International Securities Services Association

SYMPOSIUM 19

23 – 25 May 2018

AN ACCOUNT OF PROCEEDINGS

By Dominic Hobson

June 2018

CONTENTS

Keynote Address

The keynote speaker is a self-confessed "internationalist" dismayed by mounting global instability. The post-war consensus has broken down. There are trade tensions between the United States and China. The United States has imposed, unilaterally, a "tax on multi-lateralism." The United Kingdom has voted to withdraw from the European Union. Italy is governed by a coalition of extremists. In France, president Macron has dispatched the two major governing parties. Angela Merkel, the chancellor of Germany, is weakened.

These maladies are, he thought, a consequence of the great financial crisis, and especially of its impact on economic growth and the distribution of wealth. The crisis cost around 25 per cent of the Gross Domestic Product (GDP) of the European Union and pushed public debt towards 100 per cent of the collective GDP. Despite the recovery of growth, rates of youth unemployment in Europe remain shockingly high. The financial services industry, widely seen as responsible for the crisis, has paid for its greed, opacity and bail-outs in hefty fines and burdensome regulation.

"It must not happen again," warned the keynote speaker. He cited Paul Tucker, the former deputy governor of the Bank of England, who told governments in 2012 that they risk an "uncontainable" explosion of public anger if they have ever to be bailed out by taxpayers again. It follows that the banking industry must work hard to rebuild trust with both regulators and the public, by adhering to the highest standards of integrity, and forging deeper, more responsible and more ethical relationships, especially with small and medium-sized firms.

One way in which the banks can contribute to that recovery of trustworthiness is to work with regulators to achieve a better understanding of how the global financial system works. The quality of the data available to central banks and securities markets regulators is woeful. It is not real-time, or harmonised.

Even the creation of trade repositories to collect standardised information on OTC derivatives trades have failed in their primary purpose of improving regulatory understanding of positions and exposures. This is particularly true of Europe, where the regulators imposed competition between trade repositories without making proper provision for inter-operability. "Regulators cannot do anything with the data because it is not linked up," said the keynote speaker. "They cannot see from that data where the risks are building up."

This shortcoming, he thought, needs to be addressed. In 2014, Andy Haldane, chief economist and executive director, monetary analysis and statistics, at the Bank of England, spoke of a Star Trek-style console through which regulators could monitor global flows of capital in real-time.[1] It is possible for this to be

[1] "I have a dream. It is futuristic, but realistic. It involves a Star Trek chair and a bank of monitors. It would involve tracking the global flow of funds in close to real time (from a Star Trek chair using a bank of monitors), in much the same way as happens with global weather systems and global internet traffic. Its centre piece would be a global map of financial flows, charting spill-overs and correlations. Such a global financial surveillance system could serve a number of policy ends. It would allow policymakers to monitor the evolution of the financial system in real time, as it expanded, contracted and changed shape. It would also allow them to simulate and stress-test this system to help detect impending financial cliff-edges." See Andy Haldane, "Managing global finance as a system," Maxwell Fry Annual Global Finance Lecture, Birmingham University, 29 October 2014.

built, giving the industry as well as the regulators a real-time view of stocks and flows and volumes and volatility, allowing them to head off potential financial disasters before they occurred. Its value is indubitable. Only wars can rival the destructive power of financial crises, yet policymakers currently have exceptionally poor forward-looking data. "It is like trying to run a power station or a public transport system without a map of the pipework or a signalling system," said the keynote speaker. "We do not know enough."

The answer, he argued, is to build an inter-operable, real-time database. Constructing it requires co-operation between the industry and the regulators. The keynote speaker urged the industry to take the lead, by producing a detailed blueprint laying out the deliverables and setting a time-frame, citing the way that investment banks had led the development of contingent convertible securities ("CoCos") and "bailing-in" as an example of how banks can lead as well as respond to public policy. He thought distributed ledger technology (DLT) a potentially useful tool in building the database, and that the data should be made available to all at the aggregated level.

"I am lobbing the ball firmly in your direction – you should do it," he said. "The prize is huge. It just takes leadership and determination. This is a unique opportunity to have a real-time data system that will greatly reduce the risks of financial instability. You cannot put a price on that. We should not continue to accept this huge risk, uncertainty and lack of effort to improve our knowledge. After the next crisis, the public will ask, `Why didn't you foresee that? You've cost us enough.' We need to be ambitious and move forward boldly."

He did not under-estimate the level of international co-operation required to deliver such a tool. Neither the Bank for International Settlements (BIS) nor the Financial Stability Board (FSB) has the power to compel countries to take part. No country will accept international arbitration. Without incentives for all countries to take part, the project might easily degenerate into one dominated by large countries, which set standards others refuse to comply with. The trick to encouraging co-operation, he said, is to establish the area of common interest, and then set ambitious goals to fulfil it. Multiple initiatives, he warned, lead to divergence, not commonality.

Another area which would benefit from closer international collaboration is cyber-security, especially through the sharing of information on cyber-threats and cyber-attacks. The range of potential attackers – criminals, hacktivists and sovereign states – and the variety of their motivations makes it hard for any one entity to keep on top of cyber-threats. Unfortunately, an initiative by the International Organisation of Securities Commissions (IOSCO) to encourage the sharing of cyber-security information was vetoed by the United States. In the absence of information-sharing, the best antidote to cyber-attack is to ensure that all customers and suppliers adhere to best practices.

The Brexit negotiations between the United Kingdom and the European Union (EU) provide another example of regression in international co-operation. The politicised nature of the process means there is "no chance" of mutual recognition, so the least worst outcome is free trade in financial services with "equivalence" determined by the European Securities and Markets Authority (ESMA) in tandem with the European Commission, Council and Parliament. "The whole process is out-of-date, given the growth of the Indian and Chinese

financial markets," said the keynote speaker. "Equivalence determination does not make the slightest bit of sense. What we want is global standards everybody adheres to, and which are enforceable."

If the ten largest capital markets in the world implemented, enforced and supervised a single set of global standards in the same way, financial business would flow seamlessly. But ten countries with ten standards creates a ten-by-ten matrix of "equivalence" determinations. "The whole `equivalence' technique is unsatisfactory," argued the keynote speaker. "It says that if `you' want to sell into `our' market, your standards cannot be lower than mine because you will have a competitive advantage. It is better to have a global set of standards with enforcement at the global level. The United States will not accept it, but other countries might. And unless we have it, we will end up with messy bi-lateralism. Though the way the EU handles Brexit negotiations is a little bit insular, it is a multi-lateral institution, and it supports the WTO, so it could be persuaded."

One consequence of the "insular" Brexit negotiation is the battle to control the clearing of euro-denominated financial instruments. Strong forces, led by France and Germany, want clearing of euro-denominated contracts to take place within the euro-zone, on grounds that this is the only way to safeguard financial stability. Since the European Central Bank (ECB) would inevitably be drawn into bailing out a failed central counterparty clearing house (CCP), none clearing euro-denominated instruments could remain outside the euro-zone. The European Parliament supports this line of argument and wants to give more powers to ESMA and the European Commission to force CCPs to re-locate. "Nobody knows where this will end up," concluded the keynote speaker.

Yet common to all of the issues discussed at the ISSA symposium in 2018 – cyber-security, DLT and artificial intelligence (AI) and robotics - is an obvious need for more international cooperation, not less. To mitigate the risks of the new technologies, and realise their benefits, common standards are required, include a common understanding of legal certainty. "The more we trade with each other, the safer a place the world is," said the keynote speaker. "So work with regulators, help them technically, and put forward bold ideas to solve problems. Co-operate with and influence regulators. That is our best chance of a Pareto-optimal system and more `financial hedonism' in the future."

