THE NETWORK FORUM

Connecting Financial Institutions Worldwide

STATE OF THE NATION REPORT

Key Industry Findings From TNF Annual Meeting 2019

Part 3: Technology

Crypto-asset investing needs an institutional-quality infrastructure ~

The securities services industry is host to more than one view of the impact of technology on its business. “Clearly, the investment, the scale and the technology necessary to be a player in post-trade is quite significant,” said a panellist. “I do not see a long line of new entrants entering this space in the near-term.” He pointed to T2S, which took more than a decade to complete a single settlement platform for Europe, falling behind its timetable, exceeding its budget and being forced to raise its prices after failing to meet its volume targets, as a deterrent.

Another panellist argued that technology could never substitute for capital (which reassures clients they will be made whole if assets go missing) or trust (the belief that the promise will be honoured). But a third panellist thought this was a complacent view. “Capital and trust are still big barriers to entry,” he warned. “But within the product are a lot of areas that could go elsewhere, either through new apps or through new technologies. Unfortunately, if you decimate your product, if you take away pieces of your product, you will be left with the capital and trust but you will lose a lot of what your clients see as being your great value.”

Other panellists, working closely with FinTechs, agreed that clients were the decisive factor. A sub-custodian, currently working with FinTechs on the potential for tokenised or digitised assets to replace securities, said the spur behind the work was client demand: investors are interested in marketable digital assets as an asset class. The opportunity for custodians, she thought, is that institutional investors will not purchase tokens until they are comfortable with every aspect of the environment, including law, regulation, governance, control, operations, standardisation and inter-operability.

Immature regulation and investment costs inhibit crypto-asset investing ~

The ability of custodians to respond to the opportunity, she added, is constrained by regulation – or, rather, the lack of regulation. “A lot of work must be done with regulators, which needs to be a country-by-country discipline,” she explained. “Where the hell do you launch first? What are the things you need to prepare with the regulator? The sandbox helps, but there is huge amount of work to do in that regard, which frankly we under-estimated. To sit with a technical solution that works, but you cannot bring it to bear, is very frustrating.”

Another major obstacle is the need for new technologies such as DLT to inter-operate with legacy technologies at the banks, because it is hard to build a business case for the wholesale replacement of legacy technologies when they work well enough to support current needs.

One reason SWIFT has enjoyed rapid success with its transparency-enhancing and transaction-tracking global payments initiative (gpi), for example, is that it offers a novel benefit – real-time transaction management, as opposed to point-to-point messaging – without requiring wholesale replacement of existing technologies. In fact, it is now being extended from correspondent banking to securities.

In the same way, SWIFT is providing Australian market participants with an alternative to a direct connection to the new distributed ledge technology (DLT) platform the ASX is building with Digital Asset to replace its ageing CSD technology.

That said, SWIFT has a direct interest in DLT too. It is trialling with R3 Corda a link with gpi which will allow trade finance banks to create transactions on a DLT platform provided by R3 Corda and then confirm and settle them via SWIFT. “The promise of Corda is that two systems both see the same version of the truth,” explained a panellist. “What I see is what you see, and what you see is what I see. When we talk about Corda and SWIFT, both systems will see the same version of the truth without one or two or ten people in between looking at something manually to make sure that those two systems do actually represent the same thing.”

As the panellist pointed out, achieving the elimination of the need for physical reconciliation is easily taken for granted, but it entails a great deal of work to deliver even in a proof-of-concept. Raising the DLT breakthrough to an industrial scale in trading, clearing and settlement infrastructures is the next challenge, he said, for traditional as well as digital assets. His firm is working with SWIFT to confirm trade finance transactions agreed on SWIFT and to support the digital exchange being built by SIX.

DLT needs to move from proofs-of-concept into production ~

"In the DLT space, there has been lots of innovation, lots of experimentation and lots of try-it-out projects over the last few years," he said. "2019-20 is about moving things into production." He pointed to projects which had proved they work with a single trade, and networks that were functioning with a handful of participants, whose challenge now was to support "serious volumes that actually move the industry and make people sit up and realise this technology brings real business benefits for the end-users - the issuers and investors."

He was less confident that banks would act quickly. Although the securities industry was adept at the experimental and proof-of-concept stages, he said, it was less successful at the transition to scale. He conceded that the pace of change was bound to be slower in a highly regulated industry like banking, but argued that too many established businesses thought technology alone could be transformational. "We are finding that getting familiar with the technology is not the sticking point," he said. "It is really about taking that next step."

A sub-custodian admitted that banks could get caught up in the technological excitement, particularly if they were based in a financial centre with a lot of digital currencies being issued and FinTechs starting up. "The whole thing becomes very infectious," said the sub-custodian. "You are very strongly driven and influenced by the marketplace in which you operate and the clients and counterparties that you are working with." But, she added, "transforming the business is damn tough. You know it is going to be tough before you start, but there are always things that surprise you."

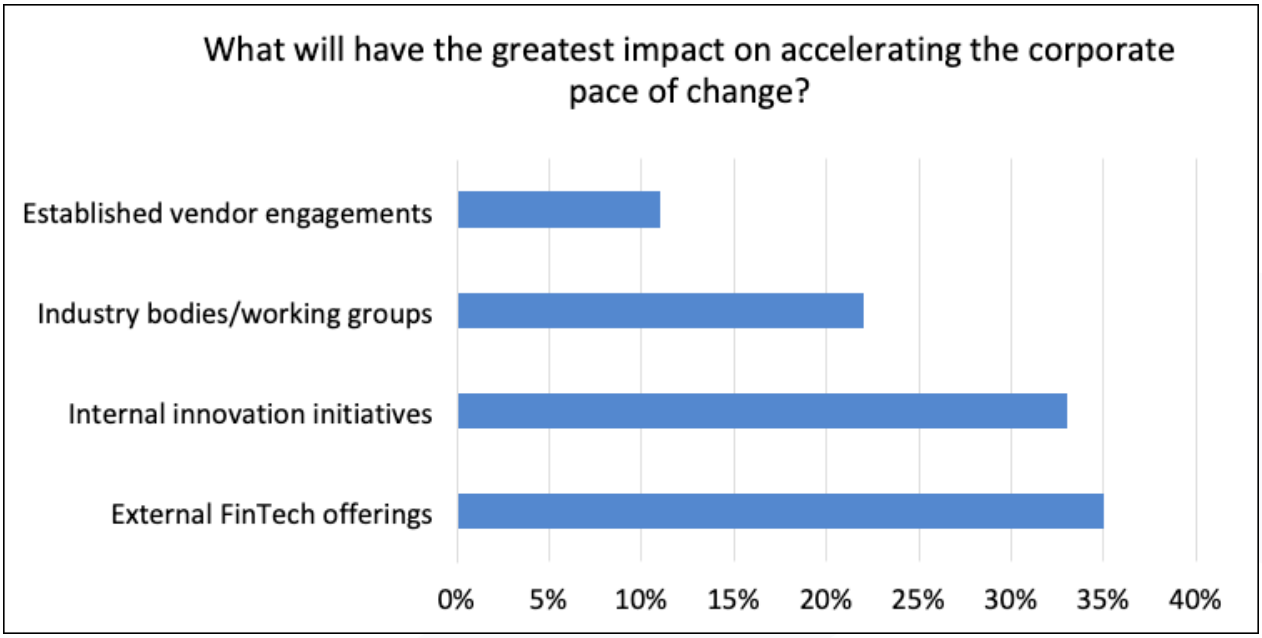

Chart 22.

