ISACA Melbourne Chapter

Article 2025 | Author Reshma Devi

The Challenges of Underfunding Data Teams: How Data Drives AI and Security

Organisations are increasingly allocating significant portions of the budgets to artificial intelligence (AI) and security initiatives. While these areas are undeniably crucial for driving innovation and safeguarding data, there's a growing concern about the underfunding of data teams; the backbone that fuels AI systems and supports security measures. This article explores the challenges that arise when data teams are underfunded, emphasising the critical role they play in ensuring the effectiveness of AI and security operations.

The Role of Data Teams

Data teams are responsible for collecting, processing, and managing the vast amounts of data that organisations generate. This data forms the foundation upon which AI algorithms operate and security protocols are built. Without high-quality, well-managed data, AI models may produce inaccurate results, and security measures may fail to identify and mitigate threats effectively. In addition to data management, data teams also oversee data governance activities, ensuring data quality, consistency, and compliance with regulatory requirements. Therefore, data teams are essential for maintaining the integrity, reliability, and usability of data within an organisation.

The Imbalance of Budget Allocation

Despite the importance, data teams often receive a smaller share of the budget compared to AI and security teams. This imbalance can be attributed to several factors, including the high visibility of AI projects that promise transformative capabilities and the urgent need to protect against cyber threats. However, this skewed allocation overlooks the fact that both AI and security initiatives are heavily dependent on the quality and availability of data managed by the data teams.

Potential Risks and Inefficiencies

Underfunding data teams can lead to a range of risks and inefficiencies, including:

1. **Compromised Data Quality:** Insufficient funding can limit data teams' ability to implement robust data quality management and governance processes. This can result in inaccurate, incomplete, or outdated data being fed into AI systems, leading to flawed insights and suboptimal decision-making.

2. **Data Silos:** Without adequate resources, data teams may struggle to integrate data from various sources, leading to data silos. These silos hinder collaboration and prevent organisations from gaining a comprehensive view of the operations, which is crucial for both AI and security initiatives.

3. **Increased Vulnerability:** Underfunded data teams may lack the necessary tools and expertise to implement strong data governance and security measures. This increases the risk of data breaches and compromises the organisation's ability to protect sensitive information.

4. **Inefficient Data Processing**: Limited resources can also hamper the efficiency of data processing and analysis. This can slow down the development and deployment of AI models and delay the identification and response to security threats.

Case Studies

Several organisations have experienced the negative impact of underfunding the data teams. For example, a leading healthcare provider faced significant challenges when the AI-based diagnostic system produced erroneous results due to poor data quality. Similarly, a financial institution suffered a major data breach because the data governance policies were insufficiently funded and poorly implemented.

Conversely, companies that have recognised the importance of balanced budget allocation have seen positive outcomes. A global e-commerce giant invested heavily in its data teams, leading to improved data quality and more accurate AI-driven recommendations. Additionally, the robust data governance framework significantly enhanced its security posture, reducing the risk of data breaches.

Recommendations for Budget Reallocation

To address the challenges of underfunding data teams, organisations should consider the following recommendations for more balanced budget allocation:

1. **Recognise the Value of Data Teams:** Acknowledge the critical role that data teams play in supporting AI and security initiatives. Communicate this value to stakeholders and ensure that data teams are included in strategic planning discussions.

2. **Allocate Sufficient Resources:** Provide data teams with the necessary resources, including funding for advanced tools, training, and hiring skilled professionals. This will enable them to manage data more effectively and support the organisation's AI and security goals.

3. **Foster Collaboration:** Promote collaboration between data, AI, and security teams. This can be achieved through cross-functional projects, regular meetings, and shared goals. By working together, these teams can leverage each other's strengths and address challenges more efficiently.

4. **Implement Strong Data Governance:** Invest in robust data governance frameworks that ensure data quality, security, and compliance. This includes implementing policies for data access, usage, and protection, as well as regular audits and reviews.

5. **Leverage the Three Lines of Defence:** Use the three lines of defence to advocate for and optimize budget allocation for data teams. First Line: Data owners and stewards highlight data quality's impact on AI and security. Second Line: Monitors and reports on data management effectiveness. Third Line: Independently assess data governance maturity and use audit insights to recommend budget shifts that strengthen data teams and address critical gaps.

6. **Empower Boards and Committees:** Ensure that boards and committees are well-informed about the critical role of data teams. Provide the necessary resources and authority to oversee data governance and budget allocation. This can help align organisational priorities and ensure that data teams receive adequate funding to support the essential functions.

Future Trends

As organisations continue to recognise the importance of data teams, we can expect to see a shift in budget allocation trends. The growing focus on data-driven decision-making and the increasing reliance on AI will likely drive greater investment in data teams. Additionally, the rising threat of cyber-attacks will underscore the need for robust data governance and security measures, further highlighting the value of well-funded data teams.

The underfunding of data teams presents significant challenges for organisations that rely on AI and security initiatives. By recognising the critical role that data teams play and allocating budgets more equitably, organisations can enhance its data quality, improve the effectiveness of its AI systems, and strengthen security measures. As the digital landscape continues to evolve, the importance of investing in data teams will only become more apparent, paving the way for more balanced and effective budget allocation.

Some related links to ISACA:

- **Artificial Intelligence in the Boardroom: ISACA's Approach to AI and Cybersecurity**
- **Press Releases 2025 Privacy budgets set to decrease in 2025 new research from ISACA reveals**
- **In Pursuit of Digital Trust | ISACA**
- **IT Certifications | Earn IT Credentials | ISACA**