He dismissed the notion that regulators do not wish to co-operate with banks. No regulator, however sophisticated, can ever know everything about a market. Regulators need outsiders to tell them the truth. They are adept at distinguishing between those who seek the common good, and those who are seeking an advantage for their firm. Personalities matter too, and personalities change in the regulatory world, just as they do in the political world. "So bring blueprints to solve problems," said the keynote speaker. "Regulators respect that."

Cyber-Security Risks in the Securities Value Chain

How vulnerable is the securities services industry?

Cyber-crime is now more lucrative than the global narcotics trade. In the Global Risks Landscape survey conducted by the World Economic Forum, cyber-attacks have risen from one of the top five risks most likely to occur in 2014 to a top three risk this year. The AV-TEST Institute registers over 250,000 new malicious software programmes ("malware") every day. The global average cost of data (per incident) being compromised is $3.62 million, according to the 2017 Ponemon Institute Cost of Data Breach Study. In the United States, this figure rises to $7.35 million.[2]

In the payments industry, cyber-frauds perpetrated against customers are already exacting a heavy and continuous toll on banks. Last year, one global payments bank dealt with billions of cyber-security events, which equates on average to an incident occurring every ten seconds. "A good day is one when nothing drastic is happening," a chief information security officer (CISO) told the Symposium.

Although the securities services industry has so far escaped unceasing cyber-assaults of this kind, it would be complacent to assume this will continue. "For me, there is nothing that distinguishes a securities house from a payments house," said a cyber-security expert familiar with both. Yet the high level of awareness of cyber-risks in the payments industry is much less evident in securities services, although attacks have almost certainly started already. "We talk a lot about payments, but we see increasing attacks on the securities industry," warned a cyber-security expert.

Because participants in the securities markets transact in and safekeep assets of much higher value than cash payments, and move cash and securities in bulk between limited numbers of counterparties, they are naturally tempting targets for cyber-attackers. Settlements, corporate actions, dividends, redemptions, securities loans and collateral calls all put assets at risk of being stolen, through fraudulent transactions, manipulation of settlement instructions, or falsification of records or reports. Sensitive client and contractual information is also at risk of being stolen.

In addition, the complexity of the securities industry means it has more points of vulnerability than the payments industry. In the securities markets, transactional information passes continuously between trading venues, investors, asset managers, broker-dealers, clearing brokers, custodian banks, clearing brokers, clearing houses, settlement infrastructures, trade repositories (TRs) and data vendors. This creates multiple entry points for cyber-attackers, not least because of the information dependencies which build up.

There are many examples of these dependencies. Asset prices, for example, are generated by automated, high frequency trading algorithms that are vulnerable to manipulation. Yet they drive fund accounting valuations. Likewise, crucial reference data such as standing settlement instructions (SSIs) and bank identifier codes (BICs), is sourced from a limited number of data vendors.

[2] Ponemon Institute, 2017 Cost of Data Breach Study: Global Overview, Ponemon Institute LLC, June 20-17, pages 1 and 5.

Transactions are processed by combinations of automated and manual processes, and operational staff are under constant pressure to meet settlement deadlines and cut-off dates – making checks harder to run. The exchanges of cash and assets which take place are not only of high value but highly predictable. Dates and amounts, in cases such as dividend and interest payments and redemptions, are even published.

Worse, it is still commonplace in the securities services industry to deliver securities free of payment, without matching the counterparties or the terms of the trade, and with no exchange of monies. Such transactions are manifestly open to fraudulent delivery instructions. If those instructions specify delivery to an omnibus account, detection is further complicated. Omnibus accounts inevitably obscure ultimate beneficial owners, making it hard to spot fraudulent positions.

In securities services, there is also a heavy reliance on centralised functions - matching services (such as Omgeo), payments messaging networks (such as SWIFT), central counterparty clearing houses (CCPs), central securities depositories (CSDs) and TRs – to intermediate flows, safekeep assets and hold data. This increases the risk of a disabling distributed denial of service (DDos) or ransomware attack. Many participants also outsource functions, further concentrating transactional activity and asset holding, including in lower-cost, offshore locations where cyber-security standards may be lower.

Modern customers demand the same level of service from the securities services industry as they get from Amazon, Apple, Facebook, Google and Netflix, creating fresh vulnerabilities through the provision of mobile applications, and customer access to data. Disruptive innovators such as FinTechs, which make use of new technologies and techniques such as AI, machine learning and smart contracts to gain a foothold in the market, not only create new hazards for themselves. They are also forcing established players to assume the same risks, by mimicking their services in order to remain competitive with new entrants.

What are the key risks?

Cyber-risks in the securities services industry fall into four main groups, whose plausibility varies from the difficult to the easy, and whose potential impact ranges from the systemic to the local. The most serious systemic risk is the disablement of a major market utility such as a CSD, CCP or TR, closely followed by disruption of a major global custodian or a messaging (SWIFT) or matching (Omgeo) utility. The effects of any of these entities being disabled are hard to contain.

The second most serious group of cyber-risks is the manipulation of data. Pricing feeds and stock market news can be falsified and distorted relatively easily, with sizeable impact on the wider industry. Databases containing reference data or information about collateral posted, corporate action entitlements, stock transfers, proxy voting records, and lists of sanctioned individuals, companies and states, are open to manipulation. The general ledgers and asset master databases of custodian banks are also vulnerable, and potentially expensive to the institutions affected, but such attacks are difficult to execute and limited in their wider effects.

The third most serious cyber-risk is the outright theft of assets. The most obvious instance of this is bogus settlement instructions or reconciliations, especially when securities are delivered free of payment. But assets can also be stolen by fraudulent stock borrowing and lending, alteration of records of collateral posted, falsification of statements of holdings or portfolio reports to clients, and re-direction of account transfers or dividend or interest income or redemption proceeds. None of these is easy to accomplish but nor is any especially difficult, and the potential cost is high.

The fourth – and, for the most part, least impactful - set of cyber-threats is the theft of information. The loss of competitive information about, say, pricing and service level agreements, is not trivial and relatively easy for an attacker to do, but its impact is limited. The loss of sensitive customer information, such as details of holdings and positions, contractual terms, and contact details, is more serious. Nor is it difficult for an attacker to attempt.

What forms do attacks take?

Attack vectors include the familiar viruses, worms and trojans (all of which are propagated via shared files and email attachments) and DDoS attacks (which disable on-line systems by flooding bandwidth with a high volume of traffic). The hardest to combat are the so-called Advanced Persistent Threats (APTs). These are carefully aimed and highly sophisticated threats that lurk undetected inside the target system for months or even years, researching the flows of money and data, before being activated.

To inject malware of these kinds into an organisation, the attackers rely mainly on unwitting employees opening malicious email attachments or USB sticks, emailing documents to less secure personal email accounts, or disclosing keys to a system such as user IDs and passwords, which allow them to log in, impersonate operators and initiate (and erase traces of) fraudulent payments.

ISSA Cyber-Security Working Group

To help raise awareness of cyber-risks in the securities services industry, ISSA launched in January 2018 a Working Group on Customer Cyber (Fraud) Risks in Securities Services. At a two-day workshop held at the BNY Mellon offices at Canary Wharf on 22 and 23 January, attended by Citi, Clearstream, Deutsche Bank, the Depository Trust and Clearing Corporation (DTCC), SIX, Standard Chartered Bank and SWIFT, as well as the ISSA CEO Office, the content of a preliminary paper for the Symposium was drawn up. The next objective is to create a report that sets out what cyber-risks the securities services industry faces, with a first draft due by the end of July 2018 and a full report by year-end. The brief given to the membership of the Working Group, which includes chief information security officers (CISOs) as well as central securities depository (CSD) officials and custodian bankers, is to help the securities services industry identify and mitigate cyber-security risks. By involving CISOs as well as securities services industry insiders, the Working Group aims to assess whether cyber-risk management techniques used in other fields can be applied successfully to securities services – or whether the industry has unique risk characteristics.

