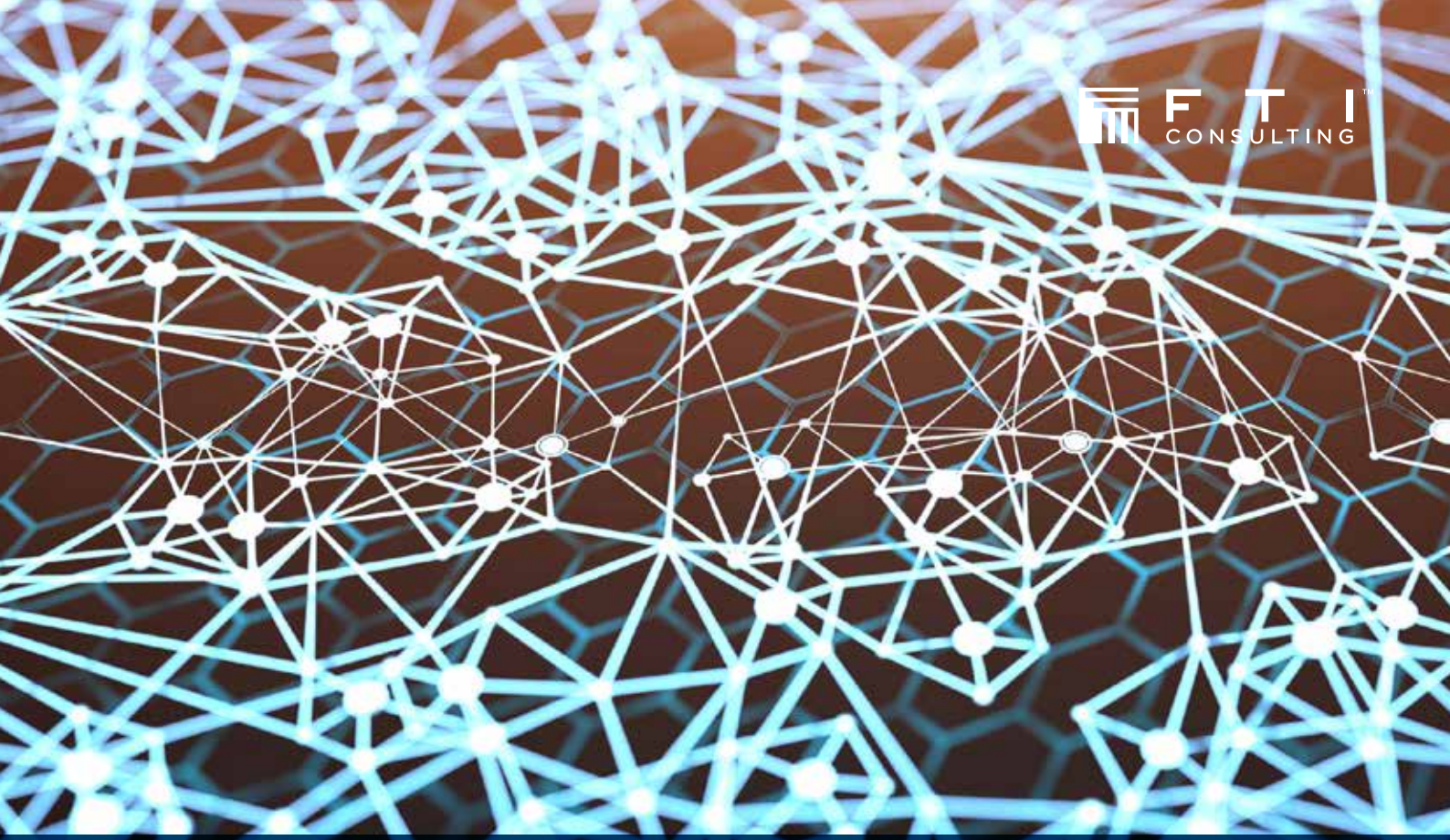

SMALL CRIMES CAN LEAD TO BIG CONSEQUENCES:

Raising Awareness of Cybercrimes and Links to Terrorism

Evolving Digital Environment and the Terror Threat

Cybercrime has been ranked as a top tier threat and combating Cybercrime has become a priority for governments and corporations worldwide. In the UK, both Action Fraud and the National Crime Agency (NCA) have recorded an increase in cybercrime and it has become a preferred avenue for both large and small scale organised crime groups, including terrorists and groups looking to finance terrorist activities. Anyone can purchase tools on the black market to carry out cybercrime which includes activities such as credit card theft, online scams or identity theft. Criminals and terrorists have a great advantage through information and communication technologies to carry out crimes with minimal effort quickly generating funds from multiple small value transactions, which could ultimately lead to the financing of terrorist organisations, individual terrorists and ultimately lead to a terrorist attack.

The financial sector's shift into a more digital environment has made it more susceptible to cyber threats and has led to greater awareness of the emerging sophistication of the cyber-criminal and terrorist. According to the FATF report, 'Emerging Terrorist Financing Risks', methods of terrorist financing continue to evolve in response to changes in technology. Electronic, online and new payment methods pose increasing vulnerability as these systems grow. These electronic and online systems can be assessed globally in jurisdictions with weaker AML/CTF controls and used to rapidly transfer funds.

