USA*

© 2025 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-1943-1/25/07
https://doi.org/10.1145/3736252.3742520

Additional Key Words and Phrases: Cybersecurity Strategy, Access Control, Economics of Security and Privacy, Network Security, Bipartite Graphs.

**ACM Reference Format:**
Ruslan Momot, Marat Salikhov, Oleh Stupak, and George Charlson. 2025. Managing Cybersecurity: Data Access Protection. In *The 26th ACM Conference on Economics and Computation (EC '25), July 7–10, 2025, Stanford, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3736252.3742520