"It is not computers infecting computers," explained a CISO. "It is people, reasoning people." Sometimes, the reasoning person is a malicious employee who has been bribed or is nursing a grudge. Personalised emails or text messages, known as "spear phishing," look increasingly authentic because they draw on personal information published on social media or derived from mobile telephones, which rarely carry anti-virus applications.

An email invitation to "validate your salary and bonus" has proved especially effective in encouraging employees to open attachments. Banks have taken to employing so-called "ethical hackers" to "phish" their own employees as part of their efforts to educate their staff about the nature of the threats, and to identify persistent offenders, who are then invited to a formal tutorial. "We use the stuff we blocked the week before to stay as current as we can," a CISO told the symposium.

But attacks are not always aimed at specific individuals or systems. Phishing emails, such as WannaCry, are mass "ransomware" attacks that aim to profit from charging the owners of thousands of infected computers for decrypting their data. So-called "watering hole" attacks look to infect visitors to particular web sites with malware. This happened to visitors to the web sites of the National Banking and Stock Commission of Mexico, and the Financial Supervision Authority of Poland.

Who launches cyber-attacks?

The sources of cyber-attacks fall into three broad groups. The first are nation-states. The second is organised crime, and the third are hacktivist groups. Criminals are interested almost entirely in the theft of cash, financial assets or valuable intellectual property, which tends to limit their impact to financial loss. Hacktivists have an exclusively political agenda, which they pursue by publicity-seeking disruption of organisations they oppose.

For criminals and hacktivist groups, the barriers to entry to staging a malware or ransomware attack are low, because the tools needed to commit a cyber-crime are now available as a service. In 2016 the so-called Shadow Brokers hacking group auctioned a series of hacking tools they had stolen from the National Security Agency (NSA). Initially, the group received no bids, since buyers were concerned the auction was an NSA "sting" operation. The tools it released to convince buyers the sale was genuine were behind the WannaCry and Petya and NotPetya attacks last year.

"You can find on the dark web people who will do anything for you," explained a CISO. "Crime as a service is now out there, in this space. The individuals involved never meet each other but have a lot of trust, in expectation of future pay-offs." Some ransomware attackers even provide contact centres to help people unlock their encrypted data.

They also keep up to date. As one opening closes, another is opened, creating an arms race between cyber-defenders and cyber-attackers. 75 countries around the world now have military-style cyber-commands for offensive as well as defensive action, and they always include critical financial market infrastructures in their lists of likely targets. One CISO told the symposium his bank employed more than 50 intelligence analysts to monitor the data and track the behaviour

of around 100 different potential adversaries: nation-states, hacktivists, criminals and disaffected insiders.

This constant vigilance matters, because the most impactful attackers are patient, spending as many as 200 days inside a system to understand how to get fraudulent but fool-proof credentials. They work at weekends and bank holidays too, knowing staffing levels are low. They also co-ordinate their efforts with other groups so they can, say, execute both the initiation of a payment and its confirmation by apparently different counterparties.

But it is nation-states that are the most prodigious actors in cyber-crime. In 2013, Iran attacked several American banks. In 2014, North Korea attacked Sony. In 2015, China breached the database of health insurance company Anthem. In 2016, North Korea stole money from the Bank of Bangladesh. In 2017, Russia attacked FedEx and Merck. The motivations behind these cyber-attacks included money – both Iran and North Korea are sanctioned states short of hard currency – but nation-states are also interested in industrial espionage and the pursuit of political or geopolitical advantage.

Cyber-attacks have become existential to North Korea, which uses them to acquire foreign currency. The North Korean state employs between 6,000 and 7,000 "cyber-warriors" whose only job, since China imposed sanctions as well, is to steal hard currency. They also use ransomware attacks and crypto-currency mining to acquire foreign exchange. Teams are formally assigned to monitor major banks such as BAML, Barclays and Citi, looking for opportunities to steal money.

How can you defend your organisation against attacks?

Naturally, the private sector looks to governments to help defend themselves against attacks by nation-states, which enjoy unlimited funding and immunity from normal police action, let alone prosecution. It is also unlawful for private entities to launch pre-emptive or retaliatory "counter-malware" attacks, or counter-attacks to destroy stolen information or intellectual property. While governments remain free to do so, none has yet publicly announced a cyber-deterrent effective enough, in terms of the repercussions, to deter nation-states from launching cyber-attacks.

In the United States, for example, the Department of Defense was supposed to announce a cyber-deterrence strategy in August last year, but the announcement was postponed. "A cyber-deterrent means a red line to say, if a country crosses that line, we will take an action," a CISO told the symposium. "We usually know who the adversary is – but they are in a part of the world where we cannot get at them. At what point do we do something kinetic? Throw a missile at it? We cannot live without this technology. We have seen hospitals shut, and emergency services cut off. People are going to lose their lives. Governments have to think through the escalation process."

Where governments are helping the private sector is through the publication of best practices, such as the guidance on cyber-security resilience for financial market infrastructures published by The Committee on Payments and Market

Infrastructures (CPMI) and the Board of IOSCO.[3] In September last year, the European Commission adopted an updated cyber-security strategy. In April this year, the 53 member-states of the Commonwealth also agreed to tighten their collective cyber-security.

However, concern was expressed at the symposium about the risk of proliferation of official cyber-security measures. Last year the Financial Stability Board published a list of 56 cyber-security regulations and other measures agreed and disseminated by its 25 member-states.[4] In addition to the recommendations of CPMI-IOSCO, the G7,[5] the Federal Financial Institutions Examination Council (FFIEC)[6] and the International Standards Organisation (ISO)[7] have also published cyber-security standards and frameworks.

The symposium heard that the most suitable framework for private sector organisations to follow is the *Framework for Improving Critical Infrastructure Cybersecurity* published by the National Institute of Standards and Technology (NIST). This covers identification, protection, detection, response and recovery measures, and using it is more practical than trying to comply with multiple national regulations. The seven-step cyber "kill chain" framework developed by Lockheed Martin, for identifying and preventing cyber-attacks, was also thought to provide a useful set of best practices.

The SWIFT customer security programme (CSP) provides a live example of private sector collaboration. The CSP was launched after the partially successful cyber-attack on the central bank of Bangladesh in February 2016. The CSP aims to enhance security via a set of 16 mandatory controls (such as two factor authorisation) to be implemented by all members of its messaging network by the end of this year, on penalty of being reported to regulators for non-compliance.

By the end of 2017, 89 per cent of SWIFT customers, representing 99 per cent of SWIFT message traffic volumes, had self-attested compliance. SWIFT expects the proportion to rise to 100 per cent by the end of this year. SWIFT itself contributes to cyber-security by sifting transactions for signs of fraud and halting them. It also stores copies of all transactions and has rectified a vulnerability identified in the Bangladesh Bank attack – the deletion of the instructions to transfer the money - by maintaining "golden copies" at a separate site.

The symposium was told that more attacks could be stopped through co-operation of this kind, and especially by intelligence-sharing, which would increase resilience by raising the overall standard of cyber-security. "Cyber-criminals work as teams, and so should we," said a delegate. It also makes good commercial sense, since the alternative is to do less business with each other or do it at a higher cost by lowering the standard of contributory negligence.

[3] Committee on Payments and Market Infrastructures (CPMI)and the Board of the International Organization of Securities Commissions (IOSCO), *Guidance on cyber resilience for financial market infrastructures,* June 2016.
[4] Financial Stability Board, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, 2017.
[5] G7, Fundamental elements for cyber security, 11 October 2016.
[6] Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, May 2017.
[7] ISO 27001, the international information security standard, International Standards Organisation.

One CISO pointed out that his bank had reduced its range of counterparties by a third, on grounds the rewards did not offset the cyber-risks.

A better answer is to advise counterparties on how to fix shortcomings. "We want to be a business enabler," as a CISO put it. This is expressly a private sector responsibility. After all, only a fraction of critical financial market infrastructures is not privately owned, and the high cost of failure provides a clear incentive to act. Merck says the Not Petya cyber-attack it suffered last year has so far cost the company $400 million. And banks, it was pointed out, face the additional risks of being held liable for losses incurred by clients, and of being fined by regulators if the attack was part of a money laundering exercise.