Small Crimes

In a sense the world of Cybercrime consists of the same financial frauds and scams we have known for years, they are just carried out by a more sophisticated type of criminal exploiting the internet and computers. There has been a large increase in the volume of cyber-attacks by organised criminal gangs and the lines between organised crime and terrorist financing are becoming blurred.

There is a perception that most terrorism and organised crime has a transnational link, however recent acts of terrorism have been characterised as locally grown, domestic or "lone-wolf" attacks. These attacks have become much harder to predict as they can be anyone, anywhere at any time and can be facilitated online through small terrorist cells.

The new age of terrorist attacks are often cheap and effective and organised by small groups or individuals who rely on activities such as purchasing stolen personal identifiable information from the underground economy to carrying out unauthorised transfers or credit card fraud. Hacking for money, making small unauthorised wire transfers from customer accounts has also become a popular way to raise and move funds rapidly. Small sums of money moving their way through financial system and the use of multiple payment accounts are difficult to detect through transaction monitoring systems so the element of intelligence and appropriate due diligence on customers becomes more paramount. It has been noted that Islamic State has used online technology platforms, including online money transfers and prepaid cards to transfer money into its territories.

Small criminal activities can provide terrorists with the quick funds they may need to purchase equipment and weapons.

It takes very little to finance a terrorist attack, for example the U.N estimated the total cost of the London bombings in 2005 was around $14,000 and Finance Minister Michel Sapin has reported the Paris attacks in November 2015 came to approximately $32,000. This contrasts with the larger scale attacks of 9/11 which were reported to have cost between $400,000 and $500,000 according to the final report of the National Commission on Terrorist Attacks.

Funds raised by members of Islamic State in connection with the Paris shootings in November of 2015 were raised by local criminals and have been partially linked to fraud schemes and other financial crimes. Reports indicate that money to finance the attacks was moved in tiny sums often using prepaid credit cards to pay for apartments, transport and weapons. It is important to note that as fraud begins to evolve into the cyber world the terrorists and criminals are evolving as well.

Use of Fintech

In 2011, a terrorist plot discovered in the English city of Birmingham uncovered that terrorist, Rahin Ahmed dabbled in online trading, trading dollars and euros, raised through a fraud scheme, to raise money for a large scale terrorist attack on UK soil. His ability to engage in online forex trading illustrates the difficulty in detecting possible terrorist financing using conventional transaction monitoring. He was able to apply for an online account at Forex Capital Markets Ltd. by exaggerating his experience annual income and net worth. This highlights the importance of appropriate controls and the application of robust customer due diligence procedures.

It has been noted in reports by the Financial Action Taskforce that Islamic State has revolutionised terrorist financing through leveraging new fundraising platforms such as crowdfunding, to effectively market and draw donations using the latest technologies through large groups of people. Often the true reasons for funding campaigns are masked and donors are solicited to contribute under the impression that they are donating for a social and humanitarian cause. The donors in these scenarios may be fully aware of the underlying purpose of the terrorist financing charity or tricked into donating to what appears to be a legitimate cause.

As terrorists are evolving with technology new payment and fundraising methods expose vulnerabilities in our financial systems and security frameworks. They can be accessed globally and used to move funds quickly and anonymously. The new evolution of terrorist financing is reflective of the profile of today's terrorist ranging between the ages of 21 and 35 years, with tech savvy skills and able to compromise systems from the comfort of their own homes.

Cyber Security Awareness

Promoting a culture of cyber security awareness is a key element to the prevention of cybercrime. Employee engagement and awareness is a strong first line of defence against cybercrime. It is important that employees undergo awareness training so they are aware of the different ways in which their organisation can be compromised and the different types of common fraud and cybercrime methodologies.

One of the biggest cybersecurity threats as technology becomes more sophisticated is human failure.

Understanding the key vulnerabilities is the starting point for creating a robust cyber security programme. Employee negligence, a mobile workforce and hacking are the top causes for most breaches.

Cybercrime loss specifically if it can be linked to terrorist financing not only generates a financial or data loss, but can also lead to reputational damage. That is why it is important for institutions to build awareness about the threat and encourage an emphasis from senior management and at the board level. Building a strong governance framework is a key ingredient to a successful cyber security programme. There should be a clear communication that all threats should be taken seriously and reported to law enforcement. The response, escalation and remediation process is an important element of any cyber security framework.

The financial services industry has a vital role to play in combatting terrorism and financial crime. As technology evolves and terrorists and criminals become more sophisticated financial institutions must be vigilant in developing systems and controls within their cybersecurity frameworks to detect and prevent vulnerabilities and breaches.

In this rapidly changing environment it is important to remember that terrorists and criminals are constantly looking for quick and easy ways to raise and move money through any available outlet they can exploit.

Nigel Webb
Senior Managing Director
T +44 (0) 20 3727 1568
M +44 (0) 7786 656278
nigel.webb@fticonsulting.com

Sarah Tomalewicz
Senior Consultant
T +44 20 3727 1169
M +44 78709 18970
sarah.tomalewicz@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc, its management, its subsidiaries, its affiliates, or its other professionals, members or employees.

www.fticonsulting.com

twitter.com/FTIConsulting facebook.com/FTIConsultingInc linkedin.com/company/fti-consulting

©2016 FTI Consulting, Inc. All rights reserved