The age of Automatic Information Exchange:

Protection and security of client information data

By Martin Straub

Automatic Information Exchange (AIA) of client financial data under the US Foreign Account Tax Compliance Act (FATCA) and the OECD's Common Reporting Standard (CRS) is now reality. Information is flowing under FATCA and information will start to flow under CRS in September 2017. These unprecedented invasions of personal privacy have now removed any remaining illusion of client privacy or confidentiality.

Requirement four of the CRS to "Protect confidentiality and safeguard data" is the OECD's realisation that hacking, leaks, loss or sale of confidential, private, often sensitive data can potentially be extremely harmful to people and their families. On roughly the same timeline therefore as implementation of the CRS, the EU is introducing the General Data Protection Regulation (GDPR) and the Network & Information Security Directive (NIS). With these, Brussels wants to show it is serious about protecting peoples' data, and not just taking government nosiness to unprecedented levels. The GDPR will unify data protection throughout the EU with a single law. Being a regulation, not a directive, GDPR affects all EU member states after the two year transition period. It does NOT require any enabling legislations to be passed by any member state.

As more and more personal data is collected and used, policymakers want to make at least a show of protection. This is putting cybersecurity increasingly on the agenda for compliance and management. The US'SEC has understood and recognised the seriousness of the issues. In a recent communique, SEC Chair Mary Jo White said that "Cyber security is the biggest risk facing the financial system" in one of the frankest assessments yet of the threat to financial institutions from digital attacks.

Within the EU, the GDPR extends data protection law to all companies processing the data of EU residents, including non-EU countries. Security breaches carry severe penalties under the GDPR of 2-5% of global revenue for the offending company. Yes, you read this right. For large multinational companies, banks or insurance firms, this could easily become painful. For Google, Amazon or UBS, the numbers involved have the potential to make this cartoonish. With around 640 million records breached in the EU during the period 2005–2014 the potential is huge; a new, lucrative, "sure fire" source of revenue. Even better, easily marketable under the banner of "protecting EU citizens". However, there appear to be no penalties or consequences for government agencies when they lose your client data. Nowhere. In the CRS, there also appears to be no penalties for a "competent authority" or any other agency for losing client data, be it leaked, hacked, stolen or just misplaced.

With good reason. Governments' record on security is rotten. One large OECD tax authority lost over 600,000 tax records to hackers in 2013. In a very well-known hack, the US Office of Personnel Management (OPM) lost over 21 million records to hackers in 2014. In the stolen data were 5.6 million sets of fingerprints, including CIA, FBI and secret service agents' prints. These were two cases that could not be hushed up. The UK government is relatively open, admitting to around 20 serious security breaches between 2008 and 2013 with several million records hacked, stolen, lost or sold. EU governments own up only to 55 serious cases of data breach between 2005 and 2015, involving the breach of around 55 Million records. There is no doubt that this is only a small fraction of the true number. Unknown is what governments are not owning up to and, of course, what they don't detect. It took OPM a year to even realise its security had been compromised. The realisation hit when the information turned up for sale.

Why does this matter so much? Breaches lead to fraud, identity theft, financial damage, increased kidnapping and extortion risk. Plus, in many countries, political pressure, blackmail and trumped up criminal charges. Firms will need to get much more serious about safeguarding data. Most of these leaks would most likely have been prevented had the data been securely encrypted on devices and servers. Additionally, who accesses which data, when, should be logged with user patterns modeled, thus alerting firms to suspicious or unauthorised activity. Firms must work with specialist data security partners to put systems, processes and procedures in place to keep data secure. Server and device encryption erects hard barriers. User logging and behavioural modeling enables firms to identify persons internally who may have leaked or sold data. In light of the penalties in the GDPR, you do not want your company to be the one to lose data.

Governments will continue to lose data in increasing quantities as AIA moves forward. You need to have asset protection strategies and structures in place for your clients for when this happens. Because damages will result, for the "unprotected" or "naked", it's a certainty. For the "prepared", you can mitigate the effect. When damage results, work with specialist legal teams to demand accountability and obtain compensation and reparation. Do not hesitate to take legal action to hold government agencies accountable. Class action suits for losing confidential data are already underway in the US. With AIA we are entering a period where we begin to find out

what governments can be held accountable for and what compensation and damages may be claimable.

Compliance officers and managers need to talk to IT staff about the data security both “at-rest” on servers and “in-motion” during transmission. Partnerships with specialist providers need to be established to implement solutions, process and procedural, to address this latest challenge in an ever changing, increasingly complex world.

Martin Straub, martin.straub@envisage.ch, is a Swiss based expert for Wealth Management.

Martin Straub’s article has been published on behalf of GGI member firm
Westleton Drake
Advisory, Tax
Zurich, Geneva Switzerland
London, UK
Paul Bolland
E: paul.bolland@westletondrake.ch
W: www.westletondrake.com