Keith Robertson, Chartered FCSI, long-time investment and financial planning guru at the CISI, has spent much of this spring distilling his seminal – and at times controversial – contributions to the debate on behavioural finance for our Review of Financial Markets. The following pages are a gateway to his full paper, available at cisi.org/rfmq3-18

Robertson believes that “finance has worn a theoretical straightjacket since the end of WWII. The history is fascinating, but not for this paper. At its core, modern financial theory (MFT) is composed of a pick-and-mix collection of individual theoretical conjectures including Modern Portfolio Theory (MFT), the Efficient Markets Model (EMM), the Capital Asset Pricing Model (CAPM) and the Black-Scholes equations for options pricing; this last-mentioned is ignored for current purposes. Also in the mix would be a trio of quasi-behavioural theories: Utility Theory, Expected Utility Theory and Decision Theory”. All these share some common factors, he explains:

- Fundamentally, all are mathematical or econometric ‘models’, but not sufficiently tested to meet the scientific definition of a ‘theory’, like Relativity Theory, Evolutionary Theory, Quantum Theory; far less could any of them hope to ever qualify for the optimal status of being a scientific ‘Law’.
- All have been developed by brilliant minds; yet all remain essentially unproven conjectures.
- A mathematical theorem takes the format: if certain assumptions are true, then a given conclusion follows; ie, the validity of the output rests on the validity of the underlying assumptions used.
- The assumptions in fact used are not to be found in the real world.

“For the sake of good order,” he says, “it is worth stating the assumptions on which MPT is founded. The above clutch of associated hypotheses requires a ‘rational’ and perfect neoclassical economic environment”:  
- All agents/investors will behave rationally to optimise their own economic self-interest.
- All relevant information is freely available and effectively instantly priced into the market.
- Markets are permanently ‘frictionless’, fully liquid, and without costs, taxes or delays in employing dividends, capital and so on.
- Each price change is random, conforming to the Random Walk Hypothesis.
- Each price change is independent of its predecessor and successor price changes.
- Price changes are normally distributed [while this assumption is often termed thus, it is generally accepted that price changes have a lognormal distribution, and returns have a normal distribution].

“All this has resulted in the employment of deductive logic and the general mathematisation of finance, which is where we remain today,” says Robertson. The full paper covers three related aspects of psychological behaviours in finance:

- Psychological biases and traits.
- Prospect Theory, which provides absolutely fundamental insights for advisers.
- The ever-present role in finance of cognitive dissonance and narrative fallacy.

It will certainly spark debate, some of it heated. Feel free to send me your comments, and suggestions, to the email address below. Or tweet to #futureproof. And prepare for a roller-coaster ride through the varied landscapes of financial mathematics and psychology.

George Littlejohn MCSI, editor, Review of Financial Markets, and CISI senior adviser. george.littlejohn@cisi.org

BEHAVIOUR, BLOCKCHAIN, AND CYBER – A BOARDROOM BBC

In July 2018, Britain’s Financial Conduct Authority published its near-final rules on the extension of the Senior Managers and Certification Regime to almost all regulated firms. While the obligations for ‘enhanced’ firms are very similar to those that currently apply to banks, the combination of personal liability for senior managers and the potential of a career crash driven by a conduct breach will mean significant cultural shifts in many firms. Issues around ‘behavioural finance’ – understanding the true needs of clients – the use of blockchain for greater operational and cost efficiency, and dealing with the many-headed Hydra of the cyber threat, all covered in this edition, will feature on many boardroom agendas.
We are all prone to biases, and so the recognition of behavioural finance and its contributions in recent decades is to be welcomed, says long-time financial planning and wealth management expert Keith Robertson. But take care, he warns, to weigh that work against the solid achievements of the mathematical giants – starting with Daniel Bernoulli almost 300 years ago – on whose shoulders much of it stands, oft-times rather shakily. The “asymmetry of skill and knowledge between fee-charging professional and fee-paying layperson ... should prod us into considering whether we are quite as smart as we appear to believe”.

Financial advisers, as a sub-species of Homo sapiens, are remarkably incurious. They have a tendency to accept and absorb any information which looks to help their businesses, without necessarily troubling themselves to subject such information to the higher mental processes. For example, behavioural finance is most often presented [as in Nick Edwards’ briefing paper – see cisi.org/behaviours] as the study of investors’ flawed decisions, caused by naïve misunderstandings and underlying psychological biases. The lack of critical thinking is worrying. Martin Wheatley, as CEO of the shiny new FCA, in 2013 immediately started the ball rolling. He continues to sit on the CISI masters’ level exam panels and forum committees.

Keith Robertson, Chartered FCSI, is among the highest-qualified practitioners in the UK, and spent over 20 years as a practising fee-charging financial planner and investment manager. He continues to turn, should prod us into considering whether we are quite as smart as we appear to believe.

Economics shows that some errors made by consumers are persistent and predictable.” He goes on in like vein with “consumer choice in retail financial products and services is particularly prone to errors,” or “people are generally bad (even terrible) intuitive statisticians and are prone to making systematic errors in decisions involving uncertainty,” and “stress, anxiety, fear of losses and regret, rather than the costs and benefits of the choices, can drive decisions”.

The received opinion in our sector is that investors are really rather stupid, poor things. They make terrible decisions and worse. As advisers, we should therefore tread carefully and be aware how irrational and dangerous customers might be. This view is reinforced by seminars, statements from the regulator, books, and articles, explaining all the biases and errors to which investors are prone. This attitude is dangerously short-sighted. While stupidity exists, and egregious errors are without doubt made in investment, a moment’s thought will show they are made primarily by the investment sector itself, not by retail investors.

After WWII, most stock exchange transactions were still undertaken directly by individuals; not now. The growth of the investment sector, as a sector, has taken place during the past 50 years. Today, for all practical purposes, retail investment (including pension funds) is entirely intermediated. It may be a convenient fiction to maintain that clients make the flawed decisions but, in reality, it is more likely to be advisers who do so. By definition, clients are acting on our advice, not their own fallibility. Clients do not make their own free investment decisions, even if they have signed-off on risk profiles and proposed investment strategy. Clients are overwhelmingly likely to always act under their adviser’s influence. Who, therefore, is making the errors?

**As Smart as We Appear?**

If money is lost in markets it is we, as professional intermediators, who are as likely to have made all the mistakes and irrational choices as the clients whom we ridicule. All the worst things that have happened historically (such as market crashes, illiquidity, major banks and fund managers going bust, zero savings rates, wholesale fraud in foreign exchange, LIBOR, swap contracts, money laundering, mega bailouts, sub-prime mortgages, collateralised debt obligations and other derivative-based investments) have not been the result of behavioural financial errors on the part of private clients. We need to look critically at our behaviour and uncertain knowledge, and consider how much we really understand about the processes we use to manage other people’s money. As in medicine, if things go wrong, it is likely to be our fault, not our clients’. Asymmetry of skill and knowledge, between fee-charging professional and fee-paying layperson, inevitably brings responsibility which, in turn, should prod us into considering whether we are quite as smart as we appear to believe.