Yet many parts of the industry, and especially the central securities depositories (CSDs), lack the resources to erect effective cyber-defences. They need either to merge, or to ask their members for money to invest, because the cost of a cyber-security failure is likely to far outweigh the cost of investing in cyber-defences. But there is no guarantee resources will be made available.

According to a survey by the Ponemon Institute, a third of CISOs believe their cyber-security budget is inadequate, and two thirds that it will either not increase or be cut. 67 per cent told the same survey their companies are more likely to fall victim to a cyber-attack or data breach in 2018 than in 2017. More than half think they will suffer irrecoverable losses of data and business as a result, chiefly because they lack they lack the expertise and intelligence to outwit their attackers continuously.[8]

A CISO advised the symposium to follow the Scout motto: "Be prepared." By this he meant not only preparing adequate defences against cyber-attack but planning the response to a successful cyber-attack in detail, in advance. Adequate defence begins with firewalls to block hostile software, updating legacy systems and patches to protect against new threats, backing up data, and educating employees to recognise phishing and spear-phishing attacks. It is important these defences are extended to new technologies, such as AI, robotics and the smart contracts used by distributed ledger technology (DLT). "With basic hygiene, you can identify or prevent 90 per cent of attacks," one delegate told the symposium.

Other delegates asked whether Cloud-based software was a defensive advantage or not. Cloud account credentials are seen by some as a source of vulnerability. Others argue the economic case for moving to the Cloud is too strong to resist, and that it offers a higher level of security - especially for small and medium-sized enterprises (SMEs), including smaller banks – because it updates patches much faster than internal processes.

"Data losses in the Cloud reflect lack of controls by the victim," explained a CISO. "I need the same visibility of my data in the Cloud as when it is directly in my control. All the Cloud providers, who used to say they would report breaches within 24 hours, now recognise that is not good enough and are starting to give real-time visibility."

[8] *What CISOs Worry About in 2018, A Ponemon Institute Survey, 9 January 2018.*

In planning the response to a cyber-attack, early detection is obviously crucial, but even then time is of the essence. Malware cannot function without electricity, but who decides whether to switch it off? "You may have only 30 minutes to decide," warned a CISO. "Looking back at 15 destructive malware attacks, the best team had only 45 minutes to decide what to do. If you decide by committee then we are going to be reading about you in the paper."

It is impossible to get the heads of businesses together fast enough to deal with a destructive malware attack occurring on such a short time-scale. Instead, organisations should form crisis management teams, made up of business leaders, PR advisers, lobbyists and legal counsel as well as technology specialists. They should draw up detailed playbooks to deal with malware, DDoS and ransomware attacks, practise regularly and "war-game" scenarios.

"If you follow a prescriptive set of directions, you will understand what to do next," explained a CISO. "It builds `muscle memory' so all the people involved know what their responsibilities are, and where they need to be, and what they need to do. You cannot build trust overnight. It cannot be surged at a time of need. The more you sweat in practice, the less you will bleed in battle."

Findings of the cyber-security break-out groups at ISSA 2018

1. A successful cyber-attack on a financial market infrastructure such as a CSD or a CCP represents the most serious risk, though it is hard to accomplish;
2. The greatest single vulnerability in any organisation is the human factor: the risk that an employee will fall for a phishing scam, share passwords or go rogue;
3. The weakest links in the securities value chain lie, relatively speaking, on the buy-side: investors and investment managers;
4. The top three factors that make the securities industry most vulnerable to cyber-attack are the high value of assets, the complexity of the value chain, and the predictability of movements of money and financial assets;
5. The risk of cyber-attack on the securities services industry will not occur in the future: it is almost certainly happening now;
6. There is no need for ISSA to create its own best practices and playbooks in cyber-security: the NIST, ISO 27000 and SWIFT CSP programme provide a ready-made set;
7. Adoption of best practices is best enforced by a combination of pricing incentives and contractual obligations to adhere to minimum standards;
8. The impact of new technologies such as AI, robotics and DLT on vulnerability to cyber-attack is poorly understood, and warrants consideration by the ISSA Working Groups on both;
9. Failure is not an option: the cost of not taking measures to enhance cyber-security outweighs the cost of taking measures to protect an organisation from cyber-attack;
10. The Working Group on Cyber-security will deliver an interim report by end-July 2018, present its key findings at Sibos in October, and publish its final report by year-end.

Distributed Ledger Technology

How large an impact will DLT have on the securities services industry?

"The disruption has already started," was the verdict of one delegate on the likely impact of DLT. The symposium heard that its ultimate effects will be comparable to those of the Internet. The precise consequences in particular business areas are hard to gauge, just as they were for the Internet in the mid-1990s, but the overall impact is already clear. Unlike traditional databases, which are siloed, DLT enables competing entities to share a single database, and make changes to the data, in a secure fashion, while preserving both the privacy and the confidentiality of the data.

"That is a big, big deal, because it creates the capability to do STP in a different way than we did it in the past, in which everybody had their own copy of the data and we reconciled them at a cost of billions of dollars and hundreds of thousands of people," the symposium was told. "At a minimum, you get cost savings. You only have to do things once, so you get reduced errors, reduced reconciliation, reduced time and delay, reduced risk, and lower capital requirements, leading to more cost savings."

Another delegate agreed that "in future, people will say it was crazy to send messages to each other to keep databases in sync." The benefits of a single database extend beyond an improved cost-income ratio. Having a single set of consistent data visible to all parties to a transaction with permission to see it will accelerate the adoption of AI, machine learning and robotics, because they all depend for their value and productivity on access to clean data in real-time - and DLT can deliver it. Regulators will also be able to access in real-time the data they need to understand conditions in a marketplace.

Why are custodian banks cautious about adopting DLT?

Despite these benefits, it proved difficult initially for DLT vendors to engage the major global custodian banks, even though the potential cost savings provide a powerful antidote to a range of existential threats to the industry. "It was career-threatening to have a blockchain or bitcoin meeting at that time," a vendor told the symposium about discussions with custodians a few years ago. One global custodian, noting that custodians were still concerned about disintermediation by DLT platforms, said stock analysts had predicted DLT would save the bank a third of its costs (32 per cent) but also rob it of nearly two fifths of its revenues (38 per cent).

The fear of disintermediation is understandable. The Internet did overthrow the incumbents in several industries, and some long-established companies disappeared. "They were on the wrong side of the 38 per cent hit to revenues without capturing the 32 per cent savings," explained a vendor. "But the Internet also created the FAANGs - Facebook, Amazon, Apple, Netflix and Google – and others who just got on with it and changed their model. It is extraordinary that there is no equivalent of the FAANGs in the financial services industry. Regulation scares them. Eventually they will understand and embrace it, so it is only for now they are not in this space."

If that is true, argued a delegate, the securities services industry needs to be ambitious about what it can create with DLT, because the FAANGs will be nothing if not ambitious. One delegate saw no sign of the requisite ambition. "If we had discussed the future over a beer ten years ago, which would we have thought more likely – settlement on T+1 or a driverless car?" asked a delegate. "Now we are celebrating settlement on T+2. People do not want the liquidity challenge of settlement on T+0."

ISSA DLT Working Group

The ISSA Symposium of May 2016 led to the establishment of a Working Group on Distributed Ledger Technology (DLT), which was charged with devising a set of principles by which DLT networks could operate in the securities services industry. The Working Group established five work streams – on governance, adoption and integration, legal and regulatory initiatives, impact on existing ISSA principles, information security, and the definition and servicing of digital assets – whose initial results were summarised in a first draft of the Working Group report published in January 2018. It was decided to focus on the impact of DLT on conventional assets, such as equities and bonds, and to reserve consideration of crypto-assets for future publications. A revised Working Group report will be released this summer, and work on defining and servicing digital assets will begin in the third quarter of this year.

