STAYING AHEAD IN THE NEW ERA OF BANKING

WHY BANKS MUST REIVENT THEMSELVES

RiskMinds 365

CONTENTS & INTRODUCTION

RISKMINDS

Strategy Director
Victoria Chatterton

Editor-in-Chief, RiskMinds International, RiskMinds Americas
Ed Stapley

Editor-in-Chief, RiskMinds Insurance & RiskMinds Asia
Ana-Luiza Olanescu

Digital Content Editor
Charlie Burgess

Business Development Managers
Georgia Hood & Josef Lanjri

CONTRIBUTORS

Group Chief Risk Officer, Maybank Group
Dr. John Lee

Managing Director & Head of Singapore,
CBG Technology, DBS Bank
Sonia Wedrychowicz

The finance industry is constantly evolving, and keeping up with new players and innovations from the competition can seem like an insurmountable task.

Traditional banks are coming head-to-head with new FinTechs, as both compete for the same customers and strive to create new products to meet expectation. Conventional business models are being disrupted and only those who adapt can win. It's not only external factors pushing banks to the brink, cyber threats and conduct risk are also consistently found as the top concerns for CROs across the globe. Whether it's a determined hacker or staff breaking rules for personal profit, the risks are real and a constant threat.

2018 ushers in a new era of banking - a time where reinvention is a must to remain relevant. In this RiskMinds365 eBook, we explore the challenges and opportunities that should be at the top of your new year strategy.

Enjoy!

The RiskMinds Team

What keeps CROs awake at night?

RiskMinds365

We brought together some of the leading CROs to discuss the common "pain points" in the industry today, and ultimately answer the question: "what keeps you up at night?".

CYBER SECURITY

Out of all CROs questioned, 53% responded with cyber security as a "top 3" concern.

This isn't surprising, as our dependence on the internet has increased, so cyber-crime has moved from obscurity, into the spotlight for not only the consumer, but also for corporate and international security concerns. Former Scotland Yard Detective Superintendent, Charlie McMurdie, gives it straight: "Cyber-crime is cheap to commit and expensive to defend, criminals operate within the virtual environment and as such are not constrained by real world boundaries. It's not by chance that they exploit the widely differing legal and regulatory regimes in place within different countries."

One respondent elaborated further, "the sheer complexity and exponential growth make cyber-crime one of the most significant risks that keep me awake at night. I have spent a significant amount of time during the past year familiarising myself with the nature and complexity of the threat vectors. It is incredibly difficult for organizations to protect themselves and I believe we are at a very early stage of the evolution of this risk type. We are bound to see significant incidents over the next few years." Indeed, the recent breach of U.S. credit monitoring firm Equifax, which resulted in the leaking of personal information for around 143 million individuals, demonstrates that the scale and impact of data breaches are only increasing.

"It might be quite hard to hack a server, but a poor password policy may result in the very same data breach in a much simpler way."

Another senior CRO discussed the risk of social hacking within the realm of cyber security, "Often enough people speak about cyber security, compliance, policies, and procedures, forgetting that after drafting any policy they should also work on its effective implementation. It might be quite hard to hack a server, but a poor password policy may result in the very same data breach in a much simpler way." The fact of the matter is, the methods of would-be hackers have not changed dramatically: phishing—increasingly spear-phishing—is still amongst the most popular attack vectors. Simple employee awareness remains a major challenge.

GEOPOLITICAL INSTABILITY

The CROs we panelled have a widespread geographical influence and responsibility, and so the current geopolitical climate was an expected top pain point. In fact, one third put it in their top three concerns, with some stating specific concerns with Trump and Brexit, and others pinpointing more localised pressures within their own markets.

Delving into this a little further, one respondent said they were concerned about, "any risk which is hard to measure and might have systematic effects, like geopolitical risks. When

it comes to risks which are hard to measure, the complexity of having an effective strategy to mitigate that risk increases exponentially."