For sure, people are prone to biases and making flawed decisions, and the recognition of behavioural finance in recent decades is to be welcomed, but the growing body of work needs to be assessed critically and sceptically and not swallowed whole.

If recent original behavioural research is examined, much of it has nothing to do with investment or finance but simply takes an experimental view of people’s behaviours in certain hypothetical circumstances and contexts. It is unfortunate that researchers find using monetary gambles and simple probability scenarios so useful, because that increases the chance that results will be automatically applied to personal financial decisions and the economic choices which have to be faced in life. Very few (if any) experiments have been done using real people and their own
hard-earned money in real-life scenarios. To the extent that real-life behaviours have been studied, the experiments have been ex-post facto, looking back on historical events and trying to deduce or imply ex-ante behaviours. Such experiments are of course likely to be contaminated by hindsight bias and vulnerable to data-mining to suit researchers’ premises.

In behavioural finance or economics, many of the experiments use graduate and undergraduate students and others in artificial and contrived situations to see how they react to simple probability or lottery type scenarios which, while interesting or amusing, have zilch relevance to real-life financial advice. Numerous (mostly American) papers in the field draw on public statistics, for instance assuming that owning equities is proof of risk appetite, without questioning why subjects own these assets. As in the UK, most investment is mediated and uses collective and multi-asset funds, and automated pension funding. Subjects are thus likely acting under professional guidance or discretionary management, not personal error. Particularly where utility and expected utility responses are being explored, quantitative data is collected, whereas in real life investment scenarios, behaviours and utility are usually qualitative and often deeply personal, quirky, and at odds with theory. A better way to understand behaviour might be to talk to our clients and ask them how they felt, what went through their minds, when markets ineluctably spiralled down in 2007–09. Understanding the sick feeling in the pit of the stomach when one loses much more real money than bargained for is probably a more useful lesson than the behaviour of a group of bright students playing a game with pretend assets in a psychology lab.

So, when considering behavioural finance, it may be worth examining how much some of the errors and ‘irrational’ responses apply to ourselves, rather than classifying them as pitiful characteristics of less-informed clients. And we should remember that it is nearly always the investment sector (not excluding advisers) that does damage to other people’s finances, rather than its being self-inflicted by themselves. Particularly after a market fall, failure by clients to buy undervalued assets is not down to just their irrational fear; it is our failure to explain the cyclical nature of asset markets and the countercyclical behaviour needed to profit from this eternal phenomenon.

### PERSPECTIVE AND CONTEXT

Behavioural economics is interesting in its own right, but the context in which advisers can make use of it is not as a sort of mental ‘I-Spy’ game, observing clients' confused and erroneous notions. It is crucial in understanding our own behaviour when interacting with clients, and realising that the way we present information will determine the strength of the clients’ intellectual grasp and belief in what we tell them. In short, if we appear lucid and confident in what we tell them, it is a racing certainty that clients will accept our advice and recommendations without question. In turn, that means our understanding of our own investment proposition must be impregnable. Clients are overwhelmingly likely to believe and accept what we tell them. Knowing that, we must guard against taking advantage of clients’ relative ignorance, or tricking them, just to benefit (whether knowingly or unthinkingly) from the sorts of psychological biases to which they may be prone.

The elephant in the room is the painful suspicion that, as a sector, financial planners are still subliminally motivated to accumulate assets under influence and get clients fully invested as fast as decently possible, rather than provide well-informed objective advice focused on risk. When an overwhelmingly predominant ‘black box’ process (the by-now orthodox risk profiling-cum-asset allocation (RiPAA) into multi-asset portfolios with systematic rebalancing is embraced by virtually the entire sector, one knows something is not right.

Parroting what others have told us is not sufficient; as their agents, we have to assume a sceptical perspective on behalf of our clients, challenging our centralised investment proposition (CIP) or any investment strategy. Presently, we simply do not challenge what we have embraced; it is easier to believe the herd must be right. Every adviser’s written statement of investment principles and risk should be shown to a third-party with instructions to challenge each element of it, and to provide evidence for accepting or discarding any part of it. Only then should it be given to your clients. There is a legal and ethical duty to have evidence that what you propose to do with other people’s money is likely to work in ‘normal’ conditions and, to the extent it may fail, the conditions in which it will likely not produce the outcomes hoped for. The regulator and courts are concerned not with theory but with outcomes, and the extent to which investors have been educated about the myriad risks they will be exposed to.

### BACK TO THE FUTURE

Behavioural finance is nearly 300 years old. Daniel Bernoulli was certainly on the case by 1738, when he published astonishingly perspicacious work on the theory of risk, and effectively laid the foundations for what would, in the later 20th century, become known as utility theory, expected utility theory, game theory and decision theory, loss-aversion or risk-aversion, prospect theory and the entire notion of subjective relative value. Morgenstern, von Neumann, Kähneman and Tversky et al are today’s known names, but the credit lies with Bernoulli and the 18th- and 19th-century mathematical giants who developed the fields of probability and statistics. Let us consider some uncomfortable and inconvenient truths.

### AUTOMATIC OR REFLECTIVE THINKING

It is unhelpful to make definitive statements on how the brain facilitates decision-making processes. There is good evidence that certain parts of the brain are involved in a range of physical and mental processes, but nobody knows how specific thoughts and
reasoning occur in the brain. Unravelling that physiology is still in its infancy. If neurology is to be included in an article, it is important to not make simple errors of fact. Some claim that the “oldest parts of the brain” are used in the thinking process and lead to uncontrolled actions and decisions, citing reflexes and ‘gut instinct’ as examples. Reflexes form part of the autonomic nervous system, seated and controlled mostly in the hypothalamus and brain stem. This has nothing to do with thinking or decision-making. The whole point is that the ‘old brain’, evolutionarily speaking, cannot be controlled. You cannot ‘think’ your reflexes not to work, it is impossible to ‘think’ yourself to stop breathing or your heart to stop, whether awake or asleep: these functions are autonomous, outside the capacity of anyone to subjectively control.

Even if the reference to ‘gut instinct’ had been defined (it has no meaning otherwise) it has nothing to do with ‘automatic thinking’. Thinking, and other cognitive processes are a function of several parts of the brain working together, but significantly in the frontal cortex; if a thought comes into your head, it has nothing to do with the autonomic nervous system. Thaler and Sunstein in Nudge (2008), and Kahneman in Thinking, fast and slow (2011), speak of “gut instinct” and use the terms “automatic thinking” and “reflective thinking” as System 1 and System 2 respectively, but the words are journalistic shorthand, not scientific terminology.