What is the impact of DLT on financial market infrastructures?

Just as the benefits of settlement on T+0 require as many counterparties as possible to commit to a shorter timetable, the benefits of DLT also derive from network effects. As SWIFT and DTCC have proved, financial market infra-structures naturally create network effects between otherwise competing banks.

DLT vendors have also found infrastructures more receptive, and more effective at propagating the technology. A DLT platform placed at the centre of the clearing or settlement process in a financial market, for example, will gradually persuade users of the infrastructure to also use DLT to interact with the infrastructure delivering the clearing or settlement process.

However, infrastructural DLT platforms are not yet available off-the-shelf. A financial market infrastructure which decided at the end of last year to replace its ageing CSD platform with DLT found a complete absence of vendors with a viable solution ready to implement. This is a handicap for DLT. Since CSDs do not replace their technology platforms often, a decision to adopt DLT had to be soundly based, but with such an immature technology that level of confidence is impossible to achieve.

"We had to take our customers and board on a journey to satisfy ourselves DLT could meet functional and non-functional requirements," the CSD said. "In the end, it was a due diligence decision." Instead of conducting a gap analysis of competing platforms, soliciting customer references and choosing a supplier from a short list, the CSD had to embark on a dense and prolonged interaction with a single vendor to devise a workable model and test it.

The vendor that was chosen agreed it would have been "irresponsible" to claim it could build a replacement for the existing system in a year. In effect, the construction of the DLT platform became a three-to-five-year collaborative project between a CSD and a vendor, both unconstrained by legacy technology. Their joint objective was to build a solution capable of meeting the demands of a systemically important financial market infrastructure.

Internally, that required breaking down functional silos at the CSD. Externally, the need to persuade market participants of the virtues of DLT persisted, even after a vendor was selected. Custodian banks, registrars and software vendors had to be consulted as well as educated, through a series of events. A facility was built to show market participants how the new platform would work, and what would not change as well as what would.

"We did not get that right," the CSD told the symposium. "We under-estimated the effort needed to engage the customers." A large customer engagement team is now in place, whose members maintain bi-lateral relationships with every customer, keeping them informed as the platform develops. Importantly, customers can choose to interact with the new platform in the same way that they interact with the existing platform.

What new business opportunities are created by DLT?

However, the CSD admitted that if customers continue to use outdated methods the benefits of the new technology will be hard to realise. For some customers, and especially those engaged in paper-based processing, the transition to DLT is unavoidably challenging. Other customers are already developing new skills to exploit the technology and are excited by the possibility of automating their back offices, not just in securities clearing and settlement but in trade finance and bank guarantees as well.

"As we did the due diligence, we found things that would be interesting for our customers," the CSD told the symposium. One reason for that is that DLT is not like a conventional software application written by developers and delivered to a customer by a vendor. It provides platforms on which new services can be based by competing providers. The service providers have no need to own or understand the technology.

Among the opportunities being explored for the application of DLT are safe custody of crypto-assets, storage of information about credit default swaps in a TR, and the trading of carbon credits. Linking trading venues to enhance liquidity, while complex, is another possibility.

Connecting issuers directly with investors via a DLT network creates multiple possibilities. They include the replacement of out-of-date registers of shareholders based on record date. But the most intriguing possibility is a resolution of the longstanding debate over the respective merits of omnibus and beneficial owner accounts. Without sacrificing the efficiency of omnibus accounts, or the privacy of investors, or creating a fresh reconciliation problem, combinations of ledgers and sub-ledgers on a DLT platform could offer aggregated and disaggregated views of the same set of investors.

What are the regulatory and legal obstacles to adoption of DLT?

Many financial market infrastructures around the world are showing strong interest in DLT. In fact, the majority are already either familiar or extremely familiar with the technology. Their willingness to adopt the technology, and the timing of any decision to proceed, however, is governed by their particular circumstances. Those with ageing platforms are ready to adopt, while those which have just adopted a new technology are not.

However, infrastructures around the world have now moved beyond proofs-of-concept. A number of relatively small projects are in production already, and others have set target dates to enter production. Large and meaningful projects will be visible in 2019 and 2020. This does not mean the technology has reached maturity. The projects that are progressing most rapidly are those where it is not necessary to solve the problem of inter-operability between DLT and legacy systems, or between variants of DLT.

This is a major issue. It is highly improbable that the securities services industry will adopt a single model of DLT. Even if it did, not every market would transition to it immediately. There is therefore a need for uniform standards in data exchange and a high level of inter-operability at the technical level.

The securities services industry has a mixed record in adopting standardised methods of exchanging information, and there is a danger of new, DLT-based infrastructures increasing fragmentation. While a degree of heterogeneity reduces systemic risk, only inter-operability can deliver the benefits of network effects.

With DLT evolving so rapidly, achieving inter-operability through adoption of standardised data exchange is inevitably difficult. However, one delegate pointed to the successful adoption in 130 countries of International Accounting Standards (IAS), which are now resisted only by the United States.

"It took 17 years, but it shows what can be done," he said. "You do it by defining the objectives, what the obstacles are, and who is responsible for solving them. Or we can let everyone do the job in their jurisdictions, and inadvertently create new sets of barriers. It requires a public-private concept and working with global and regional regulators as well as national regulators. If you do not try, you will achieve nothing."

Regulators will also have to be convinced that implementation of DLT will not increase systemic risk. "If regulators are interested in DLT as a new systemic risk it is back to Square One," said a DLT vendor. "You cannot add systemic risk to the system with DLT." The CSD which has adopted DLT was able to satisfy its regulators that the new technology would not increase systemic risk.

Some at the symposium argued that current laws, rules and regulations – including rules on where data is held and can be sent, and on the recovery and resolution of failed banks and financial market infrastructures – cannot accommodate the ways in which DLT platforms exchange and store information.

However, the CSD that has adopted DLT found its choice did not necessitate any re-writing of securities laws or regulations, because its model is based on a private, permissioned network rather than a classic, trust-less blockchain depen-

dent on data miners and consensus. Instead, information is shared between participants only if the hash (or digital fingerprint) of the data is identical with the hash held by the participant. If not, the process is completed off the DLT platform.

"The original blockchain model had to be adapted," explained a DLT vendor. "But the benefit of blockchain is that every node has the promise the participant can rely on the data. They do not need to be told that by an authority. The original blockchain made all data available to everybody. It does not work in fields where data is confidential."

Keeping that data confidential is another challenge DLT must meet. The securities services industry stores records of value - the identity of the owners, their title to the asset, the provenance of the asset – and DLT must secure them against theft or loss.

One of the major risks that has emerged is the use of "smart contracts" – self-executing contracts, written as computer code – on DLT networks. The languages in which these must be written are unique and specialised, and it is hard to recruit the developers familiar with them, so there is a high risk of software bugs in smart contracts. They are presently being written in a variety of general purpose codes that are not always compatible, and which are vulnerable to hacking, creating a risk of financial losses that cannot be recovered by litigation or insurance.