Recent election results in Germany, France, and the Netherlands may soothe the nerves of CROs concerned with the rise of right-wing nationalist populism, but that would ignore the strong showings by far-right parties like Alternative for Germany (AfD) and the National Front in France. The forces and attitudes that contributed to the victory of Trump in the U.S. and Brexit in the U.K. are still very much present, and could continue to pose a risk to markets as well as political stability.

REGULATORY CHANGE

The third most popular pain point was regulatory change, with over one third of our CROs stating this a pressing concern.

As the risk management industry is aware, several new regulations are coming through and are due to go live in the new year, including IFRS9 and MiFID and Volcker. Even for companies well placed to handle the changes needed to implement new processes and requirements, the sheer volume of adjustments necessary is keeping some CROs awake.

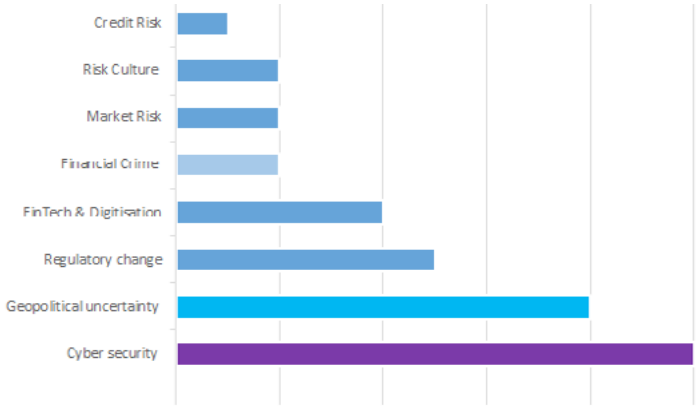
"The burden of regulation is now monumental and potentially having unintended adverse consequences. While much of the regulation was proven to be necessary due to poor industry self-regulation as evidenced by the global financial crisis, the overload of new regulations and their exhaustive implementation can impact the profitability of banks that is necessary for a strong well capitalised banking industry. Risk managers can also 'take their eye off the ball' of the commercial risks as they are distracted with the reporting, governance, and bureaucracy of compliance," stated one CRO.

OTHER PAIN POINTS

While almost all the CROs agreed on at least one of the above risks as taking up prime real estate in the top three pain points, there were a variety of other responses which were highlighted too.

These include financial crime and fraud, risks arising from digitization and FinTech, and traditional credit and market risks.

The chart shows the full range of responses to the question, and emphasizes the growing number of risks CROs must keep on their radar to be effective and ensure a sustainable and profitable business.



The two big Cs – conduct and cyber risk

RiskMinds365

Conduct and cyber risk are commonly thought of as non-financial risks. But one of the arguments during RiskMinds International was that they are just as much a financial risk as any other. That's because they nearly always have – sometimes massive – financial consequences.

Conduct risk can be quite difficult to define, but what it generally boils down to is people risk. In that respect so is cyber – it only takes one person to click on a link in an email to unleash a cyber attack. The last decade has seen an explosion in conduct-related losses. It's a topic that needs taking very seriously.

TAKING CYBER AND CONDUCT RISK SERIOUSLY

And banks are indeed taking it seriously. "Conduct and cyber need to be treated with the same rigour as credit risk," stated Alan Smith, Global Head of Risk Strategy and Senior Executive Officer of Group Risk at HSBC.

Giulio Mignola, Head of Enterprise Risk Management at Intesa Sanpaolo agreed, adding that, while cyber and conduct risk were less mature than credit risk, the discipline should be exactly the same: "You have to have a risk appetite statement, formulate a response, and make policy go all the way down the line to the operating processes."

"These two risks are financial at heart but also have impacts on customer loyalty and brand value."

For many years, cyber threats were considered technical issues, but banks are digital companies nowadays, he added: "We need to manage digital risk as a primary risk." And losses extend well beyond those that are tangible: "These two risks are financial at heart but also have impacts on customer loyalty and brand value," says Mignola. "This soft effect is much more difficult to quantify."