A poll of the audience disagreed to some extent, with a third of respondents contending that internal innovation initiatives were the most promising accelerator of change (see Chart 22). A panellist found this surprising. "It is a great way to get learning into the organisation, but the critical next step is linking those innovation initiatives to lines of business with P&Ls and real business users who are crying out for a real business outcome," he said.

Obstacles to rapid technological progress ~

A sub-custodian was surprised by the low level of confidence in established vendors. “Coming from a large institution, sometimes the starting point where you have already got an existing partner that you are working with, that knows your organisation, that you have got a track record of delivery between you, that can be a much easier starting point,” she said. “Establishing a formal relationship with a FinTech is dead hard for a bank to do.”

Another panellist agreed, saying he has seen “real progress, real benefits” from established vendor engagements. He added that the acceleration of progress could not occur in vacuum: market participants had to build a business case for change and then agree to work together to deliver it, through standardisation and inter-operability. This inevitably took time. SWIFT, for example, is often criticised for innovating too slowly, but it proceeds quickly once a goal is set and an industry consensus is established to move towards it.

A panellist thought there were alternatives to waiting for a consensus to form. He noted that social networks had turned industries on their heads by the simple device of focusing intently on the identities of users. Similarly, supply chain offerings had transformed the cost of inventory by switching to a “push” rather than a “pull” approach.
“Part of the role of external FinTech offerings is to show what is possible, what you can do,” he explained. “If you look at the challenger banks, they have done a very good job at packaging a sexy brand with a very simple and engaging user experience and the trust that you can hold your deposits there very easily. That is the type of thing that you can easily take into broader B2B markets.”

A sub-custodian agreed. “If you cannot do that satisfactorily, you are increasing the likelihood of your own demise or disintermediation,” she said. “On so many topics, we have become internally focused, and are missing opportunities in the world around us.” She alluded to the gap between the fast adoption of the latest technologies (such as Siri, Alexa, Google Home and self-driving cars) by consumers and the slow replacement of existing technologies in the securities services industry.

Incremental steps are the best guarantee of progress ~

Engineering breakthroughs can help accelerate progress. In fact, technology tends to the exponential rather than the linear form of progression. The miniaturisation of transistors on silicon chips, for example, had transformed the price-power ratio of computing.

Quantum computing might yet have a similar effect. “But none of us should sit back and wait for that transformational moment,” said a sub-custodian. “The journey is about evolution, not revolution. What is the immediate problem to solve? What step can be taken today to increase our learning, knowledge and experience?”

Another panellist agreed. “To be truly effective, digital transformation has to be really boring,” she said. “It must be about basic problem-solving. Innovation is bottom up. It comes from people in the business solving problems. There is no point having an Innovation Lab and blue sky thinking; that is too ivory tower and top-down. Success means putting developers into businesses to solve particular problems.”

This view met with the approval of another panellist. “Are we going to be able to get to this Utopian end-state where it is one system and one source of truth for the payment leg, the securities leg, the identification and the rest of it?” he asked. “That is a long way off. But if we just take it step by step, that will still deliver and take us up the incline that we are looking for.”

A sub-custodian argued that the incline could be steepened if banks were able to change their culture. “Banks generally are still sluggish and still slow,” she said. “Our process and our discipline is not conducive to the world that we need to embrace. So how do we make ourselves agile, in every sense of the word? How do we get the organisation fit for what it needs to get done over the next decade?” A large part of the answer, she thought, lay in creating a cultural environment that attracted diverse technological talent.

Technology talent prefers open source code ~

Another panellist identified an obvious obstacle to that transformation: under-investment in the back office. “Banks do not care about operations staff,” she said. “The stuff operations staff have to use at work is so far behind their personal experience that they feel they are joining an organisation that is doomed to fail. In the banks, the rock stars are still the traders.”

A further problem is high turnover in senior management (which means projects lose sponsors) and an overly bureaucratic decision-making process (which means innovative technologies struggle to escape endless internal meetings).

A custodian added that clients as well as staff were likely to be disappointed by the experience of ageing technology, which further dents staff morale. “As individuals, we have got all this technology at our fingertips on our smartphones, but that is not replicated in our industry at the moment,” she said. “It creates an expectation from our clients too. Certainly, we are driving our digital strategy at a rate of knots, and have various goals to achieve by 2020, but [the client experience] is one of the drivers we need to follow up on.”

According to one panellist, what technology talent values above all is a commitment to open source software. “Open source will be a competitive differentiator,” she said. “Although senior management will be nervous of adopting open source, it is a source of tech talent. You should not talk about AI, machine learning and blockchain but about open source development. That is the way to attract and retain talent because talent does not want on work on closed source products. Open source is as important to our industry as any of the other tech buzzwords.”

At present, custodian banks are consuming more open source code than they are contributing, because it enables them to leapfrog intermediate stages of development. Internal lawyers are hostile to sharing code, on grounds of retaining both intellectual property and competitive advantage. Chief information security officers – and regulators - worry that using and contributing open source code arms hackers, criminals and terrorists with maps of internal systems.

But adopting it looks unavoidable if the industry is to meet what a panellist called “one of the biggest challenges ever to the industry”: attracting talented developers and data scientists. “The competition for tech talent has never been more fierce and I can see no reason why that trend should diminish in any way, shape or form,” said a panellist. However, she was also able to list four techniques for competing successfully for the best talent.

How to make your firm more attractive to technology talent ~

The first was to insist on diversity, by age, gender, ethnicity and sexual orientation. “At the heart of technology lies diversity,” she said. “When you have people that have different experiences and different skills and different mind-sets you can fail fast and bring technology to market more quickly and without bias. Do not look in the same places you always have. Not just LGBT and cognitive diversity either but think about age. Five generations are working in your organisation already.”

The second was to refresh the middle layer of management - “the male, pale and stale” - by “reverse mentoring.” She urged middle managers to “actively hunt out the people in your organisation that are nothing like you” because “if you mentor someone that looks exactly like you that is just imparting what you believe to be your wisdom upon your team rather than truly engaging and listening.” She also advised sponsoring rising managerial talent, as opposed to mentoring it. “It is incredibly important that they understand a career pathway,” she said.

The third was to be flexible about working hours and methods and organisational structures. “`Presenteeism’ can destroy your ability to perform,” she warned. Simple measures such as letting employees work from home one day a week could transform morale. However, success also depends on seamless handovers of work-in-progress from one group of employees to the next.

