
0.00
0005 -4,85%
0003 -18,04%
0001 -50,00%
0003 14,29%
0005 -12,50%

AHEAD OF THE CURVE?

SEEN BY MANY AS AHEAD OF THE TECHNOLOGICAL CURVE, THE FINANCE INDUSTRY STILL FACES IMMENSE IT CHALLENGES – NOT LEAST WHEN IT COMES TO SECURITY

BY TOM PAYE

Solling: Banks are some of the most targeted organisations for attacks.

Finesse's Paul: Finance organisations here tend to be more agile than those in other markets.

The finance industry has a reputation has being ahead of the curve when it comes to IT. Whether it's new algorithms designed to take trading to new speeds, or the latest security solution designed to provide the utmost protection from criminals, finance organisations are well aware of the benefits that IT can bring. In the Middle East, things are no different, but there are still challenges that finance organisations face.

Indeed, financial institutions in the Middle East are finding it particularly difficult to keep up with the rapid digital transformation and change of the industry landscape. According to Yasser Zeineldin, CEO at eHosting DataFort, digitisation has become imperative for financial firms in order to compete in today's changing market. Unfortunately, many of these organisations have legacy systems with data stored in different silos.

"Hence, a number of organisations are looking at moving their data from in house legacy systems to more adaptable platforms such as the cloud," he explains.

"THE FINANCIAL INDUSTRY IS PROBABLY ONE OF THE MOST TARGETED AS THEY ARE PROTECTING WHAT CRIMINALS ARE NORMALLY AFTER — MONEY AND WEALTH!"

NICOLAI SOLLING, DIRECTOR OF TECHNOLOGY SERVICES AT HELP AG

Indeed, according to many, while banks and finance institutions are seen as ahead of the curve when it comes to IT, the fact is that the majority of them are no longer young companies. This means that, like any other large, old company, there are legacy challenges to contend with, and these challenges are made more pressing by the fact that the industry demands staying technologically advanced. To counteract this, banks and finance firms are investing heavily in next-generation architectures that take advantage of so-called third-platform technologies.

"To keep up with business growth, there is an increased focus on 'simplifying IT', thereby laying the foundation for private cloud deployments," explains Hidir Mag, MEA systems leader at Oracle. "Transforming data centres to deliver private cloud services to run 24-7, non-disruptive business operations is a key factor for organisations to stay competitive in the market place."

That said, while many banking organisations in the Middle East are now relatively mature, with plenty of legacy IT to contend with, there is an argument that they're in better shape to implement new changes than international finance houses. According to Sunil Paul, co-founder and COO at Finesse Global, this is down to the fact that, comparatively speaking, banks and finance institutions are smaller here than in other markets — meaning they can turn things around more quickly.

"Since the size of the institutions in the region is much smaller compared to many parts of the world, the operating dynamics are obviously different. However, this should be considered as an advantage for a quick turnaround as the industry is going through a rapid transformation," he says.

According to Biswajeet Mahapatra, research director at Gartner, it's true that there's pressure for finance institutions in the Gulf to stay ahead of the game. He also largely agrees that this will only be possible through adopting new technologies. He

"A BANK CAN BE FULLY COMPLIANT AND STILL HAVE ITS SECURITY BREACHED. WHAT IS POTENTIALLY MORE COSTLY IS THE EFFECT ON A BANK'S REPUTATION OVER TIME, AS WELL AS POTENTIAL CUSTOMER ATTRITION."

HADI JAAFARAWI, MANAGING DIRECTOR AT QUALYS MIDDLE EAST

points to some of the big areas of interest that the sector is currently looking at.

"The banking, finance and insurance industries have always been challenged to be ahead of the game globally. So is the case in Middle East. As business grows, with Expo 2020 and the FIFA World Cup coming up, more diversification is happening in the industry and there's an increase in demand for newer offerings from customers. Financial institutions in this region have to adopt new technology," he explains.

"Core banking is seeing some refresh, implementation of new HR and payroll systems is happening, new ERP solutions are also being purchased, and investment is happening in AML solutions. A lot of money is being spent on the back end, which includes upgrading the existing data centre, buying DRM solutions, and upgrading storage systems. Of course, this is apart from some investments in big data analytics, smartphone banking, and Islamic banking products."

The question of security

The other major challenge is security. It's common knowledge that most cyber-criminals — unless they are hacktivists promoting a cause — are after money, plain and simple. This turns banks into prime targets for cyber-criminals, meaning that finance institutions need to think carefully about their security strategies.

"Like anywhere else in the world, the financial sector is currently faced with a cataclysmic challenge on how to deal with cyber-criminals. The financial industry is probably one of the most targeted as they are protecting what criminals are normally after — money and wealth!" explains Nicolai Solling, director of Technology Services at Help AG.

