FStech

BLACKDUCK®

The race to digital: How FSIs are leveraging DevSecOps to meet rising digital demand

Roundtable Special

BLACKDUCK®

The race to digital: How FSIs are leveraging DevSecOps to meet rising digital demand

Senior leaders from across financial services gathered for a virtual roundtable to discuss how they are using DevSecOps and other practices to drive digital transformation in an increasingly security-concious world.

With customers leading increasingly digital lifestyles, financial institutions are under intense pressure to develop, test and rollout new products and services at pace – or risk losing their market share and top talent to more agile competitors.

But as the speed of digital transformation accelerates, many FSIs are finding that this process, alongside industry-wide shifts to cloud-based architecture, are being held back by decades of legacy IT infrastructure and a raft of new compliance and security challenges in a changing risk landscape.

Even when the migration to more modern systems and digital platforms is underway, teams are increasingly finding that an increased attack surface can open up a Pandora's box of cybersecurity issues.

To tackle this dilemma, some are exploring a DevSecOps approach. But while 'security by design' would appear a simple concept, the reality of integrating it into systems, processes and development lifecycles – and bringing staff and senior leaders along for the journey - can prove far more complex.

At a virtual roundtable hosted by FStech and security solutions provider Black Duck, industry peers focused on the use of DevSecOps to drive digital transformation, while keeping systems, customers, and the company's bottom line secure.

The discussion began with a question about how digital transformation strategies have changed in the past 12 months.

"I suppose I've been fortunate enough that our organisation started from scratch; so, I haven't had to worry about legacy issues really," said the CISO of a UK money transfer company. "It's more having a mindset to prevent them from occurring, so being proactive in terms of understanding not only how something's going to be running for the next couple of years, but where we want to be in a decade."

A guest specialising in infrastructure and engineering at a UK bank said that digital transformation had changed a lot in the past year.

"I think the pandemic has meant that we've had to step up here quite significantly to help our customers and move quicker," he said. "Some of the things that we've had to do in the last 12 months just wouldn't have been possible with the traditional and legacy infrastructure that we had."

A senior leader working in finance and risk innovation at a large British bank said that the organisation is at the 18-month point of a four-year transformation plan.

"For me, being in innovation, this has been pushed more to the forefront, whereas maybe in the past it's been more of a closed room, with people sort of hiding away and doing something that everybody else doesn't know about," he explained.

A senior cyber security manager at a retail and commercial bank said that because his organisation has been around 150 years, there is a lot of legacy infrastructure and systems.

"We started a change about 10 years ago to upgrade an awful lot of systems and move to a new digital world as well," he added.

The bank has since reduced the number of branches to 65, revamped its online presence and introduced a mobile app.

"For the last year I've been dedicated to the initiation of products within our security domain. Obviously as a big bank with thousands and thousands of developers, who are using automatic security testing tools for a variety of different purposes, there are a number of different challenges that we face," said a chief product owner working in the advanced analytics division at a large Dutch bank.

The senior leader said that he is currently exploring to what extent these challenges can be addressed with the use of machine learning.

"Our corporate IT environment benefited security wise from the crisis in terms of our digital transformation aspirations," said the group CISO for a FinTech operating globally in emerging markets. "But in addition to that, because we're quite an agile organisation as it is, DevOps has always been part of how we engineer our products."

One senior leader from a Swiss bank said that being a larger financial organisation, there are legacy issues.

"The one thing that I have noticed is that we're working with a lot more vendors in terms of providing clients with better access to information in a digital manner," she said.

An engineering lead from a large UK banking group, currently working within the fraud and authentication lab, said that the biggest change

he'd seen is the increased focus on moving towards the cloud.

Senior leaders at the event then explored what the key challenges have been when it comes to security, particularly given the changing cyber risk landscape.

"It's a combination of tools, data, information and processes and people," said Ian Ashworth, security consultant at Black Duck. "It's the architects, it's the designers and the developers; it's the risk governance, the legal teams and the security teams of course."

He added: "That challenge really is the equilibrium to keep the business wheels turning at the desired speed. But not to put too many of these restrictions and practices in place, which would destabilise that."

A senior cyber security manager at a UK bank said that the organisation has faced cyber security risk challenges from suppliers.

"We've had a number of our suppliers being hit by ransomware attacks. So we've had to close down connections in case that spreads to us, that's been a real challenge over the last couple of years from those," he said.

One senior leader said that his organisation had turned up the dial on security when it comes to the cloud.

"It even influences some of the cloud providers to enhance or change their security for some of our requirements," he explained. "However, we have this pretty broad spectrum of third party, or software as a service that we're using. They've got to actually align to the same requirements that we might want."