She also urged firms to accommodate returning parents. “The biggest untapped group of employees you can imagine is parents returning from maternity leave and paternity leave,” she said. “The organisations that get that right are transforming themselves.” But other methods could help. A custodian said one way the bank attracted technology and data talent was to give people time and space to pursue their own projects at work.

The fourth technique is to ensure that new entrants experience a meaningful corporate culture as soon as they start work. “For the younger employee, purpose matters,” she said. “What Millennials want above all else is a sense of purpose. If you want to engage and retain and inspire that level of talent make sure they understand why you exist and why you matter, because if you do not the Googles and the Netflixes and the Amazons are itching to take them on.”

An estimated 40 percent of Millennials have a business on the side, chiefly to give them a sense of purpose, and FinTechs are better at capitalising on that motivation. Innovate Finance has estimated that 75,000 people in the United Kingdom are working at FinTechs already and that by 2030 their number will have risen to 100,000.

“If you do not take care of this, the world is finding out about you, through web sites like Glassdoor,” she said. “Talent is using not-very-sophisticated social media tools to find out about you before they even meet you. Culture matters above and beyond anything else.”

A custodian agreed. In his view, there is more than enough talent working in new technologies such as DLT, artificial intelligence (AI) and machine learning. The challenge was to attract them into the banking industry at all, then into individual banks, and then retain them.

“Somebody said they retain them six to 12 months,” he said. “We retain them a bit longer than that, but if you look at where the unwanted attrition is occurring, it is generally in these fields. This is where culture becomes super-important in the organisation. Look at us. Most of us are dressed up in ties and suits. Most of them do not want to wear ties and suits.”

Data management is a competitive differentiator ~

The reason banks need talented technologists and data scientists is to remain competitive in their chosen businesses. For example, working out how to make data management a profit-generating activity is a commercial imperative in an industry where both transaction fees and ad valorem charges are under downward pressure. “The differentiator is not on fees any-more,” as a custodian put it. “We are all at rock-bottom. The differentiator is technology and data. Data is important, not just to be efficient, but to provide new services to clients.”

It is nevertheless easier to gauge the contribution data can make to operational efficiency. One panellist was openly sceptical that the industry could turn data into money. “We do not see data as a source of new revenue,” he said. “It is often talked about like that, but nobody is willing to pay for it.”

Cost-saving measures, on the other hand - greater inter-operability through APIs, DLT networks and AI and machine learning, even RPA – all depend for their success on high quality, accurate data exchangeable in convenient formats. “If you have a learning robot, and you teach it with bad data, it is just going to behave badly,” as a panellist put it. It matters because as a poll of the audience revealed, RPA is easily the most popular of the advanced technologies being used in the industry (see Chart 23).

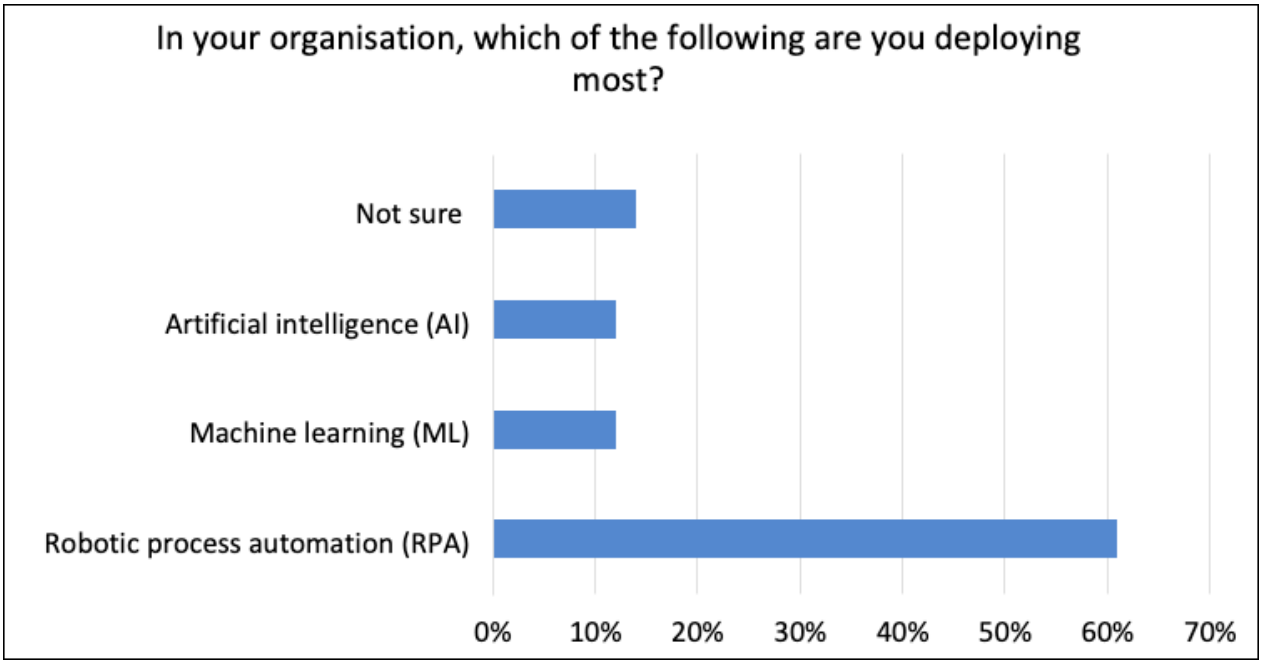

Chart 23.

A second panellist agreed on the importance of data to operational efficiency. "Everything we are talking about in the industry comes down to data management, to the ability to collect and cleanse and normalise data," he said. "It is at the root of every challenge." To take a topical example, one custodian is using AI to sift through settlement data to predict transactions likely to fail and propose possible solutions, with a focus on the highest value transactions. What makes the investment worthwhile is the financial penalties and buy-in costs associated with the CSDR.

"There is a process that has to be followed in a certain order," explained a panellist. "If you get the data wrong, and do not fix the data, and jump into something that could be a game-changer, it is going to be a game-changer in the wrong way. You have to get the data right. There are four areas where AI could be a game-changer – efficiency, risk management, investment management, such as allocations, and improving the client experience. These are areas which could leverage AI to create something very different from what we have today, but the basis is the data."

Securities services industry data is fragmented and inaccessible ~

The difficulty for the industry is that its data is not readily accessible. It is an obstacle to working with FinTechs. "It takes us three months to give them access to our data," noted a custodian. Another panellist agreed that custodians have not "normalised the data and put it into place where you can have an open innovation model. We cannot say today that the data is available somewhere in the Cloud so we can open up to FinTechs. The infrastructure is not yet at the point where we can say, `Let's collaborate.'"

Another custodian said his bank is using RPA to sort its data out before it can apply the technology to problems. "We have a plethora of legacy systems and databases and data sources that have generated data all over the place," he explained. "We had to bring all this data together manually before we could do anything intelligent – or unintelligent – with it. We have leveraged RPA quite significantly to try and bring the different silos that we have and put them in the same place so that we can create some form of data lake that we can eventually use for something else."