THE INSURANCE PERSPECTIVE

Insurance companies are also taking these risks seriously. Underwriting cyber risks is a massive growth area.

But how do insurance companies calculate the premiums? Rachel Conran, Chief Underwriting Officer at SCOR Group, walked us through the calibrations that she uses when underwriting corporate conduct and cyber risk.

"I look at the causes that lead to that conduct," she began. "For instance, cultural cohesion. If the c-suite is an island, an inner circle of people, or there isn't diversity and people that will challenge the board, that can ring alarm bells. What happens at the board level trickles down; the board set the cultural acceptance of a corporation," she explained.

So Conran watches out for things like whether family members are employed at the corporation, and the use of the corporation's private jet - whether for personal use - in other words, the blurring of boundaries. That also includes looking at how people are remunerated - which shows how acceptable it is within the organisation to spend corporate money.

"If they are self-serving there are generally two effects

among employees: people who would like what they've got, and those that want to disrupt it," she said. "Cyber attacks can be criminal or they can be perpetrated by an insider – those institutions that have the biggest difference between top and bottom, a them and us, will cause issues like these to become more prevalent."

Indeed, this was why Mark Lynch, Cyber Analytics lead for EMEA at Aon Benfield had added employee monitoring, specifically employee satisfaction, to his list of things to look at. "Disgruntled employees can be often be the cause. So we might look at how many times the same job has come up for recruitment. Is there a lot of churn?" he said.

Investors and stakeholders also drive the behaviour of a firm. "For instance," asked Conran, "How easy is it for a member of the board to move out of a high return area of equity, because it's high risk? Will they be under significant pressure not to, from shareholders who want those high returns?"

CYBER IS AN AREA OF GROWTH

Insuring companies for cyber risk is more than simply offering financial recourse, it's about dealing with the response and the fundamental issues that occur immediately post-event, Lynch argued.

"It requires a cultural change within the insurance sector, which is used to looking at bricks and mortar," he added. "Cyber takes on a completely different perspective because it's across countries, jurisdictions, and insurance frameworks."

And that cultural perspective should apply to banking too, added Smith: "You can't expect insurers to pay out for something we don't understand ourselves."

And we can't assess cyber risk in isolation, said Lynch. "Suppliers, lawyers, tax accountants, there are lots of access points that you can't control. There is so much outsourcing and third party vendors, these are all concentrations of cyber risk that can blow back to us."

"Banking is the best industry across the board in terms of risk management, but it was also the most targeted by hackers."

HOW DO BANKS GET HACKED?

Banking is the best industry across the board in terms of risk management, but it was also the most targeted by hackers, thanks to the value of their data.

Some of those hackers are ethical, meaning that they are hired by an organisation to test their security systems, like Freakyclown (FC), Co-Founder of Redacted, a company that advises firms on their security, both physical and cyber.

Dispelling any doubts about the importance of cyber risk, FC showed just how easy it was to access a company's top secrets, in a live RiskMinds performance.

Within seconds, his fictional hacker "Alice" was able to enter the desktop of office worker "Bob", who had clicked on an innocuous email.

Within twenty minutes, Alice had managed to source usernames and passwords from others in the firm, climb up in privilege to beyond administrative level, and change the bank details and the amount of a payment that Bob was planning to process.

Without Bob ever having a clue.

Interestingly, FC explained how most hackers don't use the information themselves. They take that access and sell it on to multiple people. He might find eight or nine different groups in a system that have got there this way. On average, a hacker stays for 200 days in a system before being found. That's over six months.

"Banks are considered best of the best of the best, they do security really well, but they're still not quite good enough. Just having security doesn't mean it's done well."

Physical security is so easily flawed, he continued. "I look at most companies as an armadillo. A tough outer shell, gooey in the middle. Once you are past the outer perimeter you can do anything. And the perimeter is never that secure." To emphasis the point, he showed how a security door that cost in the region of £60,000 ($80,000) door could be breached - simply by spending a few hours watching it. "It had been left in engineer mode, which means that it was programmed to open every 15 minutes," he said. "Expensive doesn't mean secure."

