LUCIDUM LEARNING

KWIK
Knowledge - I wish I Knew

IT Blunders and Geopolitical Fallout

Author: **Michael Judin**

Published: 09 March 2026

A simple IT mistake pulled back the curtain on a massive $90bn Russian oil smuggling network. Not only a headline about global politics, this exposed governance, digital infrastructure, and modern supply chain risks. Your organisation's IT security is not just a back-office technicality; it might be your only defence against a geopolitical scandal.

This **KWIK series** aims to start conversations amongst individuals, social groups, and in organisations. We share practical knowledge – built up over decades, and which would have helped us if we knew it earlier. We believe that people between 25 and 45, if they have access to this knowledge, are ideally placed to lead in rebuilding South Africa.

Think About

- Do you view IT security as a strategic necessity or just 'operational hygiene'?
- Does your board receive credible assurance that your systems can detect sanctions circumvention?
- Could a 'misconfigured system' in your company expose sensitive trade or internal data?
- Are your revenue targets implicitly encouraging 'wilful blindness' regarding high-risk jurisdictions?
- If a suspicious pattern emerged in your data today, who is accountable for acting, and how quickly would they do so?
- Is your digital infrastructure robust enough to serve as a genuine guardrail, or is it just a reporting exercise?
- Does your organisation rely on the defence of 'we did not know', and do you realise how hollow that sounds in a digital age?

The Merging of Risk:

The recent revelation of a $90bn shadow fleet, exposed not by intelligence agencies but by a technical error, underscores a shift in the corporate governance landscape. Modern governance now requires navigating the intersection of three high-stakes domains that were once managed in separate silos. Geopolitical risk is no longer an abstract concept discussed in embassy corridors; it sits inside your procurement and trading desks. Since 2022, the complexity of sanctions has turned supply chains into minefields. Any company involved in shipping, logistics, or finance is now entangled in dynamic regimes that change weekly. The 'shadow fleet' of tankers operating outside traditionally governed markets proves that where there is a profit margin, there is a loophole. As a leader, you must ask: are we inadvertently participating in these shadow markets? A misconfigured database or an unencrypted email isn't just a tech failure, it is a regulatory accelerant. Technology that enables globalised trade also creates the very data trails that can dismantle it. Once information surfaces via a leak, regulators move with a speed that traditional legal departments cannot match. Assets are frozen, credit lines are pulled, and reputations are destroyed overnight. Your IT department is now your first line of defence against international litigation. In 2026, directors and executives can no longer claim ignorance as a valid defence. Fiduciary duty has evolved. Boards must move beyond passive 'formal checks' to 'courageous questioning'. This means digging into how transactions are actually handled in high-risk jurisdictions. Sanctions evasion thrives in 'grey zones', intermediaries that are technically compliant on paper but ethically ambiguous in practice. If your governance framework doesn't account for the 'spirit' of the law, the 'letter' of the law won't save you when data leaks. The uncomfortable truth is that our digital infrastructure is now part of the global geopolitical infrastructure. Oversight failures have consequences that stretch far beyond quarterly earnings; they touch on national security, human lives, and international stability. The real battleground for the soul of your organisation no longer lies in your boardroom alone, it is in your server room and the integrity of the data you hold.

Practical Tips—The Next Gen of Leaders

1. **Sanction mapping**: Maintain a real-time understanding of exposure across all subsidiaries and beneficial ownership structures.
2. **Data integrity**: Ensure trade and payment systems are not only secure but also independently audited and stress tested.
3. **Audit culture**: Review whether your company culture prioritises ethical compliance over high-margin, high-risk revenue.
4. **Establish protocols**: Create clear escalation paths for when red flags or contextual anomalies appear in supply chain data.
5. **Verify compliance**: Move past 'ticking the box', ensure your compliance systems are genuine guardrails against manipulation.
6. **Shadow market awareness**: Be aware of the 'grey zones', jurisdictions, and intermediaries that provide just enough complexity to preserve deniability. If a deal looks too good to be true, it likely involves a shadow network.

- We provide coaching and mentoring sessions for young leaders wishing to equip themselves with knowledge to make a difference in society.
- Sessions take place face-to-face or online, one-on-one or in groups – as suitable for participants.
- Requests for topics to be covered in this series are welcome.
- Other Lucidum Learning resources are available on our website at www.lucidum.africa.

Contact Us
www.lucidum.africa

J. Michael Judin
+27 11 595 2300
www.elawnet.co.za

LUCIDUM
Governance | Risk | Ethics | Compliance | Sustainability