Risk Solutions for a Complex World

INTEGRITY | COMMITMENT | EXPERIENCE

The Paradise Papers
Implications for Law Firms and the Offshore Services Business

The much reported hack of computer systems at the offshore law firm Appleby, and the subsequent leakage of 13.4 million files, has highlighted, once again, how critical data security is to professional service providers, company secretarial companies and financial institutions in the offshore finance business.

Security and procedural weaknesses present major threats, given rising distemper about economic inequality, politically motivated investigations into offshore structures, and, of course, the enterprise-threatening impact of such leaks.

What Actually Happened?

Publically available information suggests that the hack of Appleby's computer systems was followed by a leak of some 13.4 million files to the Sueddeutsche

Zeitung, a German newspaper, and the International Consortium of Investigative Journalists ("ICIJ"), an organisation that conducts lengthy investigations. Another business affected was Asiaciti Trust, an international trust and corporate services provider, which operates out of Singapore.

This leak drew comparison with that from the Panamanian law firm, Mossack Fonseca in 2015. As was the case then, the motives are not yet clear, although the hack does appear to be part of a broader and concerted campaign by certain governments and lobby groups targeting offshore financial centres, and the businesses and individuals that use them.

Media reporting on the activities of Appleby's clients has since covered, amongst other issues:

- **Angola:** Links between a sovereign wealth fund and Mauritius.
- **Canada:** Stephen Bronfman, a fundraiser for Prime Minister Justin Trudeau, invested in entities in the US, Israel and the Cayman Islands.
- **India:** The files reportedly contain the names of over 700 Indian citizens.
- **Indonesia**: Presidential candidate Prabowo Subianto and the daughter of former dictator Suharto, Siti Hediati Hariyadi, face questions about taxes.
- **Russian Federation**: VTB Bank and Gazprom invested in Facebook and Twitter through Yuri Milner, a business associate of US President Trump's son-in-law Jared Kushner.
- **United Kingdom**: Details about Conservative Party donor Lord Ashcroft's offshore holdings emerged, and the royal family's use of offshore structures.
- **United States**: Information touched on US President Trump's staff, including Treasury Secretary Steven Mnuchin, and Secretary for Commerce Wilbur Ross.

Doubtless, more will emerge. No reports have so far suggested that any of these activities were illegal. Even so, there is also an evident political agenda at play and future disclosure – the next "chapters or episodes" from the incident will be instructive in this respect.

The leaks on the surface also hinted at some compliance failings at Appleby, such as:

- The firm's holding funds on behalf of politically exposed persons.
- Links to companies alleged to trade in "blood diamonds".
- An internal audit showing that only one of 45 files under assessment complied with standards.
- A fine imposed on Appleby by the Bermuda Monetary Authority for compliance failings.

All told, the attack has seriously damaged Appleby's reputation.

Other providers must learn from this leak, not least as Appleby itself was apparently not the target. Rather, its clients were.

Political Fallout

A separate set of risks relate to a rising regulatory tide. Pressure on offshore financial centres has risen since the 2008 financial crisis. In October 2017 the consultancy PwC stated that use of offshore financial centres was becoming "unacceptable", in part owing to the earlier LuxLeaks and the Panama Papers revelations.

Moreover, a sense is growing that people should "pay their share". Leftist politicians such as Bernie Sanders in the US and Jeremy Corbyn in the UK, as well as lobby groups such as Global Witness and the Tax Justice Network, routinely pillory offshore financial centres.

Some jurisdictions are likely to respond. Germany and the European Union ("EU") have long criticised such centres (despite Ireland, Luxembourg and the Netherlands offering such services); and the European Council has warned 52 jurisdictions to curtail preferential tax measures, meet transparency standards, and adhere to Organisation for Economic Cooperation and Development ("OECD") guidelines – or face blacklisting. Previously, the UK had sheltered its Crown Dependencies and Overseas Territories, but London may struggle to do so now that it is leaving the EU.