Similarly, he displayed the pointlessness of using a shredder if the bags are then left on the kerbside for collection. “This is highly confidential data, but once it becomes rubbish they don’t care. It wouldn’t take long to put those documents back together.”

SPEARPHISHING

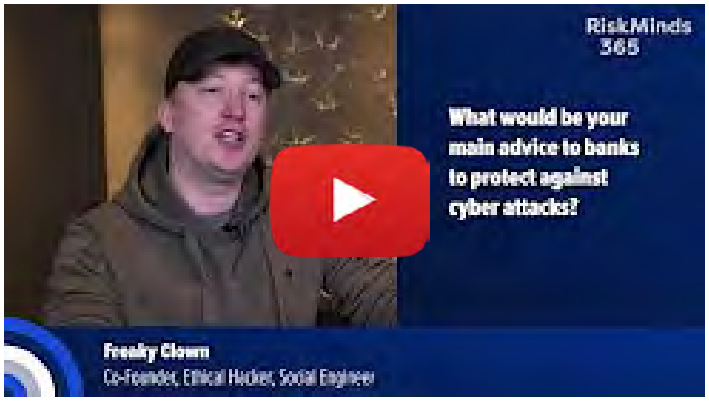
The biggest risk to companies now is not hacking groups or nation states, it’s spearfishing, he warned. “Around 30% of an organisation’s staff will click on a link in an unsolicited email. With training, that number can be reduced to 1%. But in a 10,000-strong organisation that’s still 100 people.

“Even if you email them and explicitly tell them “do not click this link”, 1% still click the link,” he said. And it only takes one for things to go wrong.

What can you do? “Know your information assets,” advised FC, “what you have that’s of value, what you have that others want.

“Approach it with an attacker’s eye view: perform penetration tests. Plan your incident response - and test it! Remember that people are at the core of your security, have an awareness of behaviour and security. Teach from the top down, people follow the c-suite , similarly, if they have security at home they are more likely to be aware of it at work.”

But ultimately, he urged us to adopt a “hacker mindset”: “Go back and up the game at your company.”



Inside the mind of a rogue trader

RiskMinds 365

RiskMinds365

Risk culture, conduct risk, operational risk, these topics have been at the forefront of the risk management industry throughout 2017, and risk managers have been privy to a lot of advice about how to handle these risks, including best practice in risk management and how technology can help us do our jobs better.

It's not often that we get to hear from someone who has caused the most feared risks to become a catastrophic reality. Someone whose very name evokes the biggest scandal of an era; like Nick Leeson and the collapse of Barings Bank.

HAVE WE REALLY LEARNED ANYTHING?

"I bet you don't know whether you should clap or boo," began Leeson as he took to the stage.

Leeson's isn't a tale of greed or of deliberate obfuscation, at least, it didn't start that way. It's a story of poor risk mismanagement and personal flaws, which contributed to series of events that spiralled out of control and ultimately leading to the collapse of a 233-year-old bank.

The Barings Bank Scandal was supposed to be a wake-up call that no one would forget, yet over the last 22 years there have been a number of other financial scandals. It seems we still have plenty to learn. In particular, the fact that understanding how to manage risk is just as important now as it was when Nick was a trader.

"I was someone who didn't understand or manage risk at the time," admitted Leeson. "I didn't manage my personal risks – I never expected to be in prison – and the bank didn't manage theirs either."

Leeson had expected risk controls to be in place. After every trade executed to cover his tracks he expected a knock on the door. Yet day after day, month after month, even year after year, those knocks didn't come. Or if they did, he skillfully batted them away, assuming all the while that he could sort the mess out.