Findings of the DLT break-out groups at ISSA 2018

1. DLT practitioners need to do a better job in educating the industry about the technology, and especially about private, permissioned networks versus the public blockchain, because they solve all the major problems that have been identified;
2. Any business looking to apply DLT should start by writing down the problems it wishes to solve with DLT, because that leads to a more productive conversation with DLT providers;
3. Network effects are crucial to the success of DLT, so it helps to have an installed client base that can be transitioned to a DLT network;
4. DLT provides a single "golden" source of data, giving permissioned participants a single source of truth that is both synchronised and accurate;
5. Smart contracts are currently neither smart nor contracts and represent a serious risk of irrecoverable loss, so users should choose a code that imposes discipline on how smart contracts are written;
6. Migrating to a DLT network precludes running old and new systems in parallel, which makes pre-launch testing more than usually important, though the risk can be mitigated by maintaining multiple connectivity options after going live, and switching from proprietary message standards to ISO 20022;
7. The slow speed and high energy consumption of the consensus-led public blockchain makes it impracticable to run current volumes of transactions in the securities industry on the technology, let alone scale the volumes up, but regulated banks and financial market infrastructures can dispense with the consensus mechanism because they do not have a trust problem and

can instead make sure data exchanges on the platform are both light (with historic data stored off the network) and flawlessly synchronised;

8. The challenge of DLT as technology is less daunting than the legal and regulatory challenges set by DLT, but DLT can be configured to work within existing laws and regulations, obviating the need for any changes at the outset while leaving room for changes in the future that might help to make the network more efficient;
9. The security of data on a DLT network is an unsolved problem because DLT replicates a single source of truth in every node on the network, so 100 per cent of the data on the network is held by every node, creating problems for a financial services industry in which law and regulation impose privacy and confidentiality rules on all market participants, and no market participant wants to give a competitor access to sensitive data, and in which protection of data through private keys is not a viable solution because computing power (ultimately, quantum computing power) will eventually break any form of data encryption;
10. Inter-operability is not a problem in a closed, permissioned network in a single jurisdiction, in which the entity at the centre (such as a CSD) installs a ledger operating under a single set of laws and regulations, and users of the central services are obliged to work out how to interact with it using their existing systems, but inter-operability between DLT networks and between DLT networks in different jurisdictions, remain unsolved problems;
11. DLT cuts costs within organisations by reducing the time taken to reconcile data and settlement transactions, enabling reductions in the capital allocated to the risk of trade failure, and by facilitating cost-reducing innovations in the back office through the provision of structured and consistent data;
12. DLT cuts costs between organisations by distributing a single source of truth to all counterparties, and assigning rights and obligations to counterparties automatically, raising rates of automation between counterparties;
13. DLT generates new revenues because an application built to run on one node in a DLT network will automatically run on all nodes;
14. DLT facilitates the adoption of AI, machine learning and robotics by feeding them with high quality and real-time data;
15. Regulatory compliance is made more efficient by DLT because reports are built from data already held within DLT network, regulators can access the data directly by becoming a node on a DLT network (with permission to read the data), and rules and regulations, including pro-active market surveillance, can be coded into the DLT network;
16. Investor protection can be improved by DLT without sacrificing operational efficiency because a DLT network can accommodate both omnibus and beneficial owner account structures, in which permissioned nodes can see through the omnibus accounts to the underlying beneficial owners;
17. The sharing of Know Your Client (KYC) and Anti-Money Laundering (AML) information through a DLT network makes KYC and AML checks more efficient;
18. DLT can be applied to multiple asset classes and use-cases, of which trade finance, letters of credit and bank guarantees are the most obvious.

Robotics and Artificial Intelligence (AI)

Can new digital technologies cut costs in securities services?

According to data published by McKinsey, securities services revenues grew at 3 per cent a year between 2010 and 2016, a slower rate than global asset prices, but enough to lift total revenues from $75 billion to $89 billion. Of that $89 billion, custody accounts for the largest share (29 per cent), followed by fund administration (20 per cent), net interest margin (19 per cent), ancillary services such as collateral management and compliance products (14 per cent), prime services (10 per cent) and corporate trust (8 per cent).[9]

Profitability, however, has worsened. Between 2010 and 2016, the overall revenue margin in custody has declined by 2 per cent a year, from 1.7 basis points to 1.5 basis points. In fund administration, the margin fell by 1 per cent a year, from 4.5 basis points to 4.2 basis points in the same period.[10] This reflects a combination of higher regulatory costs and margin pressure in the asset management industry, chiefly as a result of the switch from high cost active to lower cost passive investment strategies.

So even with revenues up, margin pressure in their core businesses has placed custodian banks and fund administrators in a Red Queen race: running faster to stand still. To change this dynamic, custodian banks need to do more than squeeze existing staff and systems harder. They have to make transformative structural changes.

This explains the interest senior management of securities services firms are showing in new forms of digital technology, such as artificial intelligence (AI), machine learning and robotics: they can cut costs. McKinsey believes automation and robotics can cut as much as $20 billion from an industry cost base of $62 billion[11], but it is not clear if the cost reduction will be a one-off gain or a sustainable reduction in costs.

What can the new digital technologies do?

There is also a danger, in referring to AI, machine learning and robotics, of being merely "buzzword-compliant," since the terms cover a wide range of possibilities. They divide into five main groups. These are *robotic process automation* (automation of routine but repetitive tasks), *smart workflows* (integrating tasks performed by humans and machines), *machine learning* (identifying patterns in data), *natural language processing* (optional character recognition of verbal as well as written texts) and *cognitive agents* (the AI component, providing a virtual workforce capable of supporting employees and customers).

Robotic process automation is a relatively mature area, with a large number of vendors[12] offering services, and most custodians running a proof-of-concept at

[9] McKinsey & Company, *A calm surface belies transformation in securities services*, March 2018, Exhibit 1, page 5.
[10] McKinsey & Company, *A calm surface belies transformation in securities services*, March 2018, Exhibit 3, page 7.
[11] McKinsey & Company, *A calm surface belies transformation in securities services*, March 2018, page 13.
[12] For example, Blue Prism, Celaton, UiPath, PegaSystems OpenSpan, and Automation Anywhere.

least, in areas such as reconciliations and corporate actions processing. The challenges lie in scaling robotised processes and capturing the value, because many processes are highly automated already and those which are not consist largely of low value-added work performed by low-cost human beings. Where robotisation has the greatest potential is in areas untouched by digital technology. Although these fields can add up to significant cost savings, they appear too small to build a robust business case, and in any event fail to attract the interest and investment of vendors.

Smart workflows, which combine machine and human capabilities, are proving effective in a limited range of areas, such as case-handling investigations and month-end processes. *Natural language processing* is also being widely used in chatbots and to segment emails. What is much less evident in the securities services industry is *machine learning* (where advanced analytics could be applied to client queries) and *cognitive agents* (which have obvious immediate application to first and second level client query handling but are intended in the long run to interface directly with clients at all levels).

The available cognitive agents, such as Amelia from IPSoft, have a limited scope, and are difficult to scale. They are learning from scripts, and evolving fast, but need time to mature. Cognitive agents are unlikely to make much impact on client service in the next two years. If cognitive machine intelligence remains a relatively remote prospect, proofs-of-concept with 50 robots where multiple employees are doing the same repetitive task are proving successful.

The challenge of scaling up from 50 to, say, 5,000 robots is harder and more complex. It requires a transformative approach, because the project soon encounters employees doing singular tasks on their own. In this situation, it is impossible to simply replace people with robots. The process has to be fundamentally re-designed to make robotisation possible, and to capture enough quality data for the robots to make better decisions.

In fact, the initial focus in robotic processes on speed proved to be misplaced. The real benefits lie in improved visibility and control, which in turn depend on clean, high quality data. “You can see every transaction a robot makes,” explained an expert. “The robot does not make a mistake. If the data input is poor, the robot does not work. It is not a case of the robot not doing a good job – it simply does not work at all.”

Who should control the investment, installation and maintenance?

This re-design necessary to improve the quality of the data capture cannot be executed by an IT department, or a vendor, but has to be led by the head of the business. In corporate actions processing, for example, an employee will take a set of data, process it and pass it on to clients in a much less structured way. Before it can be robotised, the task has to be broken down into a series of smaller tasks, and that can be done only by someone who understands corporate actions - in effect, by the people who will use the tool.

This is what motor manufacturers found when installing robots on the production line. The process had to be led by the plant manager in the factory, not least to remain compliant with regulations. “Many transactions are highly regulated,” it was explained. “Getting to the stage where a robot checks a robot is way off. The idea that a robot is owned by IT is a mistake. The robot is a tool of the

manager of the operation, and the robot has to be compliant. Robots are always blamed for a process going down, because nobody trusts them, but robots can read only what they are told to read. If you change the data it reads, it will put transactions into a queue."

