Keeping one step ahead

Software that makes networks 'programmable' could be an important weapon in the armoury against cyber attacks and transform the shape of banking, writes ***Ken Wieland***

At the Mobile World Congress in 2015, Francisco González, the chairman of Spanish bank BBVA, told the audience: "BBVA will be a software company in the future." This was not the announcement of a radical change of sector, but of the expectation that software will determine the future shape of banking.

One reason for this expectation is that software is set to change networking itself. Software-defined networking (SDN) is one of the most talked about network technologies, along with network functions virtualisation (NFV). Both mean that banks will no longer be constrained by hardware capabilities. Listen to some telecommunication companies (telcos) and their equipment suppliers, and SDN and NFV are set to change the way financial institutions do business.

A recent report by consultancy Ovum – *Creating the Future Network for the Digital Financial Institution* – concluded that

a move towards software-defined networks is necessary for some compelling reasons. These include the holy grail of cuts in operating costs, but also, the report argues, more sure-footed regulatory compliance and tighter control on security – prospects sure to interest financial services.

More agile networks, it adds, would also facilitate digital services that put banks on a level footing with companies such as Amazon, Google and Netflix, which have revolutionised customer service expectations.

Banks face a new world of digital competition. Open banking, for example, could, in principle, reduce them to utility pipes operating secure payment services while those companies that react quickly with enticing new products take the lion's share

> *"Greater automation can help eliminate security breaches caused by 'fat finger' errors*

of margins. What will save them, in theory at least, is agility. But quickly and securely bringing new products on-stream in an industry that relies on the confidence and trust of its customers, and has to meet stringent regulatory requirements, is a tall order.

"Our customers are focused on cost, agility and risk," says Tony Evans, managing director of global financial services at Juniper Networks, a US network security and performance company. He argues that software-defined networks can tick all three boxes. A cynic might point out that he would say that but it is clear that banks are facing potentially major business upheavals and patching up existing systems is unlikely to be optimal. Daniel Mayo, Ovum's chief analyst on financial services technology, warns that any move towards SDN cannot be done in a piecemeal way. The technology is disruptive and transformative, and requires significant capital expenditure.

This poses an awkward dilemma for financial institutions. How do you reconcile a strong focus on cost control with a network capital expenditure splurge and, probably, a radical internal reorganisation that could open up new security vulnerabilities?

Safety first

The notion of "programming" the data centre or wide area network (WAN) according to certain policies lies at the heart of SDN. "The reason why SDN is so important is because you can have centralised policy control," explains Winston Carrera, chief technology officer of global banking and financial markets at BT Global Services. "Processes can be automated."

How SDN can transform banking

With software-defined networks and data centres, IT administrators can stipulate policies centrally without having to tinker with the underlying network. It is also possible, through the use of "abstraction" – which hides network complexity – to set those policies in non-technical language. Knowledge of the underlying protocols involved in service delivery is not required.

"If I need my mortgage team to have access to certain resources at a particular time of day, I can define that policy in human terms," says Winston Carrera, chief technology officer of global banking and financial markets at BT Global Services.

SDN also opens up the possibility of more flexible telco relationships, something that Carrera seems happy to concede. "An enterprise might want to use BT for a particular cloud service on a particular day, perhaps because we offer the best price, and then use another cloud service on another day," says Carrera. "That policy would be painful to implement if it had to be manually configured."

Combined with network function visualisation (NFV), SDN can also allocate network and data centre resources, as and when they are needed, at branch office sites. Although retail banks are cutting back on physical outlets, Carrera sees a move towards alternative branch strategies.Mini-branches, for example, or highly (or even fully) automated branches in retail centres, or temporary "pop-up" branches to support customer demand at high-traffic events, such as large festivals or sporting events. SDN and NFV gives financial institutions the ability to scale up and down network capacity at these sites – to support videoconferencing calls with mortgage specialists, perhaps – according to demand. ■

In a non-SDN environment, an IT administrator who wants, say, to reserve data centre resources for mission-critical apps at times of peak demand, or to route data traffic across the network in a certain way to fulfil compliance, has to hand-crank each network element involved in the service. That is a laborious and time-consuming process and one prone to "fat finger" mistakes.

SDN not only seems to promise a way out of the silos and ancient operating systems that bedevil some banks, it would cut operating costs through automation and tighten security by reducing the risk of human error. Once the rules are set, the system instantly starts using them. In principle, artificial intelligence (AI) could also be used to implement a self-learning system, making the SDN both robust and reactive.

