FINANCIAL SERVICES FACULTY

ICAEW.COM/FSF

ISSUE 131
NOVEMBER 2018

FSFocus

POWER MAD
DID PSYCHOPATHS CAUSE THE 2008 FINANCIAL CRISIS?

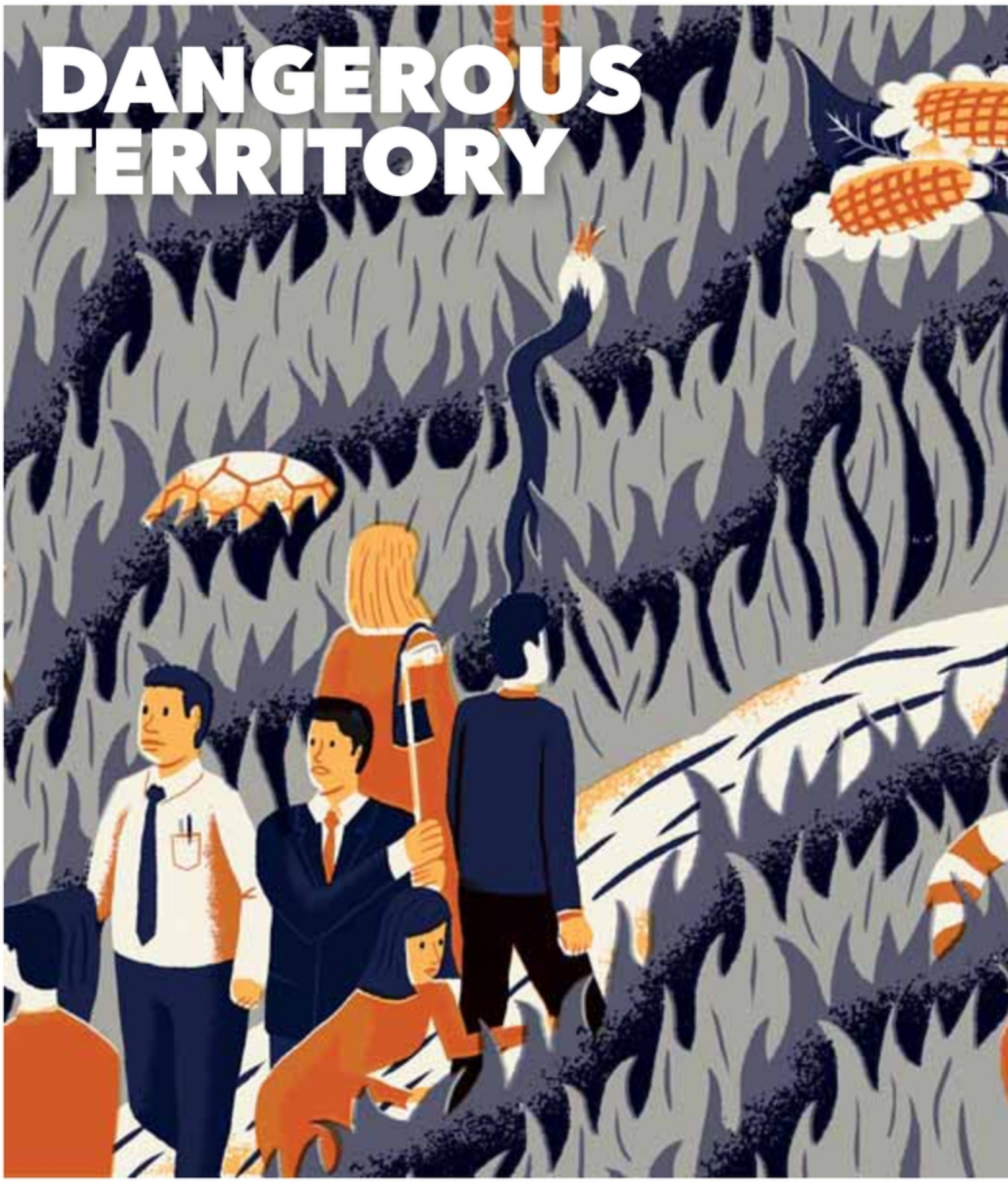
FIGHT FOR EQUALITY
JENNY TOOTH TALKS GENDER, BREXIT AND BUSINESS ANGELS

WEIGHING THE RISK
HOW ZERO-FEE FUNDS FIT INTO THE INVESTMENT PICTURE

FORTIFIED DEFENCE

How can firms improve their tech resilience and prevent cyber attacks?

DANGEROUS TERRITORY



The current political and operational environment is fraught with risk for financial services institutions. Nick Martindale assesses what action firms should take to mitigate any impact

A decade on from the global economic crisis that almost brought the financial system to its knees, banks and other institutions are having to juggle a cocktail of risks; any one of which could have existential repercussions.

The wider political and economic landscape is a major concern, as is the sheer amount of regulatory change - such as MiFID 2, General Data Protection Regulation and the Second Payment Services Directive. "The change that is happening across the sector is leading to increased levels of risk that need to be appropriately managed," says Adnan Saleem, risk governance and controls expert at PA Consulting.