This poses a governance question, which has broader implications. If robots cease to work because of invalid data inputs somebody requires the authority to change the data inputs. The same consideration applies if a robot starts to behave erratically. Robots in fact have user identities (IDs), in the same way as employees, which puts the controller of the robot IDs in a strong position to cause disruption. It raises a question familiar to custodians – *Quis custodiet ipsos custodes?* – and one which will become acute as the industry adopts cognitive AI.

But the chief lesson of the experience of robotic process automation so far is that banks wanting to use robots to make an impact on costs should not think of automation as an end in itself, but as a means of improving the cost-income ratio. That requires thinking beyond the technical capabilities of the machines. To capture the value from robotisation, firms need to understand the flows of data through their organisation, and integrate people, processes and machines. That takes time, and there will be setbacks. Structural changes are required.

"It requires a new way of working between IT and the business," the symposium was told. "You need to allocate work to humans based on what the robot cannot do, not just replace people with robots. Line managers have to understand robots are a tool and build them into the operational processes. One way to deploy bots is not to wait for data to be perfect but to experiment and see if it can work with 60 per cent of the data. Automation takes place progressively. You cannot just re-design the process and replace people with robots."

The head of robotic process automation at a major bank agreed. "IT cannot find the opportunities for you," he said. "The business people must, or you just end up in endless technical testing. If your only tool is a hammer, everything looks like a nail. If your only goal is to build 300 or 500 bots, you will get them, but you will not solve problems or seize opportunities."

Over the last two years, he has completed 44 projects and 54 change requests across 24 separate business functions, and now has 300 robots active across 212 automated business processes. "There has been nothing easy at all in moving from the pilots to the steady state," he noted. "For every two steps forward, we took a step backwards."

What processes are most suitable for robotic process automation?

Finding the right opportunities to automate was the first challenge. An early pilot, with 25 people whose sole occupation was to press the F1 key to find missing fields, and then pause while searching for the missing data from 30 separate applications and entering it once found, proved relatively easy to automate. It "took the robot out of the people."

Getting the content of unstructured faxes, some hand-written, into a format a robot could understand was more challenging, since it entailed inserting an optical character recognition (OCR) device into the process. The OCR had to read

the data and then deliver it to the robot in a structured form, so the robot could then in turn key the data into the bank systems.

The bank now subjects all processes considered susceptible to robotic process automation to a 14-day assessment process. Most processes do not get beyond day seven, because the process is judged to be too complex. Even those processes judged to be suitable have to be reviewed and streamlined. "If you automate a poor process, you just do it poorly but faster," the symposium heard. "Robots are not a bandage over a wound."

As one delegate put it: "Fix the process first. You cannot get the cost savings without the process improvement." This remark indicates how hard it is to find the right opportunities for robotic process automation when so many processes in the securities services industry have accumulated over time and have yet to be simplified and standardised.

The most suitable opportunities were found in account closures, data acquisition, foreign exchange sales, international central securities depository (ICSD) trade inputs and US dollar funds transfers. Other candidates include internal account transfers, emailing of counterparties to fix unmatched trades, account opening, and the replacement of internal calls with chatbots.[13]

Does the investment in robotic process automation pay for itself?

One wit at the symposium added to the list of opportunities, not without just cause, "anything IT do not want to do." But the more complicated processes tend to fail the return on investment (RoI) test, partly because robots do not replace employees, but take over only 30-60 per cent of what they do. In addition, linking different applications adds to the expense.

A third factor limiting the range of opportunities is the prevalence of offshoring in the securities services industry, making it harder to realise cost savings. Although there is a view that robotic process automation makes it possible to "re-shore" operations previously offshored, offshoring is at present a barrier to adoption. "You need to understand *where* the work is being done," explained a delegate. "If a lot of the work is being done in India, the cost dynamic of having 15 offshore resources versus 15 people in New York City is very different."

Another factor deflating the RoI is the high cost of talent. As more processes are automated, the collective memory of the organisation diminishes, and those that remain become more valuable. "The less people we have the more they matter," as one delegate put it. They can command higher salaries, at least until cognitive AI can replace them as domain or subject matter experts.

The immediate problem is that custodian banks are struggling to attract the right people to make use of the new digital technologies. Those they do attract tend to be expensive, further eroding the return on automation. "We are in a 24/7 environment with bots, and they have to be maintained not just installed," the symposium was told. "Finding the right talent is very hard in big financial centres like New York and London. Why would you join a 250-year-old bank when you could go to IPsoft?"

[13] See Exhibit 11, page 20 in McKinsey & Company, A calm surface belies transformation in securities services, March 2018, for a list of processes susceptible to automation and robotics applications.

Findings of the robotics and artificial intelligence (AI) break-out groups at ISSA 2018

1. Robotic process automation and smart workflows are the most prevalent forms of digital automation in the securities services industry, but they deliver operational efficiency rather than strategic transformation, which is promised by cognitive AI, natural language processing and machine learning;
2. Robotic process automation and smart workflows are best deployed to make manual processes more efficient;
3. The cost benefits of robotic process automation and smart workflows are limited to 2-3 per cent unless combined with a broader process re-design, in which case they rise to 10-15%;
4. There is limited experience of cognitive AI, machine learning and natural language processing but potential use-cases include predicting cyber-threats and client behaviour, and they are more likely to create opportunities to manage risks and generate revenue as well as increase efficiency;
5. The attraction of robotic process automation lies in its ability to make organisations leaner, and to re-shore activities previously offshored without any loss of cost savings – in other words, robotic process automation and offshoring are not complementary, but alternatives;
6. Selling robotic process automation internally nevertheless remains challenging because the return on investment (RoI) is not convincing, even after taking into account the freeing up of staff capacity to focus on higher value tasks;
7. The human dimension reduces the RoI because although automation can reduce headcount, per capita costs go up, partly because the technology demands higher quality and more expensive people, and partly because the people that remain become more valuable and losing them is a higher risk;
8. Use-cases are difficult to identify because they are driven by the part of the business each organisation operates in, and the size and scope of its business in that field;
9. Use-cases identified include corporate actions data, and predicting problems in IT deployments, but in general the tools will be applied fastest in those parts of the securities services value chain that are (a) characterised by repetitive processes and (b) have received the lowest levels of technology investment to date;
10. Customer satisfaction and revenue generation opportunities in robotic process automation are exceptionally hard to find;
11. Robotic process automation is nevertheless worth pursuing even if it only breaks even after investment and staff costs, because of the risk-reducing properties of machines that do not make mistakes;
12. Governance is an issue, since robots need to be controlled, to mitigate the risks of erratic behaviour and self-proliferation, and the controllers of the robots need to be supervised, also to mitigate the risk of erratic behaviour;
13. It would be helpful to produce guidelines for clients interacting with automated robotic applications to reduce the risks of erratic behaviour by robots;

14. ISSA should produce a summary of the Symposium discussions, but not set up a Working Group to explore robotics, AI and machine learning, because DLT and cyber-security are higher priorities, but a Working Group might become necessary as the securities services industry moves beyond robotic process automation into cognitive AI and natural language processing;
15. That said, there may be synergies between DLT and robotics, AI and machine learning, in the sense that the better synchronised, higher quality and real-time nature of data produced by DLT networks can eliminate the need for reconciliations and raise the performance of robotics, AI and machine learning tools.

Financial Crime Compliance Principles Panel

The Financial Crime Compliance Principles Working Group is not, as its name might suggest, charged with devising principles. Instead, it focuses on identifying practical ways for custodian banks and financial market infrastructures to implement the 17 Financial Crime Compliance Principles (FCCP) published by ISSA in August 2015.