What might trouble financial companies contemplating a move to software-defined networking, however, is the heavy reliance on the so-called "SDN controller".

The controller is responsible for centralised policy enforcement and, in the words of Carrera, has as an "omnipresent view of what you do". It has access to all databases needed to go about its business of setting and implementing policies.

In an SDN world, if the controller were compromised, it could wreak havoc on a bank's operations. Carrera says no financial institution has had its fingers burnt in this way, not least because telcos do not expose the SDN controller directly to the "outside world". Are telcos and equipment suppliers downplaying the risk?

Patrick Donegan, principal analyst at HardenStance, a cyber security consultancy, thinks not. "The risk of SDN controller compromise is certainly real. But, in fairness, I do think most vendors understand that very well," he says. "For example, Nokia has been working with leading security vendors like Palo Alto Networks and Clavister to drive its SDN security roadmap." Donegan also points out a recent announcement by Juniper Networks to add five new security vendor partners to support its SDN strategy.

He agrees, too, that SDN – through automation and centralised policy-setting – opens up new opportunities to strengthen cyber security: "Let's not forget that it was a 'fat finger' error that caused the massive Amazon Web Services outage a few months ago." (In March, AWS suffered a domino failure of websites it was supporting when an employee who was debugging the billing system made a mistake.)

SDN also allows a more intelligent approach to managing network security. Particular traffic flows deemed higher risk can be shunted into an intrusion detection system – or quarantined – for what is called, in security circles, "deep packet inspection". Lower-risk traffic can be allowed to flow more freely.

Many in the finance sector seem sold on the SDN promise of clever ways to fend off data breaches. In a global SDN/NFV survey of 100 institutions undertaken by Ovum, better security was hailed as one of the main drivers for future adoption.

Some may argue that a non-SDN world can have advantages when it comes to security, since each bank's network will retain its own idiosyncrasies. Outsiders find such networks difficult to navigate, which means intruders can be at a loss. There is, more importantly, also no single point of weakness. SDN proponents will need to address these objections to change if the technology is take root in the banking sector.

SDN collaboration

If financial companies are to gain the full benefits of SDN, and if telcos and their suppliers are to tap successfully into this still nascent market, Donegan advises both camps to work closely together.

"There's still a learning curve to be gone through on the part of both customers and providers," he says. "Some banks may be expecting some security features served up at a faster rate than the industry is able to deliver them. And that's fine – they're pushing the envelope as they should be. SDN also drives the need for change in the internal processes of both the provider and the end customer to derive the available performance and security benefits. The responsibility for closing the gap in alignment lies on both sides."

Although it is still early days for SDN, Mayo says he already sees "some movement" towards software-defined networks in the financial sector. It suggests that longer-term thinking is beginning to make headway. Along with a growing shift towards a hybrid cloud strategy, where banks show a greater willingness to park non-critical applications in the public cloud to reduce costs, Mayo sees SDN as a key ingredient for a leaner and more successful financial services sector. ■

***Ken Wieland** is a freelance telecoms writer with more than 20 years' experience covering the fixed and mobile markets. He is a regular contributor to various trade publications and author of extended reports for The Economist Group*

Time to stage Sister Act

*Ignore Big Brother. **David Birch** argues that banks should take on the role of Little Sister and use their apps to deliver both security and privacy to customers*

George Orwell got it all so wrong. Remember his vision of Big Brother? Some giant government computer system that would put big-screen TVs in all of our living rooms and use some nightmare always-on version of Skype to connect us permanently to the home secretary? It all seems so quaint now, not least because of our considerable post-war experiences of large-scale government IT projects. It would never have worked as the book imagined because it would have been abandoned halfway through, with billions of pounds down the drain (I would not say wasted, of course, because much of it would have gone to consultants), and the call centre would have been outsourced to the Far East so you could dob in your neighbours 24/7.

There are all sorts of things that Orwell did not see – such as chatbots and the internet, laser beams and "reality" TV. But what he got really wrong was the central conception that it would be the government spying on us when, as it has turned out, it does not need to bother because we are spying on each other, all the time.

The police cannot arrest anyone, an airline cannot "deplane" someone, a footballer cannot have a punch-up on a night out, and a member of the House of Lords cannot snort cocaine without someone recording it on their smartphone and posting it all over Snapgram or Facechat, or whatever is in fad at the time.