PERSONAL FLAWS

Partly, the collapse of the bank was was down to his own personal flaws. Having built a reputation as a high-flyer, he didn't want his wife, his family or his bosses to find out the extent of his deception. What drove him was the continued belief that he could fix it, along with a healthy dose of bravado and sense of inflated ego – he was only 23 at the time.

"I was head-hunted for Barings, I was their best employee. I was highly accurate, extremely diligent, worked really long hours and progressed rapidly through the organisation.

I wanted to climb the ladder, to be the one making the important decisions. For a period, I was very successful.
"Then I arrived in Singapore and made some very bad decisions, and then froze and didn't deal with them.

"From the first time I put a loss in the five 8s account I expected someone to knock on the door and ask me a sensible question. For three years no one did; not settlements, not the risk office, not the internal auditor. Nobody felt that they had the power to challenge me because I was the star trader. They didn't feel empowered enough to ask the difficult questions.

"The first thought process I had was that I had another day to correct this, that day turned into weeks and into months, and over time, without it being deliberate, I started to feel a certain amount of contempt for the people that were in charge of those controls. To me that meant I had longer and longer to turn things around. The longer it went on the harder it became. I couldn't put my hand up and tell anyone what was going on."

"I've been accused of deliberately defrauding the bank but the truth is I was surviving day by day."

RISK CULTURE

But partly the Barings collapse was thanks to a culture that was, at best, lackadaisical about risk, argues Leeson.

Among the characters caught up in the scandal was a manager who had made himself utterly unapproachable to his staff. No one referred any concerns to him, because they were too afraid to. There was also a significant lack of understanding of the derivatives business.

"Three main things went wrong," explains Leeson. "Disparate technology – systems that didn't talk to each other; exceptionally poor communication and everyone operating in silos; and a management system that didn't understand how the business fitted together.

"I knew what I was doing and I am fully responsible and accountable for what happened. But there are similarities in all financial scandals; poor systems, poor quality of controls, poor people in charge. If people are doing their jobs these events shouldn't occur."

REPUTATIONAL RISK

Are risk managers doing their jobs properly now? Have they learnt from the past? Several CROs gathered at a panel session immediately following Leeson's talk to outline their approach to reputational risk.

Bruce MacLaren, Chief Risk Officer Europe at RBC, explained how the bank had set up a reputation oversight committee, precisely to avoid headline risks. "These oversight committees – and most institutions have them in some form now – take the decision-making away from the transactors. Those who are profiting from the risks they are taking, as per Leeson, have clouded judgement. You have to get transactions up to a higher level," he explained.

In addition, he said, there had to be a certain "tone from the top", so that these things are identified, because "it won't come from those who are profiting from it."

Paul Berry, Chief Risk Officer at Mizuho International described how they had also added new layers of governance with regard to reputational risk, as well as new policies and procedures. They had a "zero risk appetite for reputational risk," he added.

Jacques Beyssade, Deputy Chief Executive Officer In Charge Of Risk, Compliance & Permanent Control at BPCE felt that the ultimate stakeholder was the customer base. They have 30 million customers, half of whom "are really engaged with bank" and 9 million of whom "own shares in the bank".

Alexander Vedyakhin, Senior Vice-President, Chief Risk Officer at Sberbank agreed, adding that what might previously have taken a week to travel round their 130 million customers could now be done in half an hour and as a result of a single tweet. As a consequence they now had a reputational risk committee that can come together at a moment's notice in order to respond.

THE ROLE OF COMPLIANCE VERSUS THE ROLE OF RISK

With all this frenetic activity on the part of the risk function, where did that leave compliance?

MacLaren argued that compliance was just as important but that companies shouldn't rely on them as the sole guardian of reputational risk; "It has to be embedded in the first line," he said.

Vedyakhin said that risk and compliance had to work more closely together despite being strange bedfellows: "They usually come from different backgrounds, half of risk come from business and the other half have strong mathematical skills, and compliance guys come from a legal background." Training was key, he added, as well as, according to Beyssade, making an example of bad behaviour. "When you have identified it, deal with it and don't tolerate it," he said.