In reality, the securities services industry has struggled with data access and quality issues of this kind for decades. “We talk now about structured and unstructured data but the problems are the same as they were 20 years ago,” said a panellist. “Is it complete? Is it accurate? Is it timely? Can I make a decision based on it?” All that has changed, he argued, is the speed at which clean and accurate data is now demanded. “Forget end-of-day, T+1 or T+2 – I need to know 15 minutes ago what my positions were and what my exposure is,” he said.

But another panellist countered that the need for data management is of more recent provenance because “90 per cent of the data in existence was created in the last ten years” as the “world has shifted to digital,” and data production is now on an “exponential growth path.”

Data management, in other words, is not an issue the industry had to manage in quite the same way in the past. “No matter what you do, you are faced with this notion that data will influence either your process, your decision-making or how you execute,” she said. “It may make you irrelevant or enhance your ability to guide your clients. It is not an issue we had five years ago.”

Then or now, banks - being large organisations with legacy technologies and well-entrenched business silos - naturally struggle to manage data. One solution proffered by a panellist is to use third party providers armed with advanced technologies such as AI and machine learning to “surface” (via APIs) and “consolidate and externalise” data trapped in the various parts of a bank, so it can be used.

Another panellist was not convinced. “Outsourcing your data management problems does not solve your data management problems,” he said. He added that using third party providers would also create a need for fresh regulation to govern their activities. A custodian was not dismayed by that prospect. He contended that was a good argument for clients to rely on (heavily regulated) banks to manage their data.

Cloud technology can help firms meet data management challenges ~

An alternative way forward in data management for banks was identified. This was readier adoption of Cloud technology. At present, the average Tier 1 bank uses the Cloud to meet less than 10 per cent of its needs. “Adoption of Cloud is fastest in areas like marketing materials and client-facing analytics, and research and development, but not in post-trade operations or legacy technology or portfolio accounting,” explained a panellist.

Banks have also focused on the potential of the Cloud to cut costs rather than help the business solve data storage problems. One panellist thought that the Cloud, in tandem with open source coding and APIs, could do much more. In particular, he argued, it could furnish the securities services industry with exactly the databank it needs to generate revenue from data.

“When you move your environment into this open type of infrastructure, and open approach, then you can really unlock the power of data,” explained the panellist. “There is a huge opportunity for the post-trade industry overall, when you look at the data which is managed and captured in your post-trade systems. At the moment it is all locked away in black boxes, but if you open up that data, it is the one place in your organisation where you have all the transactional history of your clients. It is fully reconciled. It is the information that is supporting your books and records. It is the true golden source and, if you can get to a place where you can query and analyse this data, that is when we are talking revenue opportunities.”

At present, however, banks are suspicious of the Cloud. “There is massive cultural resistance to Cloud, because people did not grow up with it,” said a panellist. “It can cause delays, and errors, and so people are nervous about doing Cloud. Feedback on Cloud providers is also mixed. People do not want to be locked in, so there is a lot of multi-Cloud to reduce concentration risk, and a lot of mainframes still being used.”

Nevertheless, another panellist detects “a growing realisation” at banks that they cannot exploit new technologies without investing in new systems. “You need to address the root cause and you need to look at the underlying infrastructure rather than just take what you can get out of legacy systems,” he said. “It does not happen overnight. But if you do not address the

root cause and migrate to modern infrastructure, you are always going to have these challenges. The average age of a European securities settlement system is 36-years-old. No matter how much machine learning and robotic process automation you put around a legacy system, you still have that inherent issue."

Refurbishing legacy technology is a false economy ~

Another panellist expressed surprise that banks so often chose to extend legacy technologies to solve new problems. Successful organisations, in his opinion, used new technologies to solve new problems. By that means, they are able to remain relevant to the future without putting their existing business at risk. It is a fallacy, he thought, to save money by using old technologies, because the long-term support costs outweigh the short-term gains. "Stop extending the legacy," was the succinct verdict of one panellist.

However, there is constant tension within large organisations between the pressure to innovate and the need to perform financially. Data management is often the first investment to be cut in a downturn because it is, as one panellist put it, "nebulous." But a panellist identified a larger inhibitor to the development and implementation of an effective data management strategy. This is that the industry is asking the wrong questions about data.

"There is a whole world of data that is being created and could be captured," said a custodian. "We have tended to think in the context of, `What data do I need to do something?' rather than `What data is there for me to capture?'" said a panellist. "I do not know if I am going to need it yet, I am just going to capture it now and, who knows, I might need it in the future. That is one of the shifts that is happening. Everybody believes there is something in the data that we can get value out of, whether it is something we can commercialise or make an operational efficiency out of. If we were then to go round and say, `Tell me the one thing [we can do with this data],' we might come up with 150 different answers. Or you might say you do not know yet. That is the reality. We just need to capture everything. We need to stop thinking about it and actually start capturing all that data."

Regulatory reports are a rich source of structured data ~

There are easier opportunities to exploit, thought another panellist, such as the data created by an increase in the number of reporting fields under MIFID II from 24 to 65. "I see very few people taking that enriched information, which is about their clients, and really working on that," he said.

A custodian thought the lack of interest stemmed from the fact the data was collected on behalf of regulators, but another saw the increase in regulatory reporting as an opportunity. "What an opportunity to build the collection mechanism for all that data and start to use it, rather than just say, `How do I, at minimal cost, make sure that I adhere to that regulation?'" he asked.

A second panellist agreed that regulatory reporting is a "good instance of where our industry has opportunity and continues to get it wrong. I cannot name a global organisation with regulatory challenges in different regions and business lines using the same solution. They have built silos."

As he warned, "once you have two of something, you cannot rely on either." A custodian concurred, saying "we remain concerned about having silos of new technology." A solution might be to press regulators for more relaxed deadlines, so better data management tools for regulatory reporting can be built. It could, thought a panellist, create a "virtuous circle."

But another panellist was concerned about the backward-looking nature of the data being collected today. "Typically, a computer learns from the past, from history," he warned. "We all know there are events where suddenly something changes completely, which wipes out the relevance of the history. How are going to deal with that?"

Which is why he thought the most rewarding prospect of AI was not better control of present circumstances but a release for human beings from data overload, allowing them to make better-informed judgment calls instead.

“The evolution towards a much more data-driven way of organising business lines is going to be the key success factor,” he said. “When you look at it today, the same data is actually maintained in different places within the same organisation and across organisations. We really need to start looking at data transversally, as case of information that goes through a life-cycle during the life of a security. And from there use technology to build deep insights, so that human beings can augment the insights with their own judgment.”

Views differ on whether the industry will seize the crypto-asset opportunity ~

This preference for an incremental approach, and a blending of methods old and new, is characteristic of the approach of the industry to another technology-driven opportunity-cum-threat: the crypto-currencies, crypto-assets and asset-backed tokens spawned by DLT. Naturally, these new and rapidly evolving asset classes present the securities services industry with challenging problems of adjustment.