A cyber security director at a leading Swiss investment bank said that like most organisations, the shift left approach has meant that a lot of the responsibility and even some of the accountability for cyber risk has

been spread across the organisation.

"I think the biggest challenge for most organisations is changing the internal mindset," he said. "Before you very much had infrastructure and applications, those boundaries were very clear from a security point of view. Now they're becoming very much merged."

Next the group spoke about some of the main roadblocks for established providers in keeping up with digital disruptors.

A cloud services leader from a well-known British bank said that one thing he has noticed while working with the big cloud providers is that their pace of innovation is incredible.

"It's trying to keep up with the amount of releases and new products and services that they provide," he said. "The other one is with the huge volume of FinTechs as well, so part of the role of the transport and infrastructure people is to try to at least filter out the ones that we think would really best suit us."

Cyber security expert at a large European bank said that existing services are as important as new ones.

"The frequency of change of potential security configurations of these services in the cloud has changed a lot," he said.

"I mean initially for a lot of on prem infrastructure, security changes or configuration changes were probably once a year. Now what we're seeing is the cloud providers doing updates to their security configuration every month or every two months."

Senior leaders then discussed how important DevSecOps are to financial institutions and their security posture.

"Whether it's DevSecOps or just DevOps, it's about understanding what's there first in terms of delivery," said the chief information security officer at a UK money transfer service business.

One guest who heads up innovation delivery and cloud services at a leading UK bank, said that the organisation started off with a really simple mantra: 'you build it, you own it.'

"Although that does work in a certain way, in that you know if you build it, you don't hand it over to somebody else later on, and you're building the next thing," he said. "You're responsible for the operations and for the application security at least, that's been great to a degree when you're at the scoping stage."

A senior cyber security consultancy manager at a retail and commercial bank said that the organisation is fairly new to DevSecOps.

"But we've started to deploy containers for the code where applications are built in a sort of waterflow approach," he said.

A director of infrastructure and engineering at a leading UK bank said that the company had been doing DevOps for quite a while in certain parts of the business with inconsistent results.

"I think we've probably got some growing pains of expanding that out," he said.

Frank Morris, managing director for the EMEA region at Black Duck, gave the example of Google carrying out 500 million daily tests inside its systems to demonstrate how complex security is these days.

"It really just does open up the importance of making sure that you've got security embedded in the entire lifecycle of everything that you do," said Morris. "The most important thing is understanding your picture today and then building out where you want to be tomorrow."

Black Duck's Ian Ashworth said that the shift left mantra is brought onto the shoulders of those who are developing.

"They're already having a hard enough

time in being able to run fast, just to keep up with the demand," said Ashworth. "Especially when you move into the digital world."

The guests then explored how the shift to cloud has impacted financial institutions' risk management and security strategies.

"The clear boundaries between application infrastructure are now very blurred, therefore it takes a lot more collaboration," said the cyber security director of a Swiss bank.

A cyber security consultancy manager at a British bank said that the risk for his organisation is going into the cloud.

"We know they're very robust platforms," he said. "Where our concerns lie is what the providers to us then build on top of that, how they securely configure them."

A cloud services lead at a large UK bank said that when the organisation had direct cloud, people were much more comfortable because they controlled everything.

"When you're working with suppliers and third parties and FinTechs for example, and they're using their own environments, you're actually having to spend a lot more time and focus on their security designs," he said.

A CISO from a UK FinTech said that it doesn't matter whether it's traditional infrastructure or cloud-based.

"There is such a disconnect between what the risks are on the ground and how they're portrayed to senior management," he explained.

Next, the group discussed strategies for securing board buy-in for digital transformation.

"I don't think we recognised that many of our board members would find some of the terminology quite difficult and didn't really get it," said the director of infrastructure and engineering at a British bank. "We consciously did numerous teaching sessions on a one-to-one basis at that board level; I think that that was a double-edged sword in many ways."

Black Duck's Frank Morris said that one important thing is being able to justify

the value of what you are doing, which is particularly tricky with security.

"So normally when you're presenting to try and get that buy-in they're looking for a return on investment, which is always more challenging in the security space," said Morris. "I'm sure you're all familiar with it but turning everything into some form of risk improvement or risk mitigation strategy is absolutely key to getting that board sponsorship."

The head of risk governance at a large insurance company said that he could offer a different perspective, being a member of the board himself.

"I experience sometimes that we struggle a bit to get the buy-in the other way round," he said. "That buy-in from the organisation as a whole – because maybe there is some legacy in the organisation that they can't easily overcome."

Black Duck's Ian Ashworth concluded the discussion with a reflection on strategies for striking the right balance.

"It's always going to be a combination of getting the right technology process, information, data and people," said Ashworth. "Education and awareness is the foundation to empower your staff and to draw attention to these types of risk, their impacts and suggesting the best ways of how to deal with them."