ANCHORING
This relates to any decision that involves some quantitative or qualitative factor, as there is a well-known tendency to be influenced by a recently-stated number or quantity. Thus, if you try haggling in the souk and the trader starts at a price of 100, and you plan your counter-offer based on that (countering at say 50 or even 30), you are likely to finish up paying more than the item is worth. If you price-check the item elsewhere and find out the ‘correct’ value is 15, you can avoid this common scam. There is ample research, and lots of trick scenarios contrived to illustrate this well-evidenced anchoring phenomenon.

With a high anchor value, people tend to make higher estimates and guesses than if a lower anchor value is used. Advisers might consider whether some questions in a risk-profiling questionnaire are framed in a way to take advantage of this heuristic. Many questionnaires do this, for example using (one presumes) average returns and volatilities to illustrate notional returns on a portfolio over different timescales. Investors are likely to anchor on attractive positive returns when set out against relatively modest losses. Advisers should be alert to such risk in all quantitative scenarios and decide how to explain this to their clients. Not to do so is likely to result in clients giving answers they have been subtly guided towards, and not give the answers they might really wish to have given, had they been more robustly informed. Indeed, the narrative some advisers themselves tell clients, perhaps regarding the long-term average returns from different asset classes, or qualitative ‘soft’ aspects of their proposition, are also subtle ways of getting clients to anchor their expectations on the wrong things. Risk of misguided client expectations will almost always lurk when cashflow modelling uses average returns and variance to generate future scenarios.

AVAILABILITY BIAS
The availability bias is one of the strongest in finance. Just as with anchoring, when you have information presented or hear a theory put forward confidently and persuasively for the first time, the chances are rather high that you will adhere to it. This bias is known in the academic world as the availability error where people tend to focus on recently presented (available) information and give it more weight in their minds. It inhibits critical thinking and is responsible for all sorts of biases. When the film version of Jaws was released in 1975, there was a sharp drop in the number of swimmers off the beaches of both east and west coasts of the USA. This was of course irrational, because the real risk of injury or death was many times higher driving to get to the beach than bathing off it. Making judgements on the basis of the first or most notable thing that comes to mind is the availability error. Your first thought might be right, but easily might not be. Being impressed is not enough to form an objective and rational view. It is so pervasive and subtle that mostly we don’t notice, and it requires a real effort of will and intellect to fight it; these are occasions that require deliberation.

There are two key circumstances in which availability bias acts in financial advice. The first is when the advisory firm explains its whole process to the client: from introductory meeting through risk-profiling and asset allocation to implementation, systematic rebalancing and review meetings. In the absence of anything else, clients are overwhelmingly likely to embrace the entire process, but let us not fool ourselves that this is because they can rationally and systematically analyse the proposal against fact-checked evidence and rate it the best possible approach. Other investors go to other advisers who offer different processes, and there is no reason to suppose that those clients will be any less impressed by their adviser’s approach to planning and investment than yours. There are all sorts of psychological gymnastics going on when people make such choices.

From an investor’s perspective, meeting a new financial planner is likely to fall into the same category as meeting any professional adviser. If one requires any sort of professional help (such as legal, medical, engineering, physiotherapeutic, architectural), one will carry to a first meeting the presumption that the person one meets will be professional, qualified and competent, and that he will be able to provide the advice and action to meet one’s needs. Given the likely asymmetry of knowledge in such encounters, it is not surprising if a layperson wants to accept your proposition, not directly on its merits (because the client cannot objectively judge how good your advice will actually be) but because it is you. There is huge emotional and intellectual inertia in favour of the potential client sticking with you and becoming an actual client. To reject you on any grounds other than an immediate dislike of your personality takes a gigantic effort. He would have to listen to your explanations, understand and remember them, and decide there
was something doubtful about the proposition. He would then have to seek out somebody else, for whom he would need some sort of evidence to suggest was going to be better than you, mentally reconcile the same presumptions about competence (having already discovered he could be wrong about that), have a meeting and once again listen, understand, and then compare the merits of the new proposition with those already rejected. No, it must be close to a racing certainty that, subject to unacceptable behaviour on your part, if a prospect meets you he is going to stay with you.

And there is a further factor. Having invested so much effort and emotion in finding an adviser, the client is going to rate you very highly and recommend you to others. To rate you other than good would mean admitting he had himself been incompetent in selecting his adviser. Perversely, this could also be a subconscious motive for recommending you to acquaintances: by drawing others into the herd, if his worst fears are confirmed and something goes wrong, then at least he will not be in trouble alone.

The preceding three paragraphs describe how the availability error explains the way a client is very likely to sign up with the first adviser he finds and, once signed up, to be a loyal and sticky client – for reasons completely independent of the merits of the actual ‘professional’ proposition. But there is a second way, crucial and insidious, in which this availability bias works – how you, the adviser, selected the process which you retail to your clients.

In a very short time, say 20 years, the intermediary sector has embraced and sold-on to retail investors myriad investment strategies. Before the millennium we were still in the with-profits era, and then followed core-and-satellite, mean-variance optimised (MVO) ‘efficient frontier’ portfolios, passive and index investing, 60:40 asset allocation, model portfolios, multi-manager, multi-asset, to name a few, until now we have the ubiquitous risk profiling-cum-asset allocation (RiPAA) with systematic rebalancing of a multi-asset portfolio. Why? It is unavoidably true that not one of these processes came from within the intermediary sector; all have been fed to advisers from the fund managers, discretionary investment advisers (DIMs), platforms – the sell-side of the sector in general. One doubts whether a single adviser in the UK can say “This is truly my own process, and here is the evidence for how and why I think it works.” Stop and think: every adviser will have changed its investment proposition at least once, often more, in the past twenty years. Is this because every adviser has individually striven to improve what he does and all have come independently to a similar conclusion, or because it is fundamentally easier to market a similar process to everyone else and hope that someone somewhere has done the work to ensure this strategy is better than the old one?

Every adviser has at some point been to a presentation, or read in the trade press, where an investment process, probably RiPAA, looks and sounds impressive enough to re-sell to their retail clients. Better still, every other adviser seems to be using the same process – herd protection! This near universal adoption of a single investment process is not because of its inherent merits – those have never been vindicated to any sensible standard – it is because each adviser has fallen victim to the availability bias. It looks good, sounds good, and clients seem to think so too (how would they know better?), other people are using it, so let’s also use it. No need to look further or too deeply into what we are doing. As a class, the willingness of the intermediary sector to hand over their clients’ money to sell-side operators and DIMs, without serious examination or understanding of whether the chosen strategy is demonstrably in those clients’ best interests, is as powerful a demonstration of availability bias as can be imagined. Their clients’ own surrender to the availability of their marketing story should not be taken as evidence that any of the agents and actors in this arrangement truly understand what is going on.