A custodian saw the size of the opportunity. In his view, the European Union (EU) could achieve its goal of a single European capital market overnight if it switched to DLT. “You can switch it on tomorrow with a blockchain,” he said. “It is not geographically restricted, and you just allow every European citizen to interact with it and buy and sell securities. You immediately have, tomorrow, a European capital market. It is as simple as that. All this legacy infrastructure that we have is not there anymore. The investment for the banks would be small, because blockchain is fully machine-readable.”

As he pointed out, adolescent children are already buying and selling digital assets they cannot or will not obtain from ordinary shops on the Internet and paying for them with crypto-currency. “When they grow up and want to invest their money instead, where will he go?” he asked. “He will not go into a bank branch, and he will not listen to his father telling him it is not as regulated, and there is no stock exchange. He will say, `My friend made a lot of money from this last year.’ He will want to interact with truly digital assets and buy and sell them.”

He predicted corporate issuers would catch up, because digital asset markets will be a cheaper source of capital. Yet the same panellist was not optimistic that banks could change quickly enough to seize these opportunities. “As a bank we try to see which applications in our current infrastructure can use parts of the underlying technology of Bitcoin to establish a different or alternative future for the capital markets,” he explained.

He said the main difficulty in moving quickly was the sunk cost of the existing infrastructure and the weight of staff numbers invested in the status quo. “If I go to our operations guys, five people are interested in the digital assets world, and a thousand people have a job in the old world,” as he put it.

Not all bankers fear the deadweight of legacy. “We do not fear the new business because we can exist also in the new world,” said one. “As soon as we have a fully renovated secondary market for securities, it will remain the same more or less but we will have more automation and offer cheaper services. Reconciliations will no longer be required, for example, because it is already on the blockchain. So I see a lot of opportunities to have the same business in a different operating model.”

The implication – notably of an end to reconciliations – is that employment in the back office will be hit harder by new technology than the front office, even after making allowance for new roles such as custody of private keys to digital assets issued on to DLT networks. “I do not think the front office people should be totally relaxed,” warned another panellist. “Do we need investment bankers in the future? I can perfectly well imagine a world without investment bankers, salespeople and traders, and related activities.”

Front office people will still be required, as a panellist put it, to “create a product” – but in much smaller numbers. A prediction is that five in a hundred of current jobs are likely to survive, in the front office as well as the back, but other roles will emerge to take their place. “Those of us who are old enough can remember when we cut off coupons,” said a panellist. “Those jobs are now gone. Do we miss them? The people, yes. But the jobs? Probably not.”

He added that, unless the securities industry moved as rapidly to shift from electronic book-entry to fully digital securities as it did from physical to electronic book entry securities, it would not be able to capitalise on the new technology. He was not hopeful. “There are so many vested interests like CSDs, custodians, investment bankers, investors, stock exchanges, the taxman, the regulators, the central banks, the government,” he said. “Unless they are all aligned, we will not be able to reap the benefits of going DLT in the securities space.”

He thought change was possible only if entire “eco-systems – countries, markets, entities or institutions – agreed to go to another place.” The example of ASX, which will run its existing settlement system alongside its new DLT system for a prolonged transition period – showed how challenging it is to achieve this “traction, momentum” and “critical mass” even in one country. “If liquidity is not there, the whole thing is dead,” he concluded.

However, the DLT version of Stock Connect in Hong Kong was advanced as an example of a new technology attracting exactly that “critical mass.” As a panellist pointed out, “it is going to have decent volumes, and it could be a template for a lot of the developments that are happening elsewhere.” But on the whole custodian banks will struggle to endorse a fully open financial system based on DLT.

The use-cases and proofs-of-concept they have pursued tend to prefer “permissioned” DLT networks. “As a bank we can only interact with counterparties we have approved as counterparties, and that we want in the system we interact with,” said a panellist. “We use the technology, but we apply it in a setting where we feel comfortable with it.”

Crypto-currencies are problematic for banks that profit from cash ~

Another panellist was convinced that the technology underlying crypto-currencies would eventually change the industry, but was not convinced it would be in cash, where he thought instant payments services were a formidable competitor.

“There is a price to Bitcoin but is there a value to it?” he asked. “I also struggle with the term ‘asset’ and Bitcoin. There is supply and demand, that is for sure, but as far as I am concerned that is about it. Something that goes from US$200 to US$20,000 and goes back to US$3,000 and now is at US$8,000 again [is not useable as a payment currency].” That could change, he added, once central bank digital currencies (CBDCs) are available.

The three countries most advanced in the development of CBDCs– Iran, North Korea and Venezuela – are poor advertisements for the idea, thought a panellist. “The reason central banks do not issue digital currency is cost,” she argued. “Right now, the cost of transferring to a DLT for cash is not worth the benefit.”

Another panellist, who had discussed the possibility with his central bank, thought the real obstacle was the unpredictable performance of digital currencies in a financial crisis. A third argued that the commercial banks were opposed, because digital currencies “took a lot of revenue out of the banking community. Do central banks want, as supervisors, to put the stability of the banking system at risk? Probably not, in these times.”

The lack of enthusiasm of commercial banks for crypto-currencies is fundamental. They are electronic cash, and the usefulness of digital cash in transactions is precisely that it excludes third parties such as banks. Bitcoin, for example, is already being used to transfer value between people who do not have bank accounts.

Its advantages include portability and security – after a decade, Bitcoin has yet to be hacked - but also the elimination through scarcity of the possibility of being debauched by the central government or central bank. Much of the recent upward movement in Bitcoin, for example, is attributed to Chinese retail investors anticipating a devaluation of the yuan. But the disadvantages are formidable too: price volatility, lack of scalability and slowness, all of which make it hard to use as a currency or a reliable store of value in normal circumstances.

The price volatility is attractive to speculative traders, however. They value volatility in any asset class. But a panellist argued that the current speculation is no more than a necessary phase in the maturation of crypto-currency as an asset class. He looks forward to a future in which crypto-currencies reduce the cost of transactions across borders to zero, drawing more of the population of the world into international commerce – and considers this far more important objective than incurring the unknown costs and risks of transferring the banking industry on to unproven and untested DLT platforms.

The prospect is not wholly improbable. A class of crypto-currencies known as Stablecoins have emerged precisely to eliminate price volatility, and so make them useable as currency. Banks have understood the potential. Commerzbank, for example, has joined forces with Deutsche Börse to create a Stablecoin backed by an insolvency-remote entity. The coin can, said a panellist, be used to "settle a transaction more or less in a quasi-central bank money-backed environment."

Institutional investment is vital to the growth of crypto-assets ~

Ultimately, what will drive the development of the crypto-asset markets is institutional investment in them as an asset class. "To out-perform their peers," is why one panellist thought they would eventually invest. "They want the alpha."