The ambition is to ensure that all parts of the securities services industry have implemented the principles by the end of 2019, in much the same way that private banks adhere to the comparable Wolfsberg payments transparency standards first published in 2007. "We want the ISSA principles mentioned in securities in the same way as the Wolfsberg standards are in payments," said a panellist.

The industry embarked on the long journey to FCCP to avoid regulators imposing change unilaterally. In particular, the industry was concerned to defeat the regulatory preference for end-investor or beneficial owner accounts. In the estimation of the industry, intermediated, commingled, omnibus accounts have made a large contribution to the achievement of scale and to the maintenance of competition between banks, which would be forfeit in a beneficial owner model.

It was impossible for the securities services industry to simply adapt anti-money laundering regulations (such as the Fourth Anti Money Laundering Directive issued by the European Union) because the regulations tend to focus on payments. For a custodian, responsibility does not cease at settlement. "A payment is just for Christmas," joked a panellist. "A security is for life." In other words, assets in custody have also to be serviced, and the regulations do not cover asset-servicing, even though money launderers commonly use securities to transform illicit cash into a liquid asset.

Nor is the risk confined to stocks or bonds. Money launderers also use funds. The transfer agents to funds, which run the Know Your Client and Anti-Money Laundering checks on fund investors, tend to focus on completing the paperwork rather than assessing the risk. This is because the regulators of the funds industry go further than the 17 principles, requiring transfer agents to know exactly who the end-investor is in every case, rather than conduct a risk assessment of the account-holder. "Understanding the end-investor in every case is inconsistent with the ISSA approach," said a panellist. "ISSA may need to work with mutual fund trade associations to push back."

"The custody industry has so many layers it is easy to hide the money being laundered," a panellist told the symposium. "Four years ago, we thought we just had to portray ourselves as the good guys. Today, we recognise we have to take the lead in protecting the industry by developing principles and getting banks to implement them." To this end, the Working Group has issued a revised version of its financial crime due diligence questionnaire, for distribution by banks to their account-holders to check their level of compliance with the 17 principles.

Unfortunately, the initial reaction of account-holding banks to the questionnaire was resistance. Banks have many different divisions (including trade finance and

payments as well as custody) and multiple interests (relationship management, sales, account management and reconciliations) within those divisions. The confusion and pushback suggest the language in which the principles are couched is not always clear and needs to be simplified and communicated better. "We need to demystify it," said a panellist. "In hindsight we could have done better."

Banks that have decided to re-document relationships with clients to take account of the 17 principles have certainly encountered resistance to disclosure of end-clients.[14] "That we had a problem was discovered by us with the BBH case in 2014[15]," said a panellist. "We wanted to solve that concrete problem in a quick and dirty way and added language [to service agreements] that said we might in certain circumstances need to disclose the identities of the end-clients. It was only after that that we sought an industry solution, because none of our clients understood why we asked additional questions – they just said it was `none of your business.' But we need and want end-investor information across all our clients."

In this context, the concomitant implementation of the General Data Protection Regulation (GDPR) in the European Union was unhelpful because it inhibited banks from agreeing to such disclosures. Another panellist had encountered resistance to the 17 principles on precisely these grounds of client confidentiality. "As of today, the industry is still not ready," he said. "A client seminar a month ago found only a third had heard of the principles, and only one counterparty had kicked off a project. Being the front runner [in the implementation of the principles] is not easy."

However, the panellist nevertheless thought his own bank was now close to full compliance with the 17 principles. "We are at eight or nine out of ten," he said. "To get to ten, we would need to know every beneficial owner from end-to-end, which we do not want to do. We want a trust-based model. We want to trust each other. I would hope we can come to a ten without it ending in `death by data.'" Other banks on the panel placed themselves between five and six out of ten. "Implementation is far from complete," said one. "Getting to eight is something we can reach, because the roadmap is clear. Moving from eight to ten will be more difficult."

It was explained, in response to a suggestion that ISSA could accelerate the adoption process by publishing a detailed guide to best practice in bank-to-bank due diligence, that the principles have to be adapted to each jurisdiction. "Every custodian has to refer to local laws and regulations, and tailor it to local circumstances on the basis of the minimum standard ISSA sets for the global

[14] Principle 17 stipulates that "the custodian should be entitled to require its account holder to disclose the identities of the ultimate buyer and/or seller of a security in response to a specific request predicated on risk factors (i.e. red flags) within a reasonable period."

[15] In 2014 Brown Brothers Harriman (BBH) was fined $8 million by the Financial Industry Regulatory Authority (FINRA) in the United States on anti-money laundering grounds, for executing transactions in low-priced securities on behalf of undisclosed customers. In January of the same year Clearstream Banking paid $152 million to settle claims by the Office of Foreign Assets Control (OFAC) that it had provided a sanctioned state (Iran) with access to the securities markets of the United States.

industry," explained a panellist. "That should help the industry get to best practices globally."

This is why the 17 principles were developed in such a way that they can be translated conveniently into any legal framework. "We developed the principles so that all market participants could implement them within their own local legal framework," said a member of the Working Group. "The principles aim to raise awareness - to give you a framework. You have to use the due diligence questionnaire for the practical purpose of actually implementing the principles."

There is a concern that ultimately only the largest banks will implement the 17 principles, with small banks that are customers of the larger banks taking on riskier clients. One delegate explained that sub-custodian banks obliged by local regulators to obtain information about the identity of end-investors are being refused by global custodian banks. "Even when shown the letter from the regulator, they do not provide the information," said the delegate. "Banks find they are losing business to less scrupulous competitors."

By that means, as a panellist pointed out, illicit assets are bound to reappear within the networks of the largest banks as the smaller or less scrupulous bank reinvests the cash or relocates the assets. To avoid that risk, some banks are banning all transactions with sanctioned states and individuals, and blocking their assets. But even this drastic measure does not eliminate the risk because blocked assets still have to be serviced in terms of corporate actions and tax reclaims, and there is no guidance from regulators as to whether servicing blocked assets is a breach of the rules.

One delegate explained that his organisation had chosen instead to terminate its relationship with any client that refused to sign a contract that obliged them to disclose information about their clients in certain, risk-based circumstances. "They might become clients of a competitor but over time standards will affect lower tier players as well," he said. "Not disclosing information confers no competitive advantage. It is much easier to talk to your counterparts than to deal with the Office of Foreign Assets Control (OFAC)."

The panel concluded with a warning as well as reassurance that progress is being made in implementation of the principles. The volume of transactions and holdings that create a compliance risk is rising, thanks largely to the extension of sanctions. To mitigate it, financial compliance needs to be "operationalised." If it is not, the cost of failure will be high.

"The numbers are very large," warned a panellist. "If the industry gets it wrong, one transaction can be fatal. Banks that accepted investments in securities that came from illicit sources have disappeared. Venezuela would not have happened if they could not accept those securities. This threatens our industry."[16]

[16] In January this year, the Swiss Financial Market Authority (FINMA) began an investigation of Swiss banks for alleged involvement in laundering money for the benefit of Venezuelan state officials who had accepted bribes from vendors.

ISSA Financial Crime Compliance Principles Working Group

Financial crime compliance has become a major risk factor for custodian banks, with regulators imposing heavy fines on firms which intermediate investments by money launderers, terrorist groups, politically exposed persons and sanctioned individuals and states. To help banks comply with their obligations, ISSA published in August 2015 17 financial crime compliance principles for implementation by custodian banks ond other intermediaries, akin to the anti-money laundering (AML) principles published by the Wolfsberg Group of global banks active in the private banking industry. The objective is to achieve adoption of the 17 principles throughout the securites services industry by the end of 2019. To drive that process, ISSA has established a Financial Crime Compliance Principles Working Group, made up of representatives of custodian banks and financial market infrastructures including central securities depositories. It meets regularly to discuss progress, share concerns and agree best practices. Results and conclusions should be communicated more frequently via various channels starting in the course of 3rd/4th quarter 2018.