GENETEC PERSPECTIVE

Securing your journey to digital change

By Evgenia Ostrovskaya, Business Development Director, Retail and Banking, Genetec Europe

Evgenia Ostrovskaya
Genetec

Retail banking has undergone and continues to undergo a period of profound transformation. Nowhere is this more apparent than in the high street branches themselves, whose layout, function and purpose is now almost unrecognisable from when they were first built. Once seen as the very definition of bureaucracy, they now have the look, feel and levels of customer service more commonly associated with high-level retail.

This is because the vast majority of transactions that previous generations would have conducted at a local branch have now moved online. Why make an unnecessary journey, stand in a queue and speak to a cashier when you can do it faster and more conveniently at home? Self-service was already most people's preference before COVID-19. It certainly will continue to be afterwards, now that we are all being encouraged to keep our physical distance.

Consulting firm Accenture has a particularly good model for how branches must now operate – and it means being a problem solver, digital ambassador and trusted advisor to those who do need to speak face-to-face. Individuals step in-branch because something has gone wrong, or they're less digitally-savvy and need some help, or because they're making a big financial decision and wish to consult an expert. The technology and types of retail estate necessary for meeting these customer needs have evolved rapidly, and as such, security requirements have changed as well.

Recently I was fortunate enough to participate in an online discussion with Daniel Lanecki, former Head of Physical Security for Barclays and moderated by Morten Jorgensen, Head of Consulting at RBR. Outlined below are some of the key takeaways that retail banks should consider when outlining their digital transformation journey and generating the best value from their space – for both customers and employees.

Security infrastructure can be used more widely to help organisations gain a better understanding of their environment

Think beyond security

For any financial institution undergoing a major digital transformation, top-level security – from both a physical and cyber standpoint – is of course a non-negotiable requirement. However, driving through improvements on the scale required to bring about meaningful change necessitates achieving buy-in from stakeholders right across the business, not just within the IT and security teams. It therefore pays dividends to think holistically from day one about the many different ways in which the business can benefit.

A programme setting out solely to improve security is liable to be viewed by others internally as a necessary cost that needs to be minimised. Yet a programme that demonstrates it can simultaneously enhance security, streamline operations and provide new levels of insight to the business is something for which the C-level can get excited about investing.

Reaching out early on to other stakeholders in the business and establishing how the programme can help to address some of their key challenges make it much easier to build a business case that adds sufficient value. Furthermore, this approach potentially brings additional funding and even senior executive sponsorship into play. Thus it can be the means to push through a programme of greater ambition and scale than would otherwise have been feasible, the possibility of which should allay concerns that such a strategy could dilute the focus on security.

There are many examples of how security infrastructure is being used more widely to help organisations gain a better understanding of their environment. For example, video analytics can be used to help managers understand how many people are in a particular branch at any one time, give accurate estimates of queueing times and ensure compliance with physical distancing regulations. Other parts of the business can use heat maps to see how floor space is currently being used and to highlight ways in which it could be optimised. And coming back to security operations, loitering

detection can be put in place near ATMs to alert the guard when there is something that may need investigating, and access control systems can be used to streamline visitor management.

These are just some of the ways a unified approach can underpin improved security and operations. Furthermore, provided the right decisions are made with regard to technology and deployment, it is possible to do all of the above without engendering privacy issues.

Data silos are the Ice Age

The panel unanimously agreed from past experience that for those going through a digital transformation project, the first step was to get an accurate overview of the network and all devices that are connected to it. Banks need to understand where data silos exist, what vulnerabilities can be created when networking them and how these can be eliminated.

For any large financial institution, gaining a unified view of the whole security infrastructure and everything that connects to it may initially seem expensive, especially when considering the older yet critically important legacy systems that are likely to be included. However, when the true time and monetary costs involved in independently managing and maintaining disparate systems are correctly factored in, it quickly becomes apparent that the benefits of a unified view massively outweigh the costs of achieving it.

Operating in silos is inefficient, costly and makes it impossible to fully utilise the potential of the latest technologies. To illustrate this, we can look at video surveillance systems, where it is not uncommon for large organisations to find that almost seven out of ten cameras on the network are running on out-of-date firmware, creating significant and entirely avoidable security vulnerabilities. Regularly and consistently conducting basic cyber security hygiene, such as installing the latest security updates, is simple when it can be done remotely from a central location and with full visibility of what is running on the network. However, it is all but impossible to carry out locally, across multiple locations and with a fragmented view of the task at hand. Of course, in reality this applies far more widely than to just security cameras. The benefits of unification therefore increase exponentially when we widen our view to incorporate other systems, such as access control, intrusion alarms, intercoms and others.

Take a cloud-first approach

Our panel advised that achieving the requisite levels of security and connectivity could only be achieved by taking a cloud-first approach. That's not to say every system and process must immediately be moved over to the cloud. It does still make sense to run some systems and applications on-premises, especially where the existing hardware is already paid for and meeting expectations. However, the overall strategy should be towards cloud-based solutions.

Cloud computing providers can already deliver levels of uptime, security and performance several times higher than what can be achieved in-house. In the vast majority of cases, they can do so at a much lower total cost of ownership, and this cost differential will only continue to tip in their favour over the coming years. To sceptics this may sound outlandish, but in truth this is nothing new. Computing power is becoming a utility in just the same way that electricity did more than 100 years before. It is now a given that power is generated centrally and that we purchase it in the volume we require from our supplier of choice. Yet there was once a time when large factories produced it locally on-site.

Adopting a cloud-first strategy provides banks with a global view into their security infrastructure and operations, thereby acting as a solid platform upon which to deliver further business improvements. This enables the streamlining of day-to-day operations, enhances resilience and ensures that should an incident occur, organisations can respond faster, with a greater level of insight and intelligence.

But what does the future hold?

High streets and commercial real estate are both experiencing a period of massive and likely irreversible change. We don't know the exact make-up of offices, branches and ATMs that will be most optimal going forward, especially in light of social distancing requirements. However, one thing is for sure – existing security infrastructure, especially those operating in the cloud, can help banks comply with these measures. Office space can be laid out based on security-driven insights. From data on crowd hot-spots through to occupancy management, video management systems can play a big role in helping organisations agree on a successful and safe layout. Supported by the benefits of a cloud-first approach, financial institutions can make better informed decisions, driven by a more holistic and real-time view of operations. ■

Operating in silos is inefficient, costly and makes it impossible to fully utilise the potential of the latest technologies

Cloud computing providers can already deliver levels of uptime, security and performance several times higher than what can be achieved in-house