"As financial processes are more and more supported by IT processes, these systems are under attack. For the Middle East, the issue is even more challenging as the banks are navigating a very diverse customer base, with different acceptance levels of security. To some extent, you can say that the behaviour of the clients is also a risk that the banks needs to think about."

Indeed, while Gartner says there is no data to support the claim, it's generally accepted that banking and finance firms spend more on security products than organisations which do not deal with monetary transactions and private data, says Mahapatra. He adds that confusing messaging from vendors are changing regulatory requirements are not helping the matter.

"No bank anywhere can say they are not worried about it [security]. The problem in this region is the lack of understanding of the regional requirements by the vendors and service providers and then selling the right solution. Everybody wants to sell anything and everything which is sold in other parts of the world as is into this region, which complicates the matter. Confusions around the changing regulatory needs and how much security is enough also creates a fear psychosis amongst the IT leaders in financial institutions in this region," he says.

Jaafarawi, of Qualys, says that banks need to think beyond meeting regulatory requirements.

"SINCE THE SIZE OF THE INSTITUTIONS IN THE REGION IS MUCH SMALLER COMPARED TO MANY PARTS OF THE WORLD, THE OPERATING DYNAMICS ARE OBVIOUSLY DIFFERENT. HOWEVER, THIS SHOULD BE CONSIDERED AS AN ADVANTAGE FOR A QUICK TURNAROUND AS THE INDUSTRY IS GOING THROUGH A RAPID TRANSFORMATION."

SUNIL PAUL, CO-FOUNDER AND COO AT FINESSE GLOBAL

Indeed, according to Finesse's Paul, banks and finance houses in the Middle East face significant hurdles when it comes to security, not least because there are a host of new threats out there which demand innovative methods of protection.

"The region has to do a lot to enhance their security, vigilance and to create a stronger policy with an effective approach. Most banks in the region are yet to implement systems for real-time fraud management system across channels. Also, banks in the UAE should immediately ensure to comply with the NESA regulations introduced by the UAE," he says.

Because of this, it's becoming clear that finance institutions in the Middle East are being forced into spending larger chunks of their IT budgets on security and compliance. The rationale for security is simple — without customers' trust that their assets are being securely taken care of, the bank will begin bleeding customers, particularly in such a highly competitive market. And without being compliant, well, they wouldn't be allowed to conduct business in the first place. However, the two are assuredly linked.

"Financial institutions do commit a large portion of their budgets to security, and the level of spend dedicated to IT security is increasing over time. The biggest commitment is to maintain compliance with industry regulations, but also to improve the overall business strategy for the banks involved. This investment is necessary as it keeps customer investments and accounts secure and contributes to the brand reputation that the bank has as well," explains Hadi Jaafarawi, managing director at Qualys Middle East.

"It's also worth bearing in mind that the impact of a hack or successful attack on a bank goes beyond any cost imposed due to compliance or regulation issues. A bank can be fully compliant and still have its security breached. What is potentially more costly is the effect on a bank's reputation over time, as well as potential customer attrition."

What's worrying is that all the attention being paid to security may not even be enough. Indeed earlier this year, two major reported incidents worked as evidence to suggest that the cybercriminals are much further ahead of the curve than their victims might believe. In July, it was reported that several UAE banks were hit by a co-ordinated DDoS attack, crippling e-banking operations and websites, and leaving institutions fearing further assaults.

Help AG, which played a central role in the clean-up for one of the victims, told *Arabian Computer News* at the time that the DDoS attack, which has been linked to cyber cabal Anonymous, happened on the last day of the month as the attackers sought to wreak maximum disruption during the banks' busiest period. Help AG cited "sources in the market" who reported "widespread" incidents in the UAE financial sector. And according to Help AG's Solling, there is little to suggest that this will be the last major incident.

"The dark side of information security is believed to be much bigger than the side companies like Help AG is on. Meaning there is more economic buying power in attacking organisations then there is in protecting them. As long as this is the case, we will have the issue that the bad guys will be successful while customers fail to protect themselves," he says. ■

FINANCE'S 5 BIG CHALLENGES

According to Biswajeet Mahapatra, research director at Gartner, there are five main challenges that finance organisations in the Midlde East face.

1. **Technology Obsolescence:** Most are running applications, data centres, and hardware which are getting obsolete and outdated. They need to be refreshed fast. But with an ever-changing environment, financial institutions are confused as to what they should opt for.
2. **Too much focus on 'systems of record':** This is as opposed to focusing on 'systems of innovation'. This will have a long-term impact.
3. **Regulatory issues:** Where to invest so as to satisfy the current and newer regulatory and compliance issues.
4. **Security:** Banks are getting paranoid (and rightly so) about security. They want to understand which technology, processes, and methods are best for them in the current scenario.
5. **New initiatives:** This includes initiatives like mobile banking and smart banking. How should they be going about implementing these — what are the challenges, and what solutions are available in the market?