She added that the returns would stem not just from a successful bet on new technology, but by providing a hedge against the under-performance of fiat currencies as well as stock and bond markets, and a superior store of value to gold. In reality, only Bitcoin is currently liquid enough to absorb institutional money. "They like the asymmetric risk," said a panellist. "The chance of Bitcoin going to zero, and the impact that would have on your portfolio, are dwarfed by the possibility than Bitcoin may go to US$50,000."

Inevitably, many institutions are deterred from investing in Bitcoin by an obvious question ("What backs it?") and by concerns about its uncertain legal and regulatory status and continuing use in criminal activities.

A second panellist thought end-investors forgave their asset managers for missing out on the Bitcoin bull run of 2017-18 but would not forgive them if they missed out a second time. "Back in the early 2000s, pension funds and endowments would not invest in hedge funds," he said. "We have come a long way. The fact we are on this stage, and you are all in this room, shows where the discussion about digital assets is going."

A third panellist agreed, arguing that many asset managers sceptical about crypto as an asset class were now being forced to explore it by their clients. But this was not true of all firms. "We have had no client request actually to buy the asset class," countered a panellist. "They are happy to do proofs-of-concept with us, including some of the largest insurance companies, but none of them came to us and said, `By the way, I want to buy Bitcoin. Can you custody this?'"

Another panellist thought this under-estimated institutional involvement in the market. He said that 60 per cent of Coinbase custody clients are "crypto-forward or crypto-native investors," by which he meant crypto-only hedge funds and large venture capital funds investing in crypto.

The balance is divided evenly, he said, between issuers of the crypto-assets themselves and the miners taking payments in crypto-currency (20 per cent) and "traditional institutions" (20 per cent). "You would be surprised at some of the banks, insurance funds, pension funds [which hold assets in custody at Coinbase]," he said.

One panellist said clients were asking him: "How should we invest in the ultimate fiat currency - Bitcoin? It is the ultimate fiat currency. It is created out of thin air, and it is driven purely by demand. Supply is limited, so it is a demand thing, but it is does not prevent anyone from assigning a zero price to it. They tell me that in US dollars and euros and Czech koruna and Hungarian forints, there is at least the economy behind it, supporting the currency. Why should I, as a long-only investor, invest in something that is totally intangible? At least you can create jewellery out of gold."

However, Vontobel has since 2016 successfully issued and custodied institutional grade Bitcoin tracker certificates, which trade on the Swiss Exchange. These provide an institutionally convenient alternative to trading and custodying Bitcoin on

crypto-exchanges. The bank started with Bitcoin because it was liquid and simple to store the certificates (the bank decided to store them in-house rather than rely on a third party) but it has since expanded into other crypto-currencies. Similar products, like the XBT Bitcoin trackers, have emerged.

Custody of crypto-assets presents unique challenges ~

A panellist thought parallels with securitisations and derivatives (such as options and ETFs) were misplaced, because crypto-currencies represent an "entirely new system of functioning," without issuers and bank accounts.

"Custody is so easy in the real world, and so complicated in this world," she said. "There is no one to call if anything goes wrong," she said. "You are responsible for holding the passwords to the wallets where the Bitcoin is stored. If you lose it, you have lost your Bitcoin, there is no recourse. This is something that funds, understandably, cannot accept."

Leaving the private keys in a wallet on the exchange where the crypto-currency was bought means they are vulnerable to being hacked. Locking the hard drive containing the passwords in a safe deposit box is used by some funds but remains physically vulnerable.

"At the institutional level, investors need all sorts of guarantees, not just at the operational level, but legally," said a panellist. "You have to have reliable, third party, qualified custodians for certain types of assets. You cannot go to your clients and say, `Oops!"

This is why firms such as Coinbase (founded in 2018) have emerged. They add extra layers of security, including separation of parts of the code in bunkers around the world. Coinbase, for example, has set up a New York Trust company, which is regulated, insured, capitalised and certified on the same basis as the Depository Trust and Clearing Corporation (DTCC). It is also separated from the Coinbase exchange. By June 2019, Coinbase held in custody US$1.2 billion in digital assets.

"Coinbase offers a great service, and others are emerging that are as regulated as you can possibly be, but I have personally spoken to many big institutional investors who tell me that they are waiting for State Street, BNY Mellon, Goldman Sachs, the big balance sheets – they want the big balance sheets not just behind the crypto-assets but also the security tokens, if indeed this is the evolution of capital markets that we are witnessing."

Fidelity is offering an institutional-grade custody service already through its Digital Assets arm. "What we will see when the bigger players enter the room is a partnership," predicted a panellist. "Fidelity or State Street or J.P. Morgan are not going to recreate what Coinbase or Gemini has spent the last seven-plus years developing or building. There is an opportunity to act in a sub-custodian function or form a partnership that combines the balance sheet [of the banks] with [crypto-asset custody] technology."

A custodian argued that asset safety issues were less of a problem in permissioned DLT networks. "There we have a lot of the safeguards back again which we had in the old world," he said. "There is a central authority. You have a regulatory view, so the regulator can at any moment in time see everything happening in the network."

In his view, permissioned networks transform the technical problem of crypto-custody into a question of access to the network. "Our problem is who runs the ledger, and who joins," he said. For settlement purposes, he predicted that the major banks would create Stablecoins that permit settlement on permissioned networks until such time as CBDCs become available. The Utility Settlement Coin (USC) is an example of this.

Crypto- is capable of creating multiple new asset classes

"This highlights where securities are going – where custody is going," said another panellist. "We have crypto-assets but also security tokens, or tokenised securities. That is where capital markets are going." But the chief promise of tokenisation is not as an alternative to existing securities; it is the "securitisation" of assets that are current illiquid. Unlike crypto-currencies, these are generally backed by real assets.

Numerous crypto-assets are in issue already. They include utility tokens, in which investors buy a promise that an application will be developed and used, and the value of the token will rise as usage increases. A recent example is Civic, a token sold to develop secure access to on-line identity verification. But the extension of the concept is almost limitless.

Examples of potential crypto-asset issuance offered by one panellist include trade invoices, insurance contracts (which, by paying out on the occurrence of an event, are comparable to out options), programmable shares (such as car manufacturer equities that also open the door of your car) and digital works of art (such as characters in a computer game).

However, as a panellist noted, the crypto-asset markets are still nascent. "It is not so much a race to figure this out as a race to the starting line," said a panellist. "It is that new. We are trying to figure out where the starting line even is on how we can reform, improve and open up capital markets using this new technology."

More than one panellist thought the key change in unlocking institutional interest in crypto-assets would be standards. "We do need standards, in APIs, but also in Blockchain and other new technologies," argued a panellist. "Without standards, we are going to relive the world I know very well, from when we introduced electronic banking. People had the choice of having 27 PCs around them, or just saying, `I do not want your product.'"

But panellists believed, counter-intuitively, that regulation of crypto-currencies and crypto-assets would help the most. "Every morning I wake up hoping to read about regulation," said one. "Because it changes the narrative from illicit activities going on, or bad actors in the space. I would welcome that regulatory framework." He thought it would not happen quickly but, until a global regulatory framework is in place, institutional money would "stay on the sidelines."