Ultimately, the reputational risk isn't going to disappear.

Leeson's fall from grace has since been eclipsed by the likes of Madoff and Jerome Kerviel of Société Général. "I didn't know how catastrophic my actions would be, or how small their capital base was," says Leeson. "It is the most embarrassing period of my life and I'll never get away from it."

"If you find yourself in a situation where you can't cope, do one simple thing, for me, – ask for help."

We spoke to Leeson about whether the industry has changed sufficiently to prevent a case like his from reoccurring.

Disruptive thinking for the risk management industry

Dr. John Lee, Group CRO, Maybank Group

With the digital revolution we are observing today, the world is changing at a much faster rate than before.

Economies and industries are constantly disrupted, with new ways of doing business constantly being written. The financial industry is no different. As a result, the risk landscape has been evolving, with traditional economic risks giving way to more pressing concerns in environmental, geopolitical and societal risks.

Risks are also becoming more interconnected, diverse and complex, making it difficult to contain, predict or potentially manage. This changing landscape has brought about new and emerging risks, and these have driven the need for changes in risk management in financial institutions.

In particular, we see four key trends shaping risk management of financial institutions today, and in the future, and how financial institutions need to react to these trends:

TREND 1: DEEPENING AND WIDER REGULATIONS

Need to build more robust regulatory and stakeholder management capabilities in managing constant changes of regulations.

Ensure financial, non-financial and compliance considerations to be on top of mind prior to formulating any business strategies.

TREND 2: TECHNOLOGY AND ADVANCED ANALYTICS

Innovate and enhance existing risk management analytics by leveraging big data and machine learning capabilities for better and faster risk decisions at lower costs.

TREND 3: CHANGING AND RISING CUSTOMER EXPECTATIONS

Work closely with businesses and operations to provide highly customised solutions to match changing customers' profiles and expectations.

TREND 4: PRESSURE TO OPTIMISE COSTS

Explore cost-savings opportunities via simplification, standardisation, digitisation and automation or leveraging on third parties to perform operational activities, which may also afford opportunities to reduce risk.

Risk management and risk professionals need to adapt to this 'New Normal'. To prepare for this future, risk management needs to focus on the following:

VALUE CREATION

Risk professionals should collaborate more closely with the business and other functions, such as strategic planners, and play a more influencing role in running the financial institution. Traditional focus on portfolio management will need to evolve to shaping the balance sheet and optimising capital.

AGILITY

Risk management needs to become agile and respond faster to the changing world. Being prepared will also be key to ensure we are prepared to face the 'known unknowns' as well as the 'unknown unknowns'.

INTELLIGENCE AND INSIGHTS

It will be important to develop better analytical capabilities and leverage technology to enable us to make more informed and faster decisions.

CAPACITIES AND CAPABILITIES

Risk management also needs to have better intelligence and insights, and hence internal capabilities need to be enhanced. Manual processes should be digitised, specifically core risk, credit and compliance processes. In addition, to start looking into de-biasing decisions, full automation of decisions and processes should be done to minimise manual interventions. The talent pool would also need to be developed to be equipped with superior and strategic capabilities.

CULTURE AND VALUES

Those working in risk management, and those who do not, need to continue to be astrong advocates of corporate values and principles that are key to having a robust risk culture. A strong risk culture across the organisation will help in ensuring risk management becomes part of the daily job of all employees.

The risk management function is already changing and is expected to look decidedly different in the near future. With these evolving roles, it is no surprise that risk management will become the competitive advantage among financial institutions and hence even more invaluable.

RiskMinds 365

FinTech: taking transformation by the horns

We dive into customer-centric innovation via technology transformation with Sonia Wedrychowicz, Managing Director, Head of Singapore CBG Technology.

HOW CAN TECHNOLOGY TRANSFORMATIONS RAMP UP CUSTOMER-CENTRIC INNOVATION?

Technology these days is driving our customers' experience by ensuring simplicity, speed and convenience in daily interactions. The innovative solutions are always implemented having in mind the customer view, as we call it - an "outside- in" view. Technology can only be effective in ramping up the customer experience when it is used in conjunction with reimagining the customer journeys and eliminating all the pain- points that customers experience with the current solutions.

There is a big difference between "digitising" and "digitalising" the customer experience. In the first case it is a reactive activity of making the current analogue experience digital, without really redesigning it and enhancing it using technology.

An example of digitization is transforming a paper statement into a PDF file without really changing anything. You can, however, digitalise the customer statement by making it interactive on the mobile application or through an internet banking. This can be achieved by providing automated categorization of transactions (i.e. show how much we spend on food or petrol), enabling to set up budgets for spending or setting up goals for savings.

WHAT ARE THE KEY TECHNOLOGY TRANSFORMATIONS?

In my opinion, the key technology transformations these days are related to artificial intelligence, Biometric Authentication of customers and authorizations of their transactions and cyber security. The chat bots powered by artificial intelligence will take over a lot of what we call today as "service plus" activities, such as customer requests for blocking and reissuing the credit cards etc., as well as drive the online selling processes.

Biometric customer authentication and transaction authorization will lead to vastly simplifying the account opening process and will make it 100 percent remote and digital. This move will revolutionize the customer onboarding and make the visit to the branch redundant. At the same time, it should lead to the elimination of signatures as customer biometric verification will make it so much more powerful and secure.

Cyber security is viewed by many as the necessary foundation of technology-led transformation and I fully agree with that view. Simplicity should never jeopardize security and therefore the challenges standing ahead of

"Simplicity should never jeopardize security and therefore the challenges standing ahead of making the customer experience secure are immense."

making the customer experience secure are immense. Technology, however, is also driving that by providing multiple points of security that engage not only the core technical solutions, but also involves the customers in monitoring their accounts, for example by providing them with a wide span of different alerts and notifications.

HOW HAS DBS BANK IMPLEMENTED THESE TRANSFORMATIONS WITH SUCCESS?

DBS was a pioneer in the banking industry by implementing many of the solutions mentioned before into our internet and mobile applications. Examples include: the biometric authentication of digibank by DBS customers in India and Indonesia, our Virtual Assistant, which is an AI chat bot servicing customers in India and Indonesia. That Virtual Assistant was recently also implemented on Facebook messenger in Singapore. We also integrated two more FinTech companies' solutions to reimagine the transaction authorizations using soft tokens and the transaction search and categorization, mentioned by me before. Each of our new projects starts with defining so called customers' jobs to be done i.e. understanding what our customers really want to achieve and then designing the customer journeys around it, always using technology solutions.

WHAT ARE THE KEY CHALLENGES THAT DBS BANK HAS ENCOUNTERED WITH THESE TRANSFORMATIONS?

The biggest challenge with any transformation is always related to people. It requires a vast change of the company culture and can only be achieved by engaging employees at every level - from the top and the bottom. In my personal opinion no real transformation can ever be achieved if it does not have a strong buy in and drive from the top management. We were lucky to have a CEO, who was personally dedicated to make the change into digital happen and so was the whole management team under him. Thanks to that support, the transformation happened across the organization and included not only business, operations or technology but it was equally big in the support units like legal, compliance or HR.

HOW IS THE ASIAN FINTECH LANDSCAPE PAVING THE WAY FOR INNOVATION IN FINANCIAL SERVICES?

I believe that Asia is playing an especially important role in the technology transformation - mostly driven by the Chinese giants - like Alibaba with Alipay, WeChat or Ping An. At the same time, Asia is home to a myriad of different Fintech startup companies that provide innovative solutions for the financial institutions to integrate with. Asian regulators are also very supportive in promoting their innovation that is API - enabled and is allowing the startup Fintech companies to smoothly plug into banking and other financial institutions, thus setting the pathway for Open Banking in Asia.


JOIN THE
CONVERSATION
#RISKMINDS