Fraud, including cyber activity (see box), also represents a significant threat to financial institutions, both in the potential to cause serious financial losses but also in the reputational damage it can do. Technology upgrades also represent a serious challenge, as seen in the failed IT projects that have affected firms such as TSB. "If you're a big incumbent financial services institution then legacy IT infrastructure is currently the biggest issue," says Tim Muzio, consultant in the financial services practice at Odgers Interim. "Many of the larger, well-established players have critical technology dating back to the 1960s/1970s. Updating this is the equivalent of changing the engine of a jumbo jet mid-flight, but it needs to be done in order to meet customer expectations and to stay ahead of rising competition."

With such uncertainty, institutions need to develop comprehensive plans to ensure they are prepared for any eventuality, advises Michael James, head of technical architecture at Altus Consulting. "But most firms tend to be reactionary and sporadic in their focus on particular risks. They're not consistent and do it in lumps and bumps, or when regulation comes along."

Brexit is an almost constant question mark on the risk register, says Muzio, and organisations are starting to ramp up preparation for a potential no-deal scenario. "Firms are looking at securing licences in European countries and developing financial services centres so that, in the event of a closed border, they can move employees or roles relatively freely and maintain operations with the EU jurisdiction," he says. Many are also looking at opening shared services centres across different European countries so they have access to talent outside the UK, he adds.

When it comes to fraud, businesses need to put the emphasis on proper preventative measures, says Aziz Rahman, senior partner at law firm Rahman Ravelli. "In simple terms, this involves a thorough, ongoing assessment of the potential for fraud being committed by staff, third parties, intermediaries, customers and trading partners - anyone who has either a connection to the business or knowledge of how it manages its finances. Having a whistleblowing procedure is also essential, he adds, giving staff who suspect wrongdoing the confidence to raise issues.

In the customer-facing space, push payments are also a big problem at the moment, argues Muzio. "Consumers are being conned into setting up these arrangements whereby they are sending money to an unauthorised account, resulting in the loss of millions of pounds for customers and financial services alike. Educating customers is critical if financial

SAM BREWSTER/IKON

institutions are to mitigate this risk. With this in mind, security education and communication is something that many firms have now incorporated into their product offering and services."

Simon Bittlestone, CEO at Metapraxis, says technology can help firms assess and manage the risks they face through the use of historic and current data. "Companies need to understand and closely monitor what actually drives performance within the business, as well as understand the impact market disruptions could have on these drivers," he says. "By analysing both historical and current data, businesses can build up a full, unfiltered picture of the organisation's past, present and potentially future performance, which gives executives the confidence to make effective decisions."

MANAGING SCENARIOS

Scenario modelling techniques can also help management teams to predict the impact of uncontrollable events, he adds. "Changes in consumer demand, Brexit, interest rate changes, a drop in the value of the pound - each of these should be considered when looking to safeguard the future of the business. It really is a case of 'fail to prepare, prepare to fail'."

Richard Lowe, business unit lead for the UK at SQS Group, also stresses the need for a well-rehearsed disaster recovery plan. "Mitigating operational risks can only be achieved with a plan that is second nature to the responsible parties and can be executed in the desired timeline," he says. "No IT solution is completely foolproof, but the key is knowing how a potential internal failure can be mitigated without affecting the overall performance."

"No IT solution is foolproof, but the key is knowing how a potential internal failure can be mitigated without affecting the overall performance"

In future, the use of big data and technologies such as artificial intelligence (AI), machine learning and the Internet of Things (IoT) will help organisations keep a closer eye on risk in real-time. But such technology can also introduce an additional element of risk, and is likely to result in further regulation in the future, says Saleem. "Regulators are exploring ways in which they can continue to adopt RegTech to support regulatory submissions, as well as how blockchain could impact regulation.

"In addition, the increase in adoption of AI technologies, and the often black-box decisions these systems make, is introducing a whole new suite of conduct risks into the business and this is something that the regulators are hugely concerned with."

Dan Turner, CEO of Deep Secure, notes that there are particular concerns around the quality of the data on which decisions - that could potentially be taken by machines in future - are made.

"There are obvious risks around digital purity; if companies cannot provide digitally pure inputs to AI- and machine learning-based systems then they will be tainted or - much worse - weaponised from the start," he warns. "If the financial services sector cannot clean up its act and deliver digital purity, then we can expect further intervention from the regulators."

James Ramenda, senior vice president of enterprise risk at SS&C Technologies, says effective data management needs to be combined with an independent risk analysis process.

"While data should be fully integrated across functions, the process of risk analysis and management should be independent," Ramenda says. "For example, the chief risk officer may report directly to the board of directors. The firm may also use independent, third-party risk monitoring to run parallel with internal systems. These steps are designed to keep risk analysis from being influenced by short-term profit pressures at the expense of the firm's long-term financial health." ●

SECURE TRANSACTIONS: HOW TO STAY ON TOP OF CYBER THREAT

- Protect against malware – be it in the form of viruses, ransomware, keyloggers or rootkits – by installing anti-virus software that regularly scans your system for threats and prevents your employees downloading potentially harmful malware.
- Have a firewall in place to control all points where cyber criminals could access your system, and prevent access to and from potentially malicious IP addresses.
- Install manufacturer patches as soon as they become available – these patches are often issued by software manufacturers to protect against known weaknesses and vulnerabilities.
- Vet your software suppliers to ensure that they put data security at the top of their agenda.
- Develop a cyber-conscious culture – make sure all employees take data security seriously by avoiding easily decipherable passwords, correctly indexing data and triple-checking before they send data outside of your firm.
- Consider purchasing a cyber insurance policy, which can provide access to a range of critical breach response services that help you meet regulatory requirements and keep your business running.