There is a related availability error – the halo effect. This is where one particularly salient (available) characteristic of a person stands out early in your acquaintance. This is why people can form false views of film stars, based on the sorts of roles they portray or how charmingly they smile. We ascribe all sorts of other characteristics to them or the value of what they say without any evidence or rational basis for doing so.

(This is also why first impressions are critically important, and why job interviews so often result in bad appointments.)

Combining these two types of irrationality and relating them to the investment world, if you hear a presentation by someone eminent, a chief investment officer or chief economist in the financial world, an academic with a string of letters after his name, an author (even of the quality of Thaler, Sunstein, or Taleb) with a catalogue of well-reviewed books, then obviously what such a person says has a much greater impact on you than something you might hear from, say, a colleague. Of course, often it may be the case that a leading authority is deemed to be so for good reason; but it is totally irrational to assume all you hear from any plausible source is immutable truth without subjecting it to critical thought. There are many sources of information open, and one should never make a decision on managing other people’s money on a single opinion or theory, no matter how attractive. But we live in a post-truth world, where wanting to believe something is right is equivalent to proof that a thing is right.

// HAVE ADVISERS FALLEN VICTIM TO THE AVAILABILITY BIAS? //

JOIN THE DEBATE
Keith Robertson’s full paper is available online at cisi.org/ftmq3-18. He will be discussing the implications of his work at a special Masterclass for Chartered Members and Fellows in London on the evening of Monday 24 September 2018, and at a CPD event in the CISI office in London on Wednesday 3 October 2018, which will be available to members globally by live webcast. Full details at cisi.org/events

John von Neumann (1903-1957) was a Hungarian-American mathematician, physicist, computer scientist, and polymath. He made major contributions to a number of fields, including economics, computing and statistics.
DISTRIBUTED LEDGER TECHNOLOGIES - AN EMERGING CONSENSUS ON THE BUY-SIDE

BLOCKCHAIN HAS SLIPPED THE SHACKLES OF BITCOIN. IT HAS A VITAL ROLE TO PLAY ON THE BUY-SIDE, SAY IAN HUNT AND CHRIS MILLS

Asset management clients are becoming increasingly demanding, diverse, and knowledgeable – irrespective of their retail, institutional or wholesale beginnings. Research by Dr Ian Hunt and Chris Mills on distributed ledger technologies – DLT, aka ‘blockchain’ – indicates that “their expectations of investment outcomes are sharpening, their tolerance of poor customer service is disappearing, and their delivery mechanisms are now expected to include modern digital media.”

FAVOURED DLT USE-CASES FOR ASSET MANAGERS

As a part of the analysis carried out for the report, asset managers and other buy-side participants were canvassed for their favoured distributed ledger (DL) use-cases: these are the potential developments in DL technology with the best capability to deliver the benefits outlined above, and which are therefore of most direct benefit to the asset management and asset owner community. There is an emerging buy-side consensus on these use-cases, which reflects an increasingly strong ambition to yield the available benefits of DL technology.

The use-cases which offer benefit to the buy-side are often different from those with attractions for the sell-side. Payment banks, for example, tend to focus on the potential of DLT to accelerate the settlement of high-volume and cross-border payments and foreign exchange. These are useful and sensible initiatives, but of limited direct interest to asset managers. There is considerable sell-side interest in blockchain applications in trade finance too, which again is relevant but of limited appeal on the buy-side.

In the developed markets, a distinguishing factor in the establishment of successful DLT initiatives has been the existence of a dominant market infrastructure provider (like the ASX in Australia) which can mandate change. However, the focus of DLT initiatives is by no means confined to developed markets: emerging markets are seen as attractive contexts for DLT development in the shorter term. The absence of complex regulation, the relatively simpler market structures and the smaller number of entities are all positive factors in the business case for change. Some participants went as far as to see emerging markets as the obvious starting point for buy-side DLT initiatives. Generally, the most accessible use-cases combine high value (to maximise the business case) with lower volumes, limited complexity and a small number of participants.

A subset of the relevant buy-side use-cases depend on ‘network-effect’, and would need to be delivered in the context of cross-industry cooperation; they are therefore logistically demanding. In each case, a collaborative structure would need to be established, and appropriate incentives provided for the developer of the application. Incentivisation is an issue, as in a network DL, there is no central controlling entity which will receive revenue benefit from its operation.

Other use-cases would not require wide-scale cooperation, and asset managers could make progress independently, or with a single cooperative counterpart, client or regulator. Collaboration would be limited or not required. Deployment of ledger and blockchain technology internally within an asset manager can offer real benefits (albeit generally less than those achievable from an industry-wide service), as well as making early progress easier to achieve, so the incentive for development would be transparent to the manager. For certain applications, there is a halfway house: managers could develop ledger platforms internally or in small-scale collaboration, and then deploy DLT to distribute the ledgers across counterparties, clients, regulators and service providers.

The most prominent initiatives, with the potential for progression by individual managers or small participations, are set out below. Their sequence is a reflection of the frequency with which they are cited by the respondents to the research:

1. Asset register or Investment Book of Record (IBOR), to deliver a position data service based on a single ledger of transactions. This could eliminate the maintenance of multiple internal books of record, reduce the need for internal reconciliations and provide better flexibility in the position records provided to users and applications.

2. Secure identity, to deliver a distributed entity data service, with embedded and shared ‘know your customer’ (KYC) and anti-money laundering (AML) checks. This could facilitate disclosure, eliminate parallel maintenance of client/entity data, reduce inefficiencies in client onboarding, support compliance with GDPR and reduce costs.

3. Smart contracts, to deliver practical automation to the processing of more complex asset classes. This could streamline the agreement and life-cycle management of OTC contracts, make complex loans and real estate accessible to conventional investment vehicles, standardise the application of compliance rules, and reduce costs.*

4. Direct reporting access, to deliver a ‘self-service’ report data extract capability for regulators and clients, based on a permissioned ledger. This could improve transparency, reduce the time and effort spent in report production and reporting data management, and reduce costs.

5. Repo/securities financing, to deliver near-instantaneous settlement for funding transactions. This could extend the scope of netting, make bilateral repo available as a source of liquidity to the buy-side, and reduce the cost of funding.

6. Collateral management, to automate the computation, agreement and movement of collateral on a day-to-day basis.

*While this use case is targeted to support the more efficient processing of more complex assets, it will be important to start simple, and graduate to the complex — hence repo, simpler loans, money market instruments and mortgages may be addressed ahead of OTCs, for example.
A sector-wide, distributed asset trading and settlement on ledger. To approval for widespread peer-to-peer existence of this service as a prerequisite can be expected to insist on the transactions are both peer-to-peer transactions, and clearly essential where those transactions are both peer-to-peer and instantly settled. Regulators can be expected to insist on the existence of this service as a prerequisite to approval for widespread peer-to-peer trading and settlement on ledger.

