



Economic crime in the technology sector

As guardians of digital and product security for customers and society as a whole, technology companies set high standards for their security measures.

The financial and reputational impacts can be significant when companies are seen to fall short of the expected standards. Take for example Yahoo, whose sale price was reduced by \$350m after it announced in 2017 that 3 billion user accounts had been compromised following a data breach.

Why the sector is at risk of economic crime



Emergent and disrupted environment



Heightened public and political scrutiny



Highly digitised sector, with high perceived value



Constantly evolving regulatory environment



Significant amounts of Intellectual Property



Interdependence between technology businesses

Specific economic crime challenges



Data breaches

Data breaches can result in the loss of client data, denial of service, ransom and financial loss.



Significant overseas exposure

Global companies will have significant overseas exposure, including a need to engage with public officials which can increase the risk of bribery and corruption.



Shortage of digital and cybersecurity skills

Shortage of available talent can lead to exposures, allied with a risk of cybersecurity issues from the behaviour of employees in a highly digital environment.



Guilt by association

There is a significant risk of guilt by association when technology is used to facilitate criminal activities, often without the company's knowledge.

Spotlight on: Sanctions

Technology companies face particular challenges in navigating the sanctions landscape due to the rapid advancement in products and services; the ease with which technology can be transferred globally; and the difficulties in identifying and restricting user access.

US sanctions, are broad in scope, impacting on any company dealing with US origin products, software or technology, US persons and US owned companies, wherever they are located.

Ensuring compliance with sanctions is vital in light of the recent change in regulatory focus. The use of sanctions by governments and multinational bodies has expanded beyond the financial services industry, to include corporates. Significant fines have been levied on companies in the wider sector. In 2018, for example, US regulators fined a Chinese telecommunications company \$US1.2 billion and placed it under ongoing monitoring for violating Iran and North Korea sanctions.

Helping our clients take action

Unallocated customer funds

An FCA-regulated company that handled significant volumes of cash receipts, sought our assistance with an unallocated cash surplus (the opposite of a “black hole”) totalling £7m.

Our forensic team performed a complex reconciliation of unallocated cash receipts totalling over £500m (using automated and manual methods), which enabled the client to distribute the unallocated funds to customers.

Overseas bribes

A division of a FTSE 100 technology company had concerns that a project in the Middle East was over budget.

Our forensic team examined bank statements and found that bribes had been paid to help expedite customs clearance via a third party agent acting on their behalf. This resulted in a number of individuals being asked to leave the organisation.

Phishing attack

A UK subsidiary of a US-based technology company received a letter purporting to be from one of their key suppliers regarding a change in the supplier's bank account details. This led to the company making a payment to the incorrect bank account.

We performed a forensic investigation comprising interviews and an email review, which resulted in disciplinary action being taken against the guilty parties.



Claire Jolly
Partner
Financial Advisory
+44 161 455 6315
clajolly@deloitte.co.uk



Ian White
Partner
Financial Advisory
+44 20 7303 2225
iwhite@deloitte.co.uk

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients.

Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2020 Deloitte LLP. All rights reserved.

Designed by CoRe Creative Services. RITM0419305