Everybody is doing it. It is not revolutionary socialism or social media that is the lever disrupting the old order, it is the mobile phone. In a few short years, it has turned into a combination of remote control for the real world and a Swiss army knife for the virtual one. You cannot leave home without it, whereas I regularly leave home without my American Express card (because I have it loaded into my iPhone by ApplePay).

I have, essentially, volunteered to be tracked and traced wherever I go in return for what Sam Lessin, when he was the head of identity at Facebook, memorably told me was a superpower. And he was right. The ability to communicate instantly with anyone else on the planet, to connect with any or all of the information that mankind has to offer, and (soon) my own artificial intelligence, is indeed a superpower. There is no other way to describe it.

The problem for banks is that they are not making much use of their superpowers. Our mobile phones generate a torrent of data that banks could simultaneously use and protect. Not so much Big Brother, more a sort of Little Sister who generally keeps her mouth shut but occasionally blabs to mum and dad

(and the Financial Conduct Authority) if you do something that you should not. She looks after your data, but as data protection regulation becomes ever tighter and more complex so your data, or what I should more properly be calling your personally identifiable information, is turning into a kind of toxic waste that nobody wants to hold. This is precisely why the financial services industry should seize the opportunity to be the Little Sister that delivers both security and privacy to its customers.

Yes, this is a cyber security challenge and it could all go horribly wrong but, as things stand, the way banks use data is not going particularly right. I can illustrate this with three quick stories.

I was in New York and went to an ATM to get some money. The transaction was declined, falling foul of my bank's well-meaning anti-fraud supercomputer. The next day, I was woken at 4am (ie 9am UK time) by the bank's fraud service calling to ask me if I really was in New York. I did not think anything of it at the time because I was too sleepy. When I woke up, I did wonder if the bank app that is on my phone and that I use all the time might have mentioned to the ATM host that I was in the US in general, New York in particular, and at an ATM specifically.

My second story occurred in London. I was walking down the street when I got a call from a service provider. The first question I was asked was something along the lines of "what is your name and the first line of your address?" but I did not answer because it sounded a bit like the Windows Support people who ring me at home all the time.

Instead I asked for a phone number so I could call them back, but they could not give it to me because they were a call centre. So I asked how I could be sure it was them and they could not come up with a suggestion. Yet all the time that this waste of my time and their money was unfurling, their app was on my phone. If the marketing department, the call centre and the mobile app could be linked through some sort of interconnecting network, then when the call centre rings me with a marketing message, the app could pop up on the phone and say "hey, so-and-so is calling now, can you put your thumb on something to prove it's you". Problem solved – mutual authentication that complies with the directive on strong customer authentication.

In the third story, I was in Woking when I called my bank to enquire about a new service. Not to order anything, I just had a question about business bank accounts. As is normal when you phone a bank that you have been with for many years, they first ask you to authenticate yourself using a selection of publicly available information (eg date of birth and mother's maiden name) and then ask you a series of questions to which they already know the answer. In this case, they also asked me something to do with the countries that I have been working in recently. There was no way I could remember all the countries I have worked in over the past few months, but why should I? The bank already knows, since my phone and all the financial applications that I use all the time had been with me.

> *The bank app does not only know who I am and where I am, it also knows what I have been doing*

The bank app does not only know who I am and where I am, it knows what I have been doing. It knows everything about me but does not seem able to do much with this data. But it should. The combination of the bank and the mobile operator really ought to deliver something special. For example, the end of PINs because of continuous passive authentication: software running in the mobile phone that checks how I hold the phone, where I go, what I do, how I type and so on. The next time the bank calls, there should be no question of asking me for my mother's maiden name or my PIN because the phone will already know whether it is me or not.

There is no doubt that cyber attacks are a threat to banks, but they are arguably also an opportunity. Banks are trusted as the repositories of our money and that means we are also likely to trust them to hold, and use, sensitive data. Yes, it is true that other companies may be actively fed with more details of our lives – banks are unlikely to know the cat's name without looking at Facebook – but the data that banks collect are data most of us would probably not broadcast.

If you want to know whether I am over 18, whether I am in the UK or not, whether I have travelled to the US in the past month, whether I have bought anything in Waitrose recently, whether I have children at university, whether I have car insurance or whether I play golf… The bank application on my phone already knows and it can attest to a variety of facts about me (with my consent) while keeping all this information safely locked up back in the bank vault. ■

David Birch *is a director of the secure electronic transactions consultancy, Consult Hyperion, and a visiting lecturer at the University of Surrey. He is an internationally recognised thought leader in digital identity and digital money, one of Wired magazine's top 15 global sources of business information and a research fellow at the CSFI*