THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

Transfer Pricing and Cybersecurity Costs: A Hidden Exposure

Transfer Pricing and Cybersecurity Costs: A Hidden Exposure

Cybersecurity has moved from being a back-office IT concern to a **board-level strategic risk**. For multinationals, the threat is clear: data breaches, ransomware attacks, and regulatory non-compliance can destroy both value and reputation overnight.

To manage this, most groups centralize their cybersecurity spend; global firewalls, anti-virus platforms, penetration testing, cloud security subscriptions, and ongoing audits. But once the bills are paid at headquarters, a familiar question surfaces:

Should these costs be recharged to subsidiaries? If so, how?

This is where **transfer pricing** and cybersecurity intersect; and where many businesses are underprepared.

Why Cybersecurity is Different

Cybersecurity costs are not like office stationery or HR training. They are:

- **Strategic and preventive**: subsidiaries benefit not from what happens, but from what *doesn't* happen (e.g., a data breach avoided).
- **Uneven in risk profile**: a Tanzanian logistics subsidiary processing customer data may face different risks than a small marketing support office in Mauritius.
- **Hybrid in nature**: some costs relate to global compliance (shareholder-level), others to local operations (service-level).

This ambiguity makes cybersecurity charges **a hidden transfer pricing exposure**.

The Transfer Pricing Lens

Under the OECD Transfer Pricing Guidelines, the key question is always: **does the subsidiary derive a benefit that an independent party would be willing to pay for?**

Shareholders Cost

Global security audits for consolidated reporting or HQ's peace of mind may fall into this category.

These are not re-chargeable.

Intragroup Services

Licenses for firewalls, intrusion detection software, and local penetration testing that directly protect a subsidiary's operations clearly provide benefit.

These can be recharged, typically on a cost-plus basis.

Strategic Investments

Development of proprietary cybersecurity systems may qualify as an intangible asset.

These may be charged as royalties or through cost contribution arrangements.

The challenge is to document the split and to allocate costs fairly.

Allocation Approaches: Pros and Cons

Groups typically consider three approaches:

Flat mark-up allocation (e.g., 5%)	• Costs are pooled and recharged to all subsidiaries with a uniform mark-up. • **Pro:** Simple, predictable. • **Con:** Risks being challenged by TRA as arbitrary and not aligned with risk exposure.
Proportional to revenue or headcount	• Subsidiaries are charged based on relative size (turnover, staff numbers, or system users). • **Pro:** Reflects scale of operations. • **Con:** Doesn't capture risk differences: a small subsidiary handling sensitive financial data may face higher risk than a larger distribution entity.
Risk exposure model	• Costs are allocated based on data sensitivity, transaction volume, or industry exposure (e.g., financial services vs logistics). • **Pro:** Most defensible, aligns with benefit principle. • **Con:** Harder to measure and administer; requires strong documentation.

Case Example

Imagine a multinational with:

- **HQ in Europe,**
- **A Kenyan subsidiary handling customer logistics across East Africa**, and
- **A Tanzania subsidiary providing business development and sales support across East Africa**.

HQ spends $2 million annually on cybersecurity, including licenses, monitoring, and audits.

- The Kenyan logistics entity processes customer and shipping data; its exposure to ransomware risk is high.
- The Tanzania sales support entity handles minimal sensitive customer data.

If HQ simply allocates costs based on headcount, both entities may pay averagely similar amounts. TRA could argue the Tanzanian entity is being **overcharged** for a service it barely needs; recharacterising part of the charge as a **shareholder cost**.

Tanzania's Audit Posture

The Tanzania Revenue Authority (TRA) has become increasingly alert to "head office cost allocations." Its typical audit questions include:

- *What evidence shows the subsidiary benefited from the cybersecurity expense?*
- *Were these costs necessary for local operations, or mainly for group-level peace of mind?*
- *How was the allocation basis chosen, and is it consistent across all group entities?*

Without documentation, TRA may disallow deductions, triggering adjustments and penalties.

Practical Steps for Multinationals

1. **Map the cost categories**
   - Break cybersecurity spend into:
     a) global compliance (shareholder),
     b) local protection (intragroup services),
     c) strategic development (intangibles).
2. **Choose a defensible allocation key**
   - Revenue or headcount may be fine for simple IT support.
   - For cybersecurity, risk-based metrics (data processed, transaction volume, system access levels) provide stronger defense.
3. **Document the benefit**
   - Keep evidence of security reports, intrusion attempts blocked, audit findings, and local IT risk assessments.
   - The more tangible the local benefit, the stronger the TP position.
4. **Align with local compliance**
   - In Tanzania, align cybersecurity allocations with **Data Protection Act 2022** obligations. This strengthens the argument that the spend is locally relevant and not merely for HQ.
5. **Review periodically**
   - Cyber risks evolve. Allocation keys that made sense two years ago may no longer reflect current operations.

Closing Perspective

Cybersecurity spend will only increase in the coming years; and with it, tax authority scrutiny of how costs are shared. For groups operating in Africa, where TP enforcement is tightening, this is a **hidden exposure waiting to be tested**.

The principle is clear:

- Subsidiaries should contribute to the cost of cybersecurity **only to the extent they benefit**.
- Allocations must be logical, consistent, and well documented.

For transfer pricing professionals, cybersecurity is the new frontier; one where **technical expertise, regulatory insight, and commercial judgment** must come together.

In the digital age, protecting data is protecting value. And in the TP world, documenting that protection is the key to avoiding costly disputes.

Prepared by: RSM (Tanzania) Consulting Ltd – Transfer Pricing Team