Data trap 2.0

Data trap 2.0: A double-bind of threats and laws

by Rose Bernard**.**

The global cyber security landscape will become more fractured in 2017. Companies will face legislative demands that are both increasingly restrictive and increasingly divergent – even conflicting – across different geographies. Add in rising threats from nation states, cybercriminals and cyber activists, and the task of managing and protecting data will become ever more challenging for multinational businesses.

Data nationalism and e-commerce

2017 will see growing conflicts between data legislation in different regions and countries. This began in October 2015 when the European Court of Justice struck down the Safe Harbour Principles – the overarching structure under which data could be transferred between different regulatory regimes in the US and the EU. The agreement's replacement, the EU-US Privacy Shield, implemented in 2016, is still considered deficient by many data protection groups and is likely to face legal challenges throughout 2017. This means US and EU regulations on data protection will continue to conflict. Stringent regulations are drawing together the EU's Single Digital Market, the growing structure for e-commerce. While this will create a unifying framework within the EU, it is likely to isolate the EU from the rest of the global market.

Similarly, the introduction of new cyber security laws in China and Russia will increase the regulatory burden on multinationals. The Chinese legislation, due to be implemented in 2017, has been advertised as addressing national security concerns, but really targets the cross-border transfer of data. In Russia, growing state surveillance of companies and anti-encryption legislation – such as the Yarovaya Law passed in 2016 – places legislative and regulatory burdens on companies that will be incompatible with much of the world's privacy legislation. Both states are therefore at risk of isolation in the same manner as the EU, forcing businesses to comply with a number of different regulations and creating individual blocs of legislation.

So what does this mean globally? As nation states extend legislative requirements in their respective cyber spaces – driven by fear of terrorism and cyber threats – conflicting data protection and regulatory environments will lead to increased data nationalism. This is likely to force companies to store data on local servers because they will be unable to meet regulatory requirements in international data transfers. Given that the EU-US Privacy Shield alone represents USD 500bn in global commerce, any restrictions on data flow are likely to stifle the global e-commerce market.

Cyber threats to politics, infrastructure and finance

On the political stage, rising global instability will drive greater government surveillance and the pursuit of destructive cyber capabilities behind the veil of proxy groups. This was seen in the 2016 US presidential election when hacking, information leaks and misinformation campaigns undertaken by nation states and activist groups were accused of damaging the electoral process.

This trend will continue in 2017 with further targeting of high-profile political events. Particularly at risk are the Chilean and Ecuadorian elections: cyber threat actors have previously been involved with disrupting political campaigns in South America. Germany is also vulnerable. Chancellor Angela Merkel has publicly expressed her belief that cyber actors linked to the Russian government will attempt to influence German politics.

As well as political events, foreign government surveillance will target critical national infrastructure and significant financial entities. Acquiring private-entity information believed to be important to governments is likely to be a key priority for sophisticated, often state-linked groups (known as Advanced Persistent Threat (APT) groups because of their capabilities and targeted attack campaigns).

This is a stark move away from the global attitudes dominating internet governance since the early 2000s. Instead of an attempt to implement global norms, exemplified by the Budapest Convention of 2001, 2017 is likely to amplify the shift towards differences in attitudes towards data protection, privacy and censorship. Nations and supranational organisations will meet this change by recognising and legislating for a new, disjointed cyber landscape.

Decreasing effectiveness of law enforcement

Law enforcement agencies will be increasingly constrained by national boundaries. Although 2016 saw a number of cross-border initiatives, such as the NATO Locked Shields Exercise and the EU Cybersecurity event, law enforcement must work within the bounds of national data protection, privacy and surveillance legislation. Data and intelligence sharing are unlikely to continue at the same levels as in 2016, with divisions between companies, law enforcement agencies and international bodies set to grow.

These divides will allow cybercriminal and cyber activist ecosystems to expand and develop. Cybercriminals will continue to take advantage of the growing malware market, building on transnational and cross-group links that we have been monitoring and analysing throughout 2016. Hacktivist groups such as the Anonymous collective will continue to encompass a wide range of global factions that will pick targets based on perceived political or criminal theories, rather than geographical location.

A more fractured environment is also likely to lead to a rise in cybercrime, as criminals perceive law enforcement action to be inefficient, and cybercrime a relatively low-risk high-reward way of making money. Crucially, the perceived ineffectiveness of law enforcement may lead to underreporting of cybercrime incidents and threats by companies, preventing the development of adequate and efficient responses to vulnerabilities.

A growing burden on companies

In 2017 the onus for both compliance and protection is likely to shift further towards companies and away from governments and regulatory bodies. Corporate entities will be responsible for ensuring that all data transfers, protection, storage, breach reporting and cyber security strategies are compliant with relevant legislation – in all the jurisdictions in which they operate. Corporate entities should therefore take great care to examine cyber operations from both a security and technical perspective, including ensuring that they have clear reviews of all data transfer processes, and a wide understanding of any breach reporting and data protection legislation in place.

Just as cyber security shifted from a technical threat for IT teams to a board-level strategic issue at the beginning of the decade, 2017 will move things on again. Instead of the emphasis being on the nature of the threat itself – though companies should maintain a threat-based cyber security strategy – for global companies it is the disparate legal and regulatory nature of cyberspace that will represent the biggest challenge.

Image accreditation: Press Association - The launch if the UK government's new National Cyber Security Strategy, Nov 2016. Chris Radburn/PA Wire.