Other jurisdictions may prove less reactive. The Trump administration seems unlikely to take action, and the fiscally stronger states in Asia, such as China, may not demand a regulatory response from Hong Kong and Singapore, despite these jurisdictions providing many such services. Indeed, as a rule, those offshore financial centres that are less reliant on the western states may prove those best able to protect their interests.

All the same, pressure will come from above. The regulatory burden on financial institutions, law firms and corporate service providers will grow, with initiatives on information exchange, pressure from blacklists, and requirements to watch for tax evasion or money laundering. Compliance officers will have to respond.

Pressure will also come from below, as financial institutions carry out internal investigations, update procedures, and, on occasion, disclose findings to regulators. Companies may turn to liability insurance to cover investigations, leading to a focus on "conduct exclusions". Businesses in the sector will have to keep up with these trends, or risk fines and denunciation.

Implications for Professional Service Providers

This situation thus presents two key risks to law firms and corporate services providers in Hong Kong, Singapore and elsewhere. The first risk is reputational, in that any leak can destroy a business operating in this field. Steps to prevent the compromising of confidential information are essential, as any professional services firm or financial institution is now at risk.

The second risk derives from the regulatory response, which will force businesses to expand their internal compliance and due diligence processes. Any failure to respond would be foolhardy, given the righteousness with which the opponents of the offshore financial centres pursue this campaign.

Action is Required Now

Doing nothing is no longer an option. Firms should assess their particular vulnerabilities, taking account of both **systemic** and **human risks**. SVA can assist by carrying out a **Vulnerability Assessment Programme**, which would include examination of:

VULNERABILITY ASSESSMENT PROGRAMME		
Human Issues	**Administration and Process Issues**	**Information Technology Issues**

• 'Trusted insiders'
• Defectors / Whistleblowers
• Problem employees
  - Aggrieved
  - Indebted
  - External offers / inducements
• Government intelligence initiatives
  - Rewards schemes
• Commercial intelligence
• Media targeting
• Political motives
	• Access to key data
	• Policies and procedure
	• Vetting and screening of employees
	• Vetting of third party providers, such as:
	  – Law firms
	  – Accountants
	  – Private banks
	  – Financial advisers
	  – IT providers
	  – Temporary staff
	  – Other companies as relevant
	• Use of email or social media in offices
	• Exit procedures for staff
		• Security of Data
		• Classification of data
		• Access to system
		• Encryption
		• User history and logs
		• System administration
		• Outsourcing mechanisms
		• Hardware and software
		• Alert functions
		• Destruction of historical data

Conclusion

The data breach from the law firm Appleby has highlighted, once again, how security and procedural weaknesses at law firms or businesses in the trust, offshore finance and company formation sector can damage, or even destroy, a thriving enterprise. Accordingly, urgent measures to mitigate the reputational and regulatory risks are essential.

Taking such action does not mean that these businesses have anything to hide. Rather, in the current climate, any whiff of “offshore finance” or the like could attract ill-informed comment that damages a reputation. SVA stands ready to assist.

* * * * *

SVA (www.stevevickersassociates.com) is a specialist risk mitigation, corporate intelligence and risk consulting company. The firm serves financial institutions, private equity funds, corporations, high net-worth individuals and insurance companies and underwriters around the world. We are specialists in crisis containment.

About Us

Steve Vickers and Associates (SVA) is a specialist risk mitigation and security consulting company. The company serves corporations, high net-worth individuals and insurance companies around the world. SVA assists clients both in mitigating risk and when necessary to respond swiftly and effectively to incidents and crisis situations.

24-HOUR CRISIS RESPONSE HOTLINE
(+852) 9196 2350

Unit 1501, Bank of East Asia Harbour View Centre,
56 Gloucester Road,
Wanchai, Hong Kong
Phone: **(+852) 2528 1230**
Fax: **(+852) 2528 1231**
mail@stevevickersassociates.com