Deloitte.

Tech Trends 2021

Four essential trends for the banking industry

How can banks thrive in a digital society?

Four essential tech trends for the banking industry

While banks are grappling with legacy systems and regulatory pressure, lean and agile fintech start-ups are honing in on their customers. How can banks introduce futureproof technologies and processes to keep up with their competitors? The series 'Technology trends for banks' explores four technology trends that are essential for banks to thrive in a digital society.

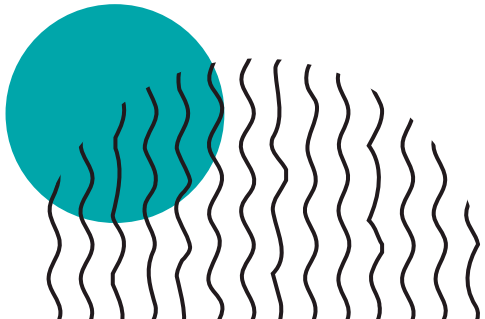
Incumbents vs. disruptors

For decades, banks were frontrunners in automation. But now, large parts of their once cutting-edge technologies have turned into legacy systems that hinder innovation. "New players in the financial services industry, such as Adyen, Mollie, Klarna and Revolut, enter the market without the burden of outdated technologies," explains René Theunissen, partner at Deloitte Consulting and focuses on enterprise technology for banking. "Traditional banks are struggling to keep up with start-ups that optimally profit from new data-driven technologies such as cloud, artificial intelligence (AI) and Machine Learning (ML), as well as lean and agile processes such as DevOