

The banker in 2050

The role of the human in fighting financial crime
for the digital age



1950 to 2050: how will the banker have evolved?

Executive summary

“ Step back to 1950 and banking was driven by pen and paper, and face to face meetings. That’s a world away from today’s connected bank, where there is a wealth of options available to consumers at the touch of a button.

Banking and financial crime are certainly changing fast, with digitisation a key driver for both the institutions and their would-be attackers. Fintech has altered not only customer experience, but also company structure and business behaviour.

I am pleased to introduce this report from the BAE Systems Applied Intelligence team, which examines what the human role will look like in the banking sector of tomorrow.

Many UK customers no longer use a local branch. There were **3,303 closures**, equating to **34 per cent of the network**, between January 2015 and August 2019, according to research from British consumer group Which?¹.

A change in frontline service is just one of the ways in which banking will be differently staffed in the future. This report explores how humans and machines will work together, maximising the potential of both, to shape a sector ready for the challenges and opportunities of tomorrow. ”

Mark Rayner

Head of Consulting, Financial Services,
BAE Systems

¹ <https://www.which.co.uk/money/banking/switching-your-bank/bank-branch-closures-is-your-local-bank-closing-a28n44c8z0h5>

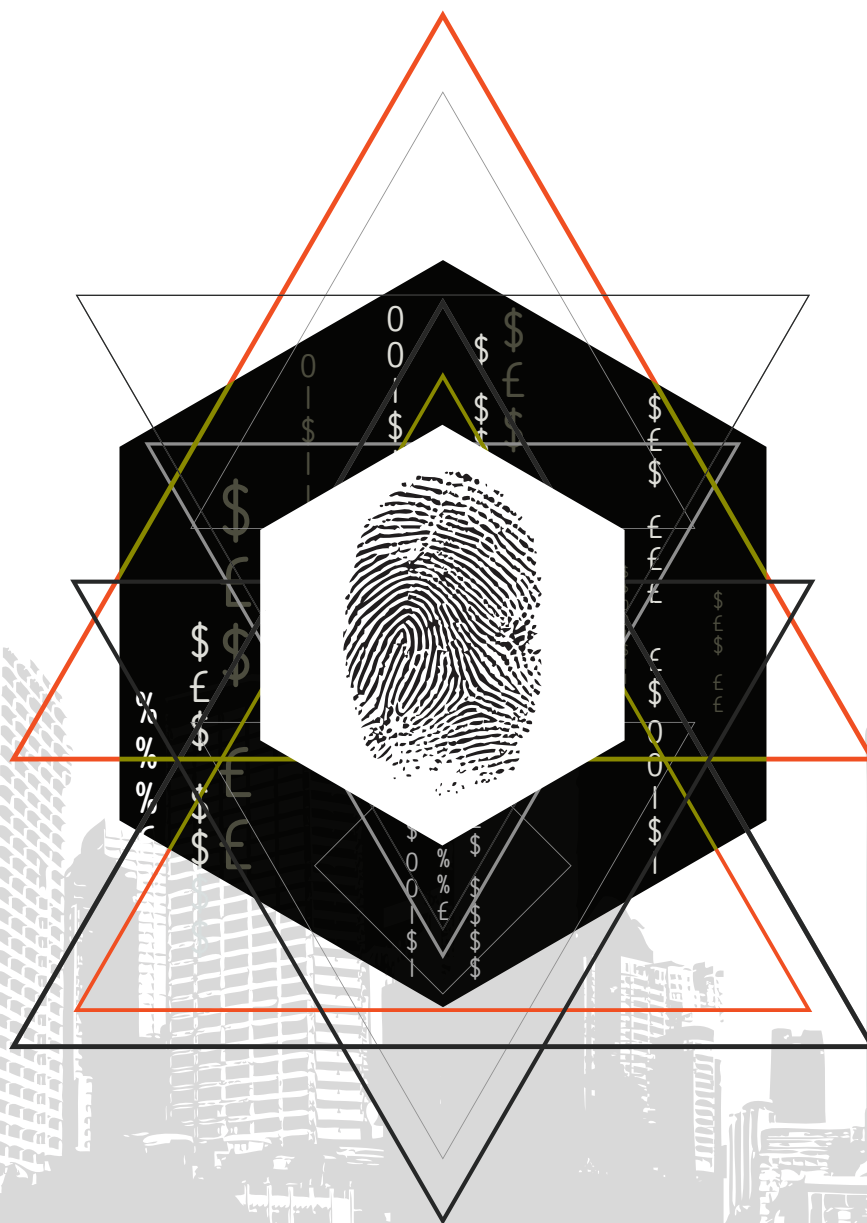


Human touchpoints in the digital age

Technology has impacted how banks forge and nurture relationships with their customers. The human touchpoints have changed, in response to the new technologically-enabled customer experience.

Human touchpoints are now higher up in the value chain. For example, while a mobile device might be used for a simple transaction, many wealth management interactions remain personal.

"Banks will want to expand this high-net-worth individual-driven trade. It is a highly personal approach banks can afford because these services tend to be very profitable," explains Rayner. The move to Open Banking is also having significant impact. "I can envisage a world where a customer doesn't really care who their bank is, as long as the products are performing well, and they are getting a good digital experience," he says.



We need bankers
as well as banks

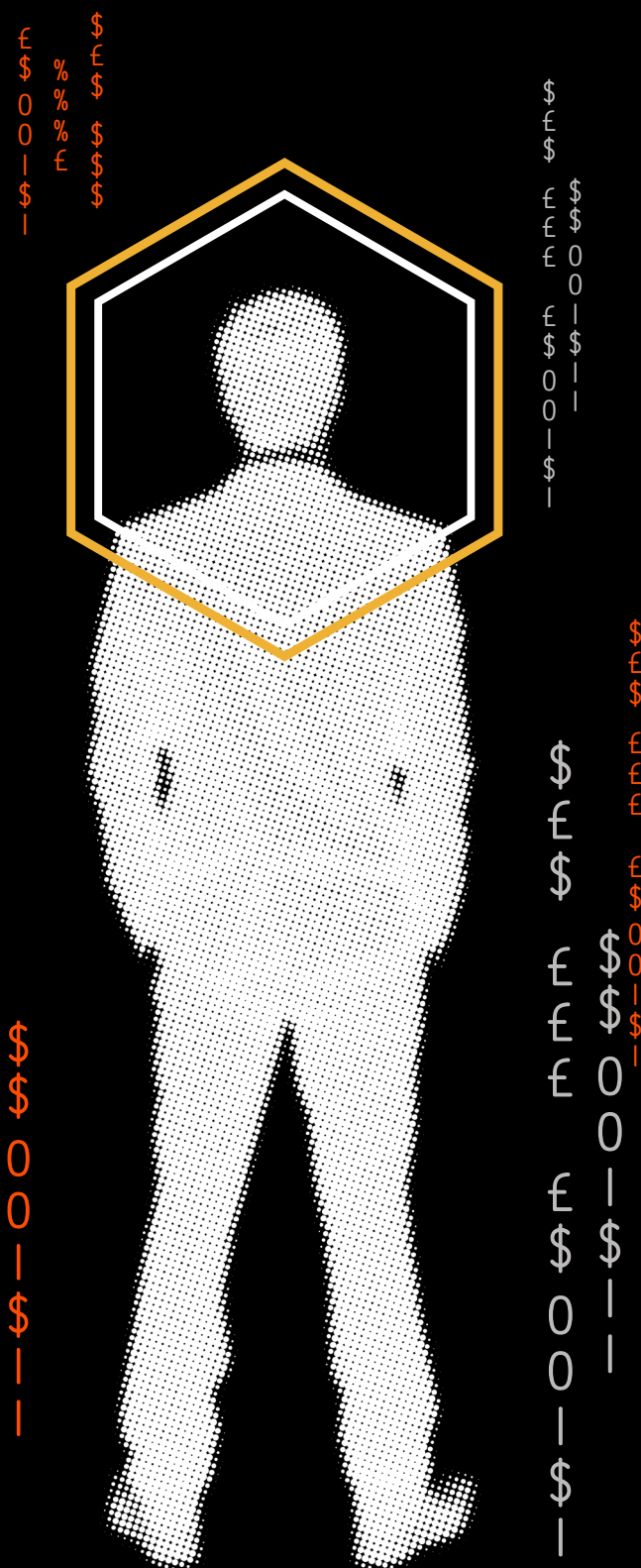
For banks to succeed in this new digital world, they will need to get the balance right when it comes to the role of the human vs the role of technology. Machines may be efficient, but they rely on human personalities and characteristics for their effective operation.

Rob Clifford, Senior Data Strategist at BAE Systems, believes bank employees will need emotional intelligence and curiosity to fully realise the practical applications of technology. "In terms of data protection for example, the human can demonstrate selectivity and discretion in how they approach the sharing of data, as well as in choosing the services they use."

Mark Rayner agrees that the way people use technology is key to maximising its benefits – in the fight against financial crime, as well as in the development of new customer journey models. “Some banks are realising they can use tech to move from a task-based and scripted approach to a more free-flowing, data-driven investigation approach,” he says.

Instead of people simply following steps, we can have people who are much more inquisitive and skilled at interrogating data sets and who are better able to communicate complex ideas.

This process of change, naturally, will present the industry with new challenges and a need for investment in training. "You're going to have people who are working through that transition. Currently the rules of engagement are unclear – there are shifting sands as banks move from one model to another," says Rayner.



Instead of people simply following steps, we can have people who are much more **inquisitive and skilled at interrogating data sets** and who are better able to communicate complex ideas.

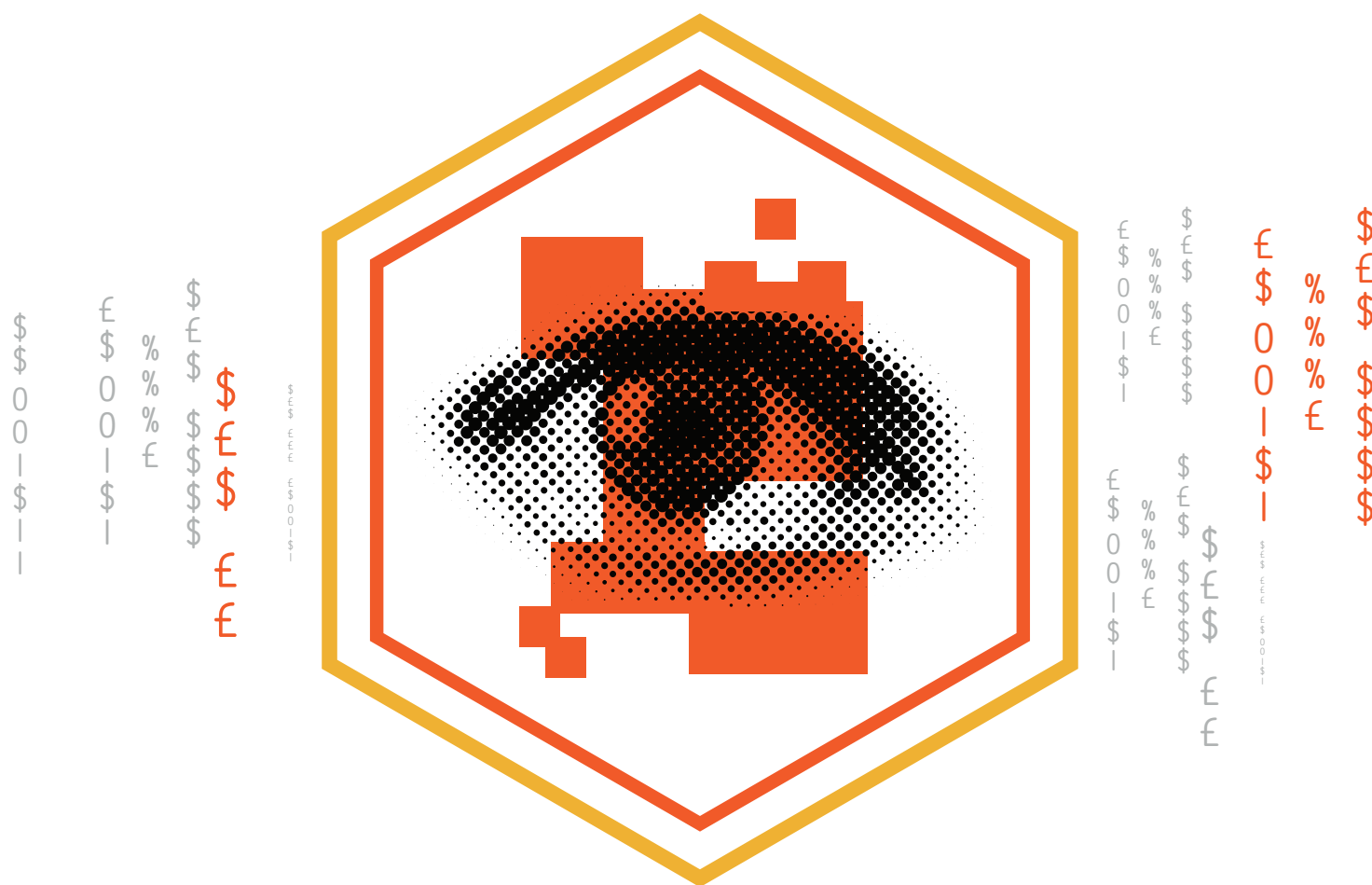
Identifying the skills we will need tomorrow

The way banks react to these skills demands of the future will be crucial to their survival and growth. "Machine learning can improve detection rates and free up the workforce to be more proactive," says Rayner. This may mean changing roles. "Banks might ask, 'can we do it with fewer people or is this actually an opportunity to take a more forward-looking stance, repurpose some of the workforce and improve outputs?'"

Some banks are already taking just such a view. In 2018, HSBC announced that it was recruiting for more than 1,000 digital roles² including user interface designers, product managers, digital software engineers, solution architects, exploratory testers and delivery managers. The bank hired a futurist to identify necessary future roles.

Many intrinsically human and transferable skills will lie behind the banking job titles of tomorrow. Conversational interface designers will need to be creative and strong at teamwork, while partnership gateway enablers (managing relationships between financial partners) will require communication and problem-solving skills.

Although automation will undoubtedly impact bank processes, the human aspect of designing and implementing them will play a leading role in financial success.



² <https://www.finextra.com/newsarticle/32355/hsbc-highlights-the-six-new-banking-careers-of-the-future>

Supporting the workforce

Banks must work out how best to support their employees, ensuring that both existing and new talent is prepared, motivated and productive.

Research from Lancaster University³ has found that the companies most successful at managing the balance between advanced digitally-enabled financial services and the fight against financial crime depend very heavily on people – with a range of skills and expertise – to ensure success.

Lesley Giles is a labour markets and work specialist and an associate of the Work Foundation, which provides advice, consultancy and research on the future of work. She says: "This is a fast paced and dynamic area. It is ever-more crucial that financial businesses are continually developing their workforce to bring in and nurture expertise.

"This calls for investment not only in specialised technical digital areas, but also in broader functional areas to ensure cross-team integrated working. The effective operation of digitalised financial activities and applications involves a complex network of support."

The most successful banks are already making recruitment changes, says Rayner, highlighting the number of roles opening for data scientists. "They have inquisitive brains and they are a valuable resource," he says. Like Giles, Rayner believes that workforce must be looked at in a holistic way. "The data scientists will depend on the work of data engineers – perhaps less exciting, but no less important."

"Data engineer is a role that we have started to see grow in recent years. Building data that is highly resilient is still absolutely key even if it has been overshadowed by other more glamorous roles."

“ Building data that is highly resilient is still absolutely key even if it has been overshadowed by other more glamorous roles. ”

In conjunction with new roles, flexibility in working practices is increasingly important. Agile working continues to grow. Lloyds Bank⁴, a member of the Agile Future Forum, is already robust in its support of agile working practices while HSBC is championing a more modular approach to projects⁵.

Efforts to break down siloed working are also vital to ensuring the full benefit of human skills is employed. The increased convergence of cyber and fincrime work is a case in point. "There's still a real opportunity for the two fields to use a consistent set of processes between them and to share intelligence. I see that as an opportunity for banks to recruit on a hybrid basis," says Rayner.

In these key developments, he observes, challenger banks and fintechs – "with their smaller teams" – can offer valuable lessons.

³ [http://www.research.lancs.ac.uk/portal/en/publications/using-artificial-intelligence-to-enhance-business-operations\(50adf101-6cbd-4407-bb92-031733afe772\)/export.html](http://www.research.lancs.ac.uk/portal/en/publications/using-artificial-intelligence-to-enhance-business-operations(50adf101-6cbd-4407-bb92-031733afe772)/export.html)

⁴ <https://www.lloydsbankinggroup.com/globalassets/careers-archive/new-pdfs/agile-hiring-v2.pdf>

⁵ <https://www.marketingweek.com/hsbc-banks-on-an-agile-insight-approach/>

With AI not against it

Those who do join the banking workforce of the future – and indeed those already in it – will rely increasingly on AI applications. This field of technology offers huge advantages in reducing search times, processing vast amounts of data to inform decisions and delivering accurate results. But the business performance benefit of these optimised results cannot be realised without the close involvement of people.

This encompasses both the design and operation of the applications and the effective use of its outcomes. Giles says: "There is a growing recognition that AI and Enterprise Cognitive Computing (ECC) applications cannot work effectively alone, but that they need to be carefully integrated into the business and require certain conditions and working environments."

The human touch

Creativity, complex problem solving, critical thinking and coordinating with others will be among the top skills requirements of the future, according to the World Economic Forum's Future of Jobs report⁶.



Critical thinking

AI is extraordinary and can do things we never imagined. But critical thinking is its essential counterpoint. Success will come from identifying and training employees with critical thinking skills and placing them accordingly.



Creativity

Many of the processes behind creative thinking are still unexplored and undefined and this is one way in which humans have the edge. Technology can mimic painters and write music, but can it ever show real originality?



Complex problem solving

The ability to handle difficult or unexpected situations and challenges is vital to successful business operations – and is beyond the scope of machines, which can only be taught how to act by humans.



Coordinating with others

AI may well create languages we can't understand and it is starting to transform how we communicate with each other. But our asset as humans is our ability to collaborate and create strong relationships with our customers and peers.

⁶ http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf

Making the technology work for us

Five functional areas of business skill have been identified in research by Lancaster University⁷. These are: technical digital and data science expertise; business domain expertise; enterprise architecture expertise (incorporating workers across a range of departments, such as senior leadership, HR and IT); operational IT expertise; and general digital expertise.

Careful planning and strategic implementation across an institution – in itself down to human judgement and experience – will be needed if workforce changes are to prove fruitful.

Giles says: "The ability to secure the benefits from these areas requires the commitment and backing of senior leaders and managers – in setting out clear strategies, goals and investment plans and through regular corrective action as an integral part of mainstream operations."

There is legitimate concern in some banks about AI's potential to perpetuate bias, but companies are starting to make proactive changes in this area. Google, for example, has removed gendered pronouns from Gmail's Smart Compose function⁸.

Bias in financial services AI, if unchecked, could have enormous implications for customer satisfaction and for business health – but where greater diversity can be achieved, better corporate performance can arguably be anticipated too.

⁷ [http://www.research.lancs.ac.uk/portal/en/publications/using-artificial-intelligence-to-enhance-business-operations\(50adf101-6cbd-4407-bb92-031733afe772\).html](http://www.research.lancs.ac.uk/portal/en/publications/using-artificial-intelligence-to-enhance-business-operations(50adf101-6cbd-4407-bb92-031733afe772).html)

⁸ <https://www.theverge.com/2018/11/27/18114127/google-gmail-smart-compose-ai-gender-bias-pronouns-removed>



Tackling human vulnerability

Human characteristics may be central to banking and the technology that underpins it; they also expose it to attack. Financial criminals continue to exploit such human vulnerability.

Giles believes this will only become more pertinent with technological advances. "As financial crime develops from transaction-based fraud to more identity-based attacks, banks are having to adapt more rapidly to the shifting profile and pace of financial crime.

"Types of crimes and cyber attacks are converging as attackers adapt to the digitisation and automation of financial services with ever-more sophisticated approaches."

Tackling social engineering and insider crime – rooted in personal vulnerability – will remain central to banks' approach to fincrime, requiring them to team their human and tech capabilities to best effect.

Mariola Marzouk, Compliance Product Manager at BAE Systems, points out that some cases of money laundering do have an insider element. "Although rare, in some cases, it can go all the way to the top management. Corrupt insiders know the gaps opened to exploitation.

All tiers of the workforce are open to these criminal approaches, meaning that efforts to identify such vulnerabilities and increase awareness must be robust.

"Everybody should count themselves vulnerable to potential criminal abuse; from tellers, to relationship managers and branch managers," says Marzouk.

Faced with cases of legitimate-seeming clients, business providers or investors – in fact criminals – staff are not always asking the right questions. Marzouk believes banks must offer more and better training to address this, allowing the human investigators, who will remain the next line of defence, to do their work more effectively. "If a report just says, 'He seemed really dodgy. I didn't like some of the responses he provided to my questions,' the investigator who picks up the alert has nothing to go on."

While human characteristics may be central to future banking and the technology that underpins it, they also expose it to attack.

Financial criminals continue to exploit human vulnerability.

Fortifying the frontline

Meanwhile, the criminals are diligently doing their research on the employees and institutions they're out to exploit – opening accounts and disappearing while the compliance team waits for information.

The solution, says Marzouk, is to strengthen defences. "The best way to protect the bank from nefarious criminal tricks is to simply educate employees on how their roles and personal circumstances might be abused. Banks often do this at a high level, but with growing digital societies, the threat needs a wider response."

She points to the 2018 example of Danske Bank, found guilty of passing nearly £180 billion of illegal money from Russia, the UK and the British Virgin Islands through an Estonian branch. "It was reported that when the bank realised the volume of non-resident suspicious activity passing through the branch, employees at the Estonian branch were contacted by Russian-speaking individuals, who refused to state their identities and instead threatened staff".

There is a fine balance to be achieved between increasing regulatory scrutiny and overpowering banks' resources to effectively spot suspicious activities.

A good example of an effective response to crime is to empower law enforcement. "Now, in the UK for example, if a law enforcer suspects something, you have to prove your innocence under the Unexplained Wealth Orders. But so much more needs to be done across the world. It seems there are still way too many things at stake."

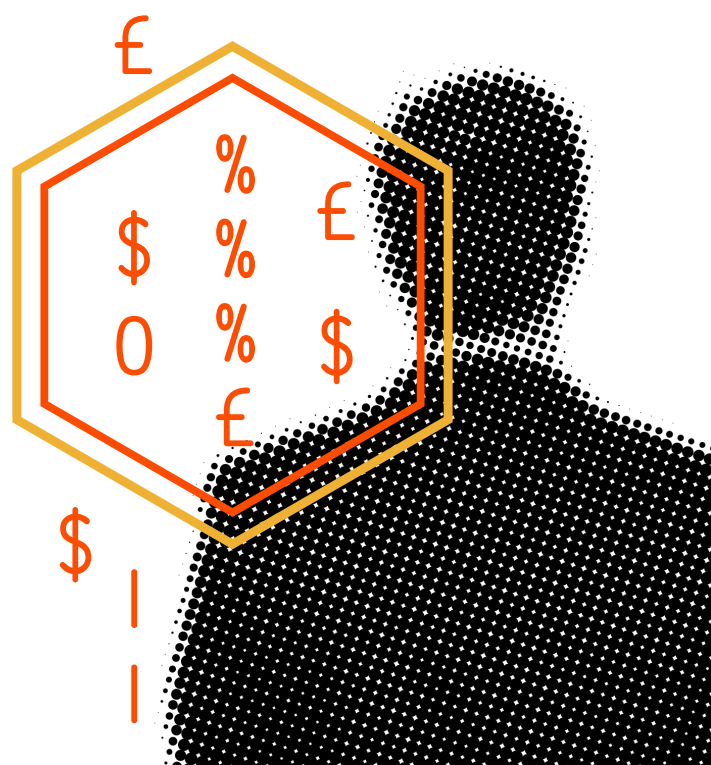
Developing a holistic approach

Clearly then, the people working in banks must be a key consideration in the development of future-proof financial crime strategies. These also need to include robust cyber security awareness, and must actively support business objectives as well as meeting evolving regulatory requirements.

But banks must consider the human aspect of fincrime more widely still – to incorporate the customer and society. In this, says Marzouk, the small size, relative agility and lack of cultural 'baggage' of fintechs, is helpful.

"Whenever I talk to people about how insider crimes happen, they say, 'Surely it's just a few people?' They don't want to hear about it or perhaps to be put in a position where they have to do something about it."

"If you let a bad guy in it's difficult to spot him later, but if your staff's risk awareness is aligned with the company from the start, and they know a good customer is going to make healthy business, than they will also be promoting state-of-the-art due diligence."



Conclusion

Ultimately, as long as humans use (and abuse) the banking system, it will need to be staffed by real people. Even as technology continues to develop extraordinary capabilities, human intelligence will be needed to design, manage and interpret it.

Those banks that see real success in the next digital age will be the ones to exploit the opportunities the shifts in the industry will bring.

This means ensuring its people are equipped with the skills they need to work with the technology, but also to work with each other and with their customers.

Tomorrow's bank will be hi-tech, but it will also be human.

What next?

The balance between human and machine will change in ways we can only begin to imagine. It may be an unsettling environment for employees, as well as a management challenge for those charged with deciding how to procure the right technology and retain the right human talent.



Start positive

When it comes to functions such as compliance, counter fraud and cyber security, automation has already started to positively impact the banking sector. There is a huge potential to increase efficiencies and accuracy. Nonetheless, human investigators' powers of deduction, pattern recognition, intuition and intellect remain at the heart of the job.



Build pragmatic strategies

The application of advanced analytics can benefit many functions, so it's important that organisations strategise effectively based on what they want to achieve. Understanding the business problem, setting objectives, and then building a picture of the human behaviours involved, are crucial steps for establishing an effective way forward.



Plan ahead

Employees will need new skills, and technical and analytical experience may need to be back-filled. Yet the fact remains: banks may not need as many people. Pilot schemes and early technology adoption bring two benefits. Banks start to understand the wider organisational impact of data science and automation, and they gain a competitive edge on tech-cautious competitors. Early and honest communication with staff about the likely impact and opportunities of machine interaction will reap benefits.

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/bankinginsights



[linkedin.com/company/baesystemsai](https://www.linkedin.com/company/baesystemsai)



twitter.com/baesystems_ai

Copyright © BAE Systems plc 2020. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.