A sector-wide, distributed asset register/position data service. This would enable us to rationalise the current proliferation of asset registers, deliver higher-quality position data, reduce external reconciliations, and reduce costs. The position data management functions of custodians, accountants, depositories and transfer agents would evanescence accordingly. And liquidity management and reduce exposure to central utilities, improve cash and liquidity management and reduce costs.

Peer-to-peer distribution, to link asset managers and fund manufacturers directly to their end clients, and to eliminate the currently high cost of retail platforms and distributors. Criteria would have to be maintained (probably as part of the entity data service) to ensure that client/product suitability is preserved in a peer-to-peer context.

In addition to the use-cases listed above, about which there is a degree of consensus among the buy-side contributors*, there are other use-cases proposed by smaller numbers of asset managers. Some of these are of specific interest to those managers, while others are more generally accessible, but of lower expected benefit. Examples include:

- Transfer agency (TA): this is a business well-suited to the rationalised ownership registers which DLT can facilitate, but relatively limited in financial benefit because of the already low cost of TA as a proportion of the cost of investment (outside the KYC and AML processes addressed above). There is, however, a benefit in making ownership records immutable, particularly in jurisdictions where corruption is prevalent.
- Proxy voting services: this uses a distributed ledger to communicate with registered asset owners, and smart contracts to capture and process the votes. This could operate on a peer-to-peer basis, or as a custodian-led service which should result in an improved service at lower cost to the asset manager/asset owner.
- Class actions: in a similar form to proxy voting, the record of a class action could be published, and participants could attach themselves as class members, through a shared ledger.
- Smart contract-based margin payments in digital coin for contracts for difference and exchange-traded derivatives: this is a subset of the application of smart contracts to complex asset processing, and may be a useful starting point due to relatively low volumes and (currently) thin regulation. The current clearing process and T+1 reconciliation is inefficient and outdated. A DLT-based solution could speed up clearing and guarantee agreed positions on trade date, thereby reducing execution and clearing risk.
- Asset ownership and provenance tracking: this is a use-case of potentially high benefit to managers with insurance businesses, and to those managing exotic assets, but of more limited interest to managers of conventional securities.
- Open inventory: the manager could give permissioned access to segments of their inventory, to enable offers to buy or borrow stock. Lending could move from a custodian-led activity to an asset manager process.
- Immutable storage: blockchains can be used to store a secure and accurate history of key investment documentation, and make access available in a permissioned form. Examples include: investment management agreements, key investor information documents, legal entity identifiers and records, client reports, and records of client positions and transactions.

WHAT THE BUY-SIDE NEEDS ITS PARTNERS TO DO
Asset managers cannot deliver the potential benefits of distributed ledgers to themselves and to their clients in isolation. There is a strong buy-side vendor community, and a set of outsource service providers on whom asset managers depend to varying extents for technology and operational efficiency. Benefits will often be delivered through their platforms. The regulators have a responsibility to facilitate and encourage beneficial change, and there is a need for standards bodies to broaden

---

*For example, in Q1 2017, KPMG published a buy-side paper, ‘Getting Practical’, which highlighted three of the listed use-cases: distribution, post-trade (middle office/clearing) and asset registry (for DLT enablement).
their scope to standardise new interactions within a DLT framework.

The full report sets out the main planks of support which asset managers need from their various partners to accelerate and maximise the delivery of benefit, starting with the regulators. While there are some areas where DLT can be deployed to deliver benefits within existing regulations, it is clear that proactive and constructive support from its regulators, in reshaping regulation where necessary, will facilitate and accelerate the buy-side’s deployment of distributed ledger technology.

New business models and new investment products will inevitably require changes to current regulatory frameworks. If the regulators do not take a positive stance, then this will at best delay, and at worst prevent the delivery of a substantial slice of the potential buy-side benefits of DLT. If the regulators clearly identify the potential benefits of the technology, and create a favourable regulatory environment, then this will drive commitment and investment from the buy-side, and accelerate the delivery of benefit.

The disruption caused by the new technology is likely to impact regulation, alongside other activities and buy-side business processes, and regulators will experience their own transformation. It is not just the rules that will change. The ways in which regulators monitor behaviour and access reporting data will change, along with the mechanisms of enforcement. One manager sees that “real-time surveillance and interpretation of data will be key themes and could foreseeably change how policy is implemented”.

Managers emphasise the need for a cooperative approach with the regulators. One said that the ‘regulators need to gain comfort with technology, understand the implications for marketplaces in financial services and approve, or legislate, key infrastructure. Furthermore, they will need to decide on the degree of oversight and transparency they require from DLT-based transactions ... we emphasise the need for a constructive engagement with the regulator’.

REGULATORS’ OPENNESS AND INTERACTION

There are well-publicised instances of governments and regulators trying to wrest control away from DLT/blockchain innovators and establish a regulatory framework. High-profile examples are China’s ban on ICOs and the SEC’s inclusion of DAO tokens (from the so-called ‘Decentralised Autonomous Organisation’) as securities under the Securities Exchange Act. However, there is no sense on the buy-side that the regulators are negative about, or do not want to engage with the technology.

One representative manager asserted a belief that “the regulators in the UK are generally supportive to blockchain development”. An FCA Discussion paper on distributed ledger technology, April 2017, bears this out, and suggests an openness to understand and embrace the technology. “We are committed to fostering innovation that advances our objectives ... DLT is an example of rapidly developing technology which offers exciting potential to support the needs of consumers and the market ... We are particularly interested to explore where the balance of risk and opportunities may lie in relation to DLT.” Respondents to the FCA consultation were positive too, and expressed “particular support for the FCA maintaining a ‘technology-neutral’ approach to regulation and welcomed the FCA’s open and proactive approach to new technology”.

Elsewhere there are encouraging instances of positive support from regulators for DLT-based initiatives. Northern Trust’s Private Equity initiative was actively supported by the Guernsey Financial Services Commission (GFSC). The design aimed to deliver compliance with current, local regulations, and to allow regulatory access when required. The GFSC was keen to accelerate the delivery of the benefits of trust and transparency that DLT could clearly enable. The GFSC stated that “Northern Trust has engaged with us as regulators from the start and we are pleased with the level of openness and interaction. This is another example of the Commission’s approach to innovation in the Bailiwick’s financial services sector”.

There are promising signs in Europe too. ESMA, in its paper dated February 2017, is equally positive, and asserts that it wants “to understand both the benefits and the risks that DLT may introduce to securities markets, and how it maps to existing EU regulation. In turn, our aim is to assess whether there is a need for regulatory action to facilitate the emergence of the benefits or to mitigate risks that may arise”.

The French Regulator AMF has launched a new initiative focused on initial coin offerings, as it looks to formalise a regulatory framework for the blockchain use case. The Luxembourgian regulators have taken positive stances on DLT too.