The heaviest users of crypto-currencies remain criminals ~

But there is another reason institutional money will stay on the sidelines. This is that bad actors are still heavily involved in the crypto-currency markets. In fact, ransomware attackers invariably insist on payment in crypto-currency through DLT service providers. "Although the technology is fascinating, and shows great potential, the elephant in the room is that, to date, the largest users of Bitcoin and other crypto-currencies are the criminal fraternity," said a panellist.

He thought this should give regulated institutions pause. "Though the technology itself is neither good nor bad, if the majority of the digital assets are owned by criminals or have been acquired through criminal practice, it raises all kinds of questions for institutions around how you satisfy your Know Your Client (KYC) and anti-money laundering (AML) requirements," he said. "The very things that make it attractive - you do not need a bank and speed of transaction – are the things that make it attractive to criminals. They cause an absolute nightmare for central banks, who are responsible for the money laundering legislation and enactment."

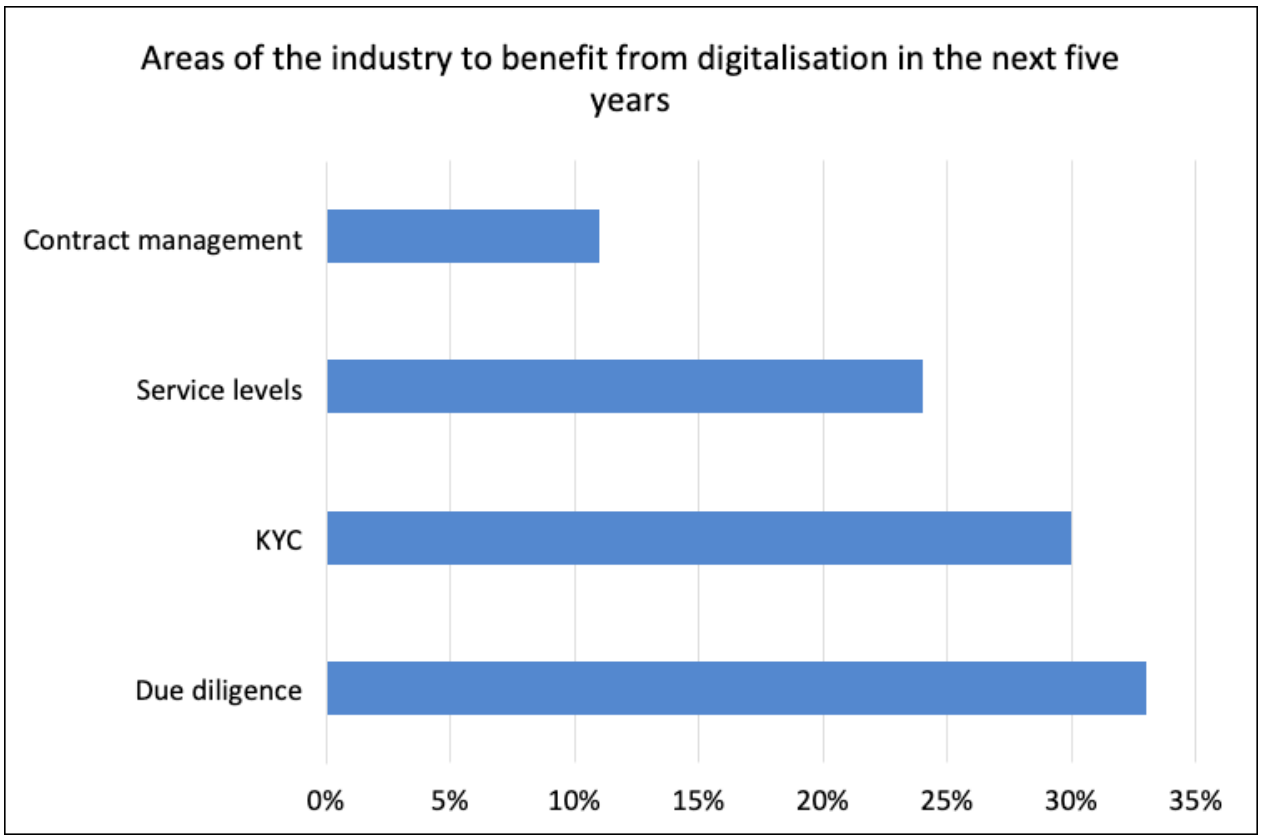

Chart 24.

This explains why central banks are at the forefront of efforts to persuade the banks and CSDs to tighten their cyber-security measures and discipline. They seem to be succeeding. A poll of the audience found that KYC and due diligence on counterparties, which now includes queries about cyber-security, were the two most popular areas for technological investment (see Chart 24).

The investment is necessary, since the number and variety of assaults by criminal cyber-attackers is unlikely to fall. The effort-reward ratio for criminals is so large that attackers will always be tempted. The largest single successful cyber-attack so far netted US$181 million in a 30-minute spell over a single weekend.

"One of the most prolific ransomware groups out there in June issued a press release announcing their retirement," added the panellist. "After 14 months in operation, the unknown number of members of this ransomware group announced that they had made over $150 million each through ransomware. Their press release went on to say, 'If you are using our ransomware in attacks, please note that, with effect from this week, we will no longer be supporting the malware. If you have been hit by a ransomware attack using our malware, please pay quickly, because the keys will not be available with effect from seven days from now.'"

Most successful cyber-attacks do not need to be sophisticated ~

The principal vulnerability is not technological but human. "We are lazy, and so are cyber-criminals," explained a panellist. "They can gain an awful lot, very easily, with cyber-attacks. You do not need to create anything special. You just spray out a phishing email, rely on the 1-2 per cent that will click on it, and you are in."[1] Successful cyber-attacks, such as WannaCry and Petya, made use of a vulnerability attributable to human laziness: unpatched openings in Microsoft software for which a patch was issued four months earlier.

1. A keynote speaker argued that the same ratio is at work at the geopolitical level. He predicted that cyber-warfare "will happen" because it is so much cheaper than conventional methods, such as firing missiles. Although cyber-attackers have not yet assaulted crucial infrastructures such as water or electricity, he thought that, if they did, the counter-attack would in all likelihood evolve into "kinetic" warfare.

Of the 1,063 cyber-breaches investigated by Kroll in 2018, most took the form of phishing attacks, in which cyber-attackers monitor in-boxes for perhaps six months to better mimic how colleagues within a business communicate with each other. Their principal goal is to identify a large invoice and change the payment details.

"95 per cent of Microsoft Office 365 breaches can be defeated by turning on two factor authentication," said a panellist. Microsoft offers this for free, as standard, but it is not turned on by default – even though phishing attacks are costing businesses an estimated $2½ billion a year in thefts and another $1¼ billion a year in investigation and repair costs, to say nothing of the goodwill with customers and suppliers that is forfeit and the impact on the share price.