The full report on which this Distributed ledger technology – an emerging consensus on the buy-side, is available by emailing co-author

### REGULATORS NEED TO GAIN COMFORT WITH TECHNOLOGY, AND UNDERSTAND THE IMPLICATIONS FOR MARKETPLACES ###

**Dr Ian Hunt**

is a well-known authority on buy-side business process and technology, with a strong reputation in order management, risk, derivatives and investment automation.

**IAN@HUNT.ORG**

**Chris Mills**

is MD UK & EU of Stradegi Consulting. He has 19 years’ experience in the asset management sector, most recently at KPMG where he was head of Blockchain UK, global head of fintech wealth.

**CHRISS.MILLS@STRADEGI.COM**

DLT WEBCAST

Chris Mills will join Keith Bear of IBM and Paul Sinthunont of AITE in a CISI webinar on themes raised in his report on 11 September 2018.

**DETAILS AT CISI.ORG/EVENTS**

*Emma Bailey, director of the investment supervision and policy division of the GFSC.*
INCIDENT REPORTING IN CYBER SECURITY

WITH THE CYBER THREAT NOW BITING MOST FIRMS’ ANKLES, THE REGULATORS NEED TO KEEP TRACK OF THE DAMAGE, SAYS RICHARD PARLOUR

In June 2018, a joint Centre for European Policy Studies – European Credit Research Institute (CEPS–ECRI)* task force published a major report on ‘Cyber security in finance – getting the policy mix right’. A key element of this in the securities and investment sector is incident reporting requirements, and in this excerpt from the report on this area, Richard Parlour, a UK solicitor renowned for his expertise in financial crime, and his colleagues outline key recommendations. Richard Parlour acted as chairman of the group. Sylvain Bouyon, head of fintech and retail finance at CEPS and ECRI, and Simon Krause, visiting researcher at CEPS, were rapporteurs. Mr Parlour will be discussing the outcomes of the report at a CISI CPD seminar on 24 September. The seminar will also be available on CISI TV. And he will be chairing a Fellows and Chartered Members masterclass on 25 October. For details please visit cisi.org/events. He welcomes comments or questions to his email address (top right).

This paper includes references to endnotes, which are on page 13.

With the inexorable rise of ecommerce comes the inexorable rise of the ecriminal. Cyber crime is now the world’s fastest growing crime. It has leapt to number two of the top ten business risks worldwide, from not even appearing in that list five years ago. For certain countries, cyber attack is now the risk of greatest concern. Gone are the days of concern about a low-level hack of a website by a script kiddie. Today’s attackers are multi-faceted and increasing in sophistication, ranging from advanced persistent threats, corporate espionage, organised crime and ‘hactivists’ to cyber terrorists, ever more competent, and ever better funded. Cyber security has moved from being a technical issue to a political and boardroom issue. Financial markets are particularly important as they oil the wheels of all major economies. So what should the priorities of cyber security be? Is the rise of cyber crime so fast and extensive that we should be changing the focus more to one of cyber resilience? There are three core themes to address:

1. Governance (at all of organisational, international and national levels).
2. Risk management (both contextually and intelligence driven).
3. Capability (cyber security by design and by default, using a standard framework applied to context).

There are a multitude of issues that the financial sector needs to address. Our task force has chosen to focus on certain key issues rather than attempt to produce an encyclopaedic tome. Any report can only represent a snapshot in time and it will be particularly important to continue to communicate as technology and the threat advances. I hope that the work that our task force has undertaken in producing this report will make a valuable contribution to the advancement of cyber security policy and protection and safeguarding of the economies of the EU member states and the financial markets on which they depend.

1.1 INCREASE IN LEGISLATION WITH INCIDENT REPORTING REQUIREMENTS

Several recent new EU regulations and directives include incident reporting requirements in the event of a cyber breach. The requirements for an institution or data controller to report or notify specific authorities, and in some cases the public, in the event of a cyber breach are notably covered in the following legislation:

• General Data Protection Regulation (GDPR) in Articles 33 and 34
• Payment Service Directive 2 (PSD2) in Article 96 as well as the corresponding European Banking Authority (EBA) Guidelines
• Directive on Security of Network and Information Systems (NIS) in Articles 6, 14 and 16
• Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) in Article 19
• Cyber incident reporting of the European Central Bank (ECB)5
• TARGET2

As shown in Table 1, high fragmentation can be observed between rules in taxonomy for reporting, reporting time frame, the template to be used and the threshold to trigger an incident. For instance, whereas there is no undue delay in the reporting time frame for the NIS, the deadline is 72 hours for the GDPR, 24 hours for the eIDAS and 48 hours for Target2. The template is not clearly defined in GDPR and NIS, while it is

*ECRI is an independent think tank that carries out research and contributes to the policy debate on financial services in Europe. It is managed by CEPS, a leading think tank covering a broad range of policies in EU affairs. This report is based on discussions in the CEPS-ECRI task force on ‘Cybersecurity in finance: getting the policy mix right’. The group met four times between September 2017 and May 2018. The policy recommendations offered at the beginning of this report reflect a general consensus reached by task force members, although not every member agrees with every aspect of each recommendation. A list of task force members, observers and invited guests can be found in the Annex to the main report. The members were given the opportunity to comment on the draft final report, but its contents may only be attributed to the rapporteurs and do not necessarily represent the views of the institutions to which the members belong.
Similarly, the eIDAS Regulation requests data breach has a high risk to impact consumers without undue delay if the institution has already done so, to inform supervisory authority, unless the financial security incident. The GDPR requires the which have been affected by a cyber security incident. The NIS Directive and TARGET2 regulations might further raise the degree of this fragmentation. Moreover, the reporting requirements are characterised by discretion, meaning that for instance financial institutions are obliged to assess consumers' personal and financial risks arising from a data breach. Therefore, the consumer dimension and scope of cyber incident reporting as well as the difficulties due to legal fragmentations should not be underestimated.

1.2 NEED TO DEVELOP A COMMON TAXONOMY FOR INCIDENT REPORTING

The development of a common taxonomy for incident reporting is needed for various reasons. First, as cyber space is global, cyber insecurity is often a multi-country issue. Often, similar patterns of threat can simultaneously affect organisations located in different countries. As such, cross-border exchange of information is needed to address cyber security issues better and manage cyber incidents efficiently and effectively. Fragmentation in taxonomies across jurisdictions is likely to impede the efficiency of cross-border exchanges of information, as the process of understanding the incident could be slower. As such, convergence in taxonomies should contribute to help respond to multi-country cyber attacks better.

Second, as shown in Table 1, there is an increase in incident reporting requirements. A standard taxonomy, adopted across all regulations and directives, regardless of whether it is on a cross-border basis, should facilitate smooth and efficient interactions between authorities and computer security incident response teams (CSIRTs), especially by contributing to avoiding inconsistencies in the reported information.

In principle, the creation of a distinct taxonomy for each piece of legislation should not be justifiable. Finally, as emphasised by the European Union Agency for Network and Information Security (ENISA) (2018), persistent fragmentation in taxonomies will slow the emergence of automation in incident reporting and responses.

Nevertheless, the development of a common taxonomy for incident reporting would not only...

---

**TABLE 1. CONDITIONS FOR INCIDENT REPORTING BY TYPE OF RULE**

<table>
<thead>
<tr>
<th>Reporting authority</th>
<th>Taxonomy for reporting</th>
<th>Reporting time frame</th>
<th>Template to send report</th>
<th>Threshold to trigger an incident</th>
<th>Reporting to consumers</th>
<th>Threshold to</th>
<th>Reporting to</th>
<th>Reporting to</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>High-level guideline</td>
<td>Within 72 hours</td>
<td>N/A</td>
<td>Provided via scenarios/examples in doc</td>
<td>Yes, reporting is required if data breach is likely to result in a high risk to the rights and freedoms of affected consumers</td>
<td>N/A</td>
<td>Yes, provided via doc</td>
<td>Yes, provided via doc</td>
</tr>
</tbody>
</table>
| NIS                 | N/A                    | Without undue delay  | N/A                     | N/A                             | Yes, provided via guideline from ENISA | N/A             | Yes, provided via doc | No additional information provided for the eIDAS (via document for the European Network and Information Security Agency (ENISA) reporting but not defined in member states) and for TARGET2 (via document in Annex II). The development of a common taxonomy for incident reporting is needed for various reasons. First, as cyber space is global, cyber insecurity is often a multi-country issue. Often, similar patterns of threat can simultaneously affect organisations located in different countries. As such, cross-border exchange of information is needed to address cyber security issues better and manage cyber incidents efficiently and effectively. Fragmentation in taxonomies across jurisdictions is likely to impede the efficiency of cross-border exchanges of information, as the process of understanding the incident could be slower. As such, convergence in taxonomies should contribute to help respond to multi-country cyber attacks better. Second, as shown in Table 1, there is an increase in incident reporting requirements. A standard taxonomy, adopted across all regulations and directives, regardless of whether it is on a cross-border basis, should facilitate smooth and efficient interactions between authorities and computer security incident response teams (CSIRTs), especially by contributing to avoiding inconsistencies in the reported information. In principle, the creation of a distinct taxonomy for each piece of legislation should not be justifiable. Finally, as emphasised by the European Union Agency for Network and Information Security (ENISA) (2018), persistent fragmentation in taxonomies will slow the emergence of automation in incident reporting and responses. Nevertheless, the development of a common taxonomy for incident reporting would not only...
faces specific challenges. First, cyber space is constantly evolving. As a result, cyber attacks are changing on a regular basis and new forms of attacks continuously appear. A non-flexible taxonomy that sets rigid standards for long periods is therefore ill-adapted.

Second, existing taxonomies are often designed for specific economic sectors or companies. Organisations often have different needs and expectations. As such, CSIRTs often end up developing their own incident classifications for internal use (ENISA, 2018).

As highlighted by ENISA (2018), one possibility for strengthening convergence in incident taxonomies is to develop a centralised repository for hosting all relevant taxonomies. Questions remain about which body should be in charge of such a task. Given the global nature of many cyber attacks, it would a priori make sense to design a global repository. But the development of a final consensus at the global scale might be unrealistic. Therefore, as a first step, it would be preferable to focus on an EU depository developed by the EU agency in charge of cyber security, namely ENISA.

The next objective would be to develop only one taxonomy that encompasses all the processes in the scope. This taxonomy should include specific sections to cover the variants applicable to the different sectors, if relevant. Given the constant changes in the type and nature of cyber attacks, the common taxonomy should also be sufficiently flexible to be continuously updated.*

**1.3 NEED TO DEVELOP AN EFFICIENT LEGISLATIVE AND INSTITUTIONAL FRAMEWORK FOR INCIDENT REPORTING**

The emergence of different reporting requirements raises questions about the most adequate legislative and institutional framework for shaping the relationships between CSIRTs and authorities. Eventually, the objective is to ensure that the framework helps financial firms protect themselves from cyber attacks and, in case of cyber attacks, helps these firms activate timely and efficient responses.

Responses that are timely and efficient should contribute to limiting the short-term and mid-term damages to firms and, in some circumstances, are likely to prevent the expansion of attacks to other firms and sectors. The framework as developed should aim at reinforcing cyber resilience and business continuity as much as possible. In order to do so, regulators, supervisors and financial firms should focus on the following five issues.

### Issue 1. Convergence in templates across the EU

For each piece of legislation whose purpose is to develop incident reporting, convergence in templates should be ensured across the EU. This priority concerns mainly the NIS Directive and the GDPR, as related templates should be primarily defined at national level. As regards the GDPR, one of the roles of the Data Protection Article 29 Working Party and the European Data Protection Board (the latter replaced the former once GDPR took effect, see Recital 139 of GDPR) should be to reinforce the harmonisation in those national templates.

### Issue 2. Adequate governance at group level

For financial firms that have activities across different jurisdictions, high fragmentation in templates and typologies could impede the ability of CSIRTs to understand the overall picture of the incidents impacting the banking group. Against this background, the banking group could be compliant with the respective incident reporting requirements at national level, while not being able to understand holistically what is at stake. Effective governance at HQ level, with adequate consolidation processes of the ‘overall cyber risk’ at group level, is therefore also needed. This is a key condition for the authority in charge to have a clear idea of the overall level of risks triggered by specific cyber incidents.

### Issue 3. Assessing the possibilities to develop an infrastructure with bidirectional flows

At present, all incident reporting processes are defined with a single direction flow, from CSIRTs to authorities in charge. None of the legislation emphasises or designs two-way flows. There was a broad consensus within the task force that a bidirectional process with respect to incident reporting will eventually be needed. In other words,

---

*For example ENISA (2018) promotes the use of ‘Other’ or ‘Unknown’ in the ‘Tag’ field by the owners of taxonomies as an indicator to revise taxonomies. This field can be used if there is an increase in that category with incidents or events of the same.*