In the United Kingdom, the share price of TalkTalk fell 48 per cent in the two weeks after a cyber-breach was disclosed - and it recovered most sharply when the leadership changed. "The share price was no longer about the company," explained a panellist. "It was the market's opinion of the leadership in place in that company. The market had lost confidence [in how the breach was managed]."

Institutions are better prepared for natural disasters than cyber-attacks ~

The ability of cyber-attackers to cause such dire consequences reflects the weakness of the defences of some institutions against cyber-attack. This is reassuring, in the sense that cyber-criminals will always seek easier targets. "If they spot monitoring or demilitarised zones (DMZs) on your network, they are going to move on," explained a panellist.

Although every business has a well-rehearsed business continuity plan in case of a fire, natural disaster or a terrorist attack, rather fewer have an equivalent instant response plans for a cyber-attack. Yet the statistics suggest cyber-breaches are likely to occur every year while natural disasters strike but once a decade. In the United Kingdom, a government survey found 95 per cent of companies had experienced a cyber-incident in the previous 12 months.

Unfortunately, the securities services industry has a poor record in crisis management generally. Although it regularly encounters operational, political and economic crises – Denmark, Egypt, Turkey and Zimbabwe were mentioned, but the keynote speaker drew attention to looming crises in India, Israel, Mexico, South Africa and Sudan – in addition to data breaches, the industry lacks rapid and effective response plans even to these.

"Crisis management is not handled particularly well by global custodians, sub-custodians, CSDs or regulators," argued a panellist. "What goes missing is leadership and collaboration and client communications." This can be reassuring: if nobody has effective crisis management plans, and every business is bound to be attacked, there is no stigma attached to being cyber-attacked.

However, the industry as not as cynical as this suggests. A poll of the audience found that the appetite for collaboration on cyber-security was strong (see Chart 25), though it still fell behind more immediately pressing issues such regulatory compliance and investment in new technology. Certainly, industry awareness of cyber-security threats is not as healthy as regulators would like.

Ultimately, every institution can expect to be attacked successfully. What counts is the effectiveness of the response. "It is not the breach that kills you," warned a panellist. "It is how you respond. How you respond, and how you are perceived to respond, will ultimately decide the survivability of the company." That response depends in turn, on having an effective response plan in place.

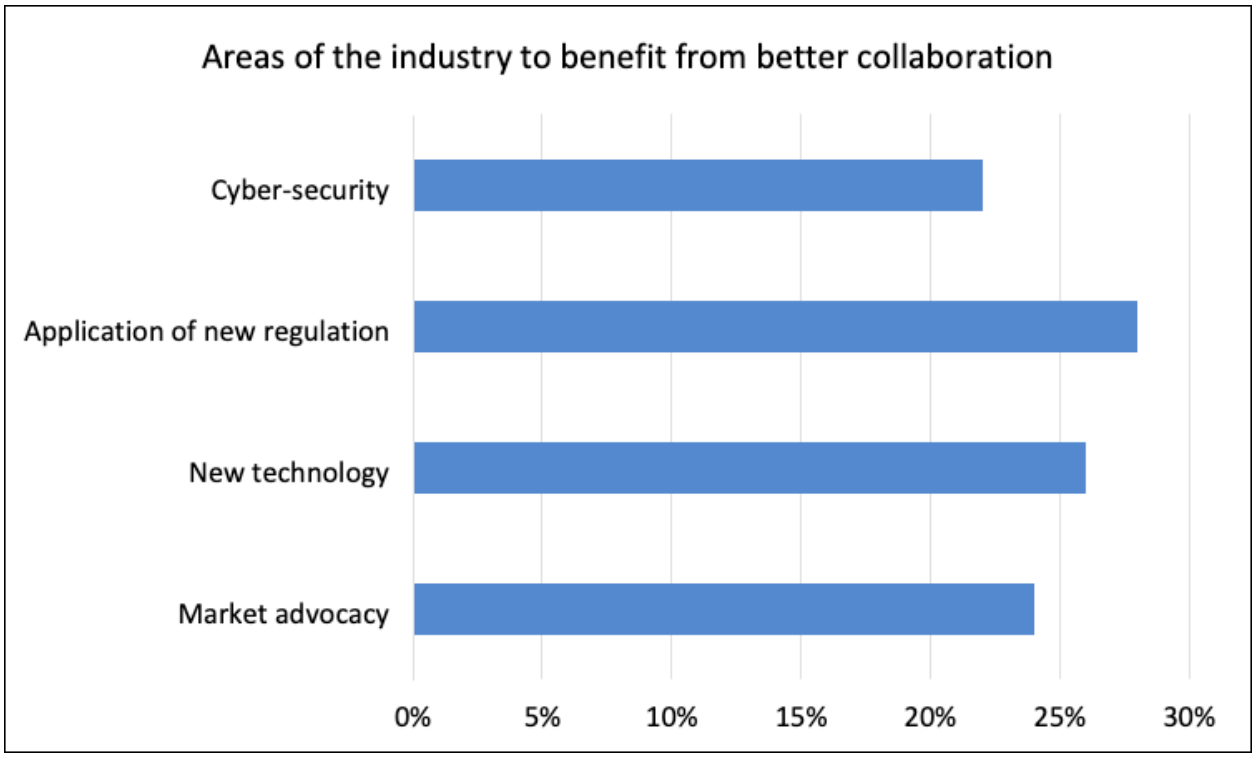

Chart 25.

An effective cyber-response plan demands leadership and communication. It must specify immediate responsibilities and roles, escalation routes, sources of essential external advice, communications to staff and customers, monitoring of and contributions to social media, and commissioning of a forensic investigation into what caused the data breach and what was lost. The faster the response time, the easier it is to mitigate the impact of a breach.

A crucial aspect of a successful plan is co-ordination of notifications to regulators. In the case of a global organisation, these must be sent to financial and data regulators in multiple jurisdictions. Regulatory requirements can vary - the General Data Protection Regulation (GDPR) in Europe sets a deadline of 72 hours, but the equivalent in Singapore is just two hours – but a larger risk is being arbitraged by regulators, which share information about cyber-breaches.

A panellist cited a company which informed their financial regulator several days in advance of their data regulator, unaware that the news would be shared with the data regulator. Their reward was a barrage of awkward questions from the data regulator when they did finally submit a notification. “Investigations getting derailed by the regulators just adds time and cost to the recovery, and makes it a far more uncomfortable experience,” said a panellist.

He advised firms to rehearse their response plans regularly. “You want to build up muscle memory in the incident response teams,” he said. “When an incident happens, you want the staff involved to just know what they need to be doing. They do not want to be reading a set of instructions from the manual.” An early priority for them is to establish which systems – not which servers – are compromised by the incident, since the commercial and regulatory consequences vary.

For example, regulators in some jurisdictions are disconnecting breached institutions from trading, clearing and settlement infrastructures - forcing firms to maintain business by physical means only until the breach is closed. A panellist was aware of a brokerage firm that was off-line for 13 weeks before the regulators allowed them to reconnect to the trading networks. As one panellist noted, reverting to paper for a week might be long enough to put some custodians and CSDs out of business.