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Authorities</th>
<th>Financial firms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS Directive</td>
<td>National NIS Authority</td>
<td>Operator Essential Service (OES)</td>
<td>Banks and financial institutions are considered as OES because they (a) provide a service which is essential for the maintenance or critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service.</td>
</tr>
<tr>
<td>GDPR</td>
<td>National Data Protection Authority</td>
<td>Personal Data Processor/Controller</td>
<td>Banks and financial institutions operate both as processor, which processes personal data on behalf of the controller, and controller which determines the purposes and means of the processing of personal data.</td>
</tr>
<tr>
<td>eIDAS Regulation</td>
<td>National Certification Authority</td>
<td>Trust Service Providers</td>
<td>Banks and financial institutions can operate with their trust services either as a qualified or as a non-qualifies trust service provider.</td>
</tr>
<tr>
<td>PSD2</td>
<td>NCA/EBA/ECB*</td>
<td>Payment Services Providers</td>
<td>Banks and financial institutions operating as Payment Service Providers.</td>
</tr>
<tr>
<td>ECB/SSM</td>
<td>ECB/Joint Supervisory Team</td>
<td>Significant Institutions</td>
<td>The ECB classify a bank as Significant or Not Significant based upon the criteria of size, economic importance, cross-border activities and direct public financial assistance.</td>
</tr>
<tr>
<td>ECB TARGET 2</td>
<td>National Central Bank/ TARGET 2</td>
<td>TARGET 2 Participants</td>
<td>A distinction is made between critical participants and non-critical participants depending on the market share in terms of value and/or the type of transaction processed.</td>
</tr>
</tbody>
</table>

* Incident reporting in the context of PSD2 has to be sent to the National Competent Authority (NCA), which sends it to the EBA, which sends it to the ECB.

Source: Intesa Sanpaolo.
authorities should be able to exploit the content of incident reporting to inform and advise CSIRTs in return.

One of the options to achieve two-way flows concerns the development of specific network infrastructure channels that provide secure messaging services. This would imply that financial firms use a common application to report incidents. The development of SWIFT messages on the interbank market could be inspirational in this respect. In the end, information about cyber incidents could be sent and received in a secure, standardised and reliable environment.

This model should contribute to streamlining incident reporting processes. High standardisation of templates should in principle increase processing speed and response. Given that speed is one of the main criteria for coping with large-scale cyber attacks, this benefit could be precious.

However, one of the main issues to address in order to create a common application for cyber incidents concerns the nature and type of information encoded in the message. The diversity of templates across pieces of legislation (and likely, for two of them, across countries) can be justified by the fact that each piece of legislation has a specific purpose. The development of standard messages should ensure that this diversity can be replicated in that new system. The different authorities need to be able to retrieve the right information within the expected time. There is a significant risk that incident reporting based on standard messaging services might end up being too generic to be adequately exploited by CSIRTs and authorities.

**Harmonisation of templates is a clear policy objective, but given the different purposes of the pieces of legislation as well as different interests pursued by national regulators, complete harmonisation will be very challenging. Yet it is worth striving for a more convergent implementation of European or international standards of templates. There are indeed possibilities for harmonisation within the existing legal framework for cyber incident reporting. For example, parts of the Target2 template are similar to the NIS template provided by ENISA. The sections ‘description of the incident’, ‘cause of the incident’ and ‘remedial action’ in the Target2 template are likely the same information as the sections ‘general description of the security incident’, ‘detailed causes’ and ‘mitigating security measures’ of the corresponding NIS template. Therefore, European harmonisation should start within the existing regulations and their templates, taxonomies and reporting standards before the policy process can move on to cushion the fragmentation between the different templates.

Should the financial sector decide in any event to go in that direction, questions would remain about the funding of such an application: Should it be funded by financial firms? By governments, for the sake of cyber security? Or should it be a hybrid model combining both funding channels?

### Issue 4. Assessing the possibility of developing a centralised hub

A hub should be developed with the objective of centralising all incident reports and dispatching them to the right authorities. The hub could be in charge of incident reporting for the whole financial sector and handle relationships with all concerned authorities, regardless of whether these authorities are national or European, and cover all sectors or only the financial sector. In return, the hub would be in charge of informing and advising financial firms on cyber incidents. By centralising all incident reports for the financial sector, the hub would have a broad and clear picture at any given time of the cyber risks in this sector.

Strong analytical capabilities would be needed in this respect. The purpose would not be to have a hub that is only a dispatcher of incident reports.

The hub could also play the role of a coordinator between, on the one hand, all authorities in charge and, on the other hand, authorities and CSIRTs. Given the global nature of cyber insecurity, the hub should be established at European level. The mandate of existing European agencies such as ENISA could be significantly extended to cover these complex tasks or a new agency could be built from scratch to focus primarily on these attributes.

A priori, the former option that builds upon the existing institutional framework would be preferable. The objective is to avoid the multiplication of EU agencies that cover broadly similar topics. But, in order to be able to handle all reporting requirements and distribute key information to the right stakeholder, the chosen agency will need a large amount of resources in terms of staff and budget. In order to fulfil its mission of technical adviser, the centralised hub would also need a clear mandate from regulators.

### Issue 5. Assessing the possibility of covering all economic sectors

So far, many of the recorded large-scale cyber attacks not only have affected more than one country; they have also disrupted more than one sector. The institutional framework therefore needs to handle a multi-sectoral dimension. The objective is to ensure that any cyber attacks are confined to one or a few firms in a specific sector and do not spread to others. If there is for example a high risk of a cyber incident spreading from the energy sector to the financial sector, the supervisor should be able to provide real-time information to financial firms on the nature of the attack and, if possible, on the best way to respond to it.

Two options can be considered to cover the multi-sectoral dimension of cyber attacks. The first is to build a centralised hub that is in charge of all sectors including the financial one. The second concerns the establishment of a multi-sectoral network for cyber incidents where one hub is developed for each sector of the economy, eg, finance, energy, telecommunications, food. Each hub would be in charge of one given economic sector for everything that relates to the dispatching of incident reports, such as notification and advice of firms in return, coordination of all stakeholders. In order to handle multi-sectoral attacks, a network of sectoral hubs would be established, preferably at European level, with a hub of hubs.

The preferred option should be the centralised hub for the whole EU economy. One of the main risks of a network of sectoral hubs is the development of sectoral silos that struggle to find agreement on relevant topics.

Richard Parlour will be addressing the issues raised in his report at the CISI on 24 September 2018 in a live webcast meeting, and also at a special Masterclass for Chartered Members and Fellows on 25 October 2018, both in London. Details at cisi.org/events
Endnotes

1. GDPR text
2. Payment Service Directive 2 text
3. Directive on Security of Network and Information Systems
4. Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) in Article 19
5. Some elements on ECB incident reporting can be found here
6. Some TARGET 2 elements can be found here. Contrary to PSD2, eIDAS, GDPR and NIS, TARGET2 is a market infrastructure rather than legislation. TARGET2 provides some guidelines that request concerned firms to notify the national central banks in case of incident.
7. See Reference incident classification taxonomy: task force status and way forward, ENISA, January 2018
8. For the financial sector, given the existing distribution of tasks between multiple supervisors (including national central banks, European central bank, twin-peak models including one supervisor for the macro-prudential part and another for micro-prudential tasks), the development of a new body to cover the tasks of a sectoral hub at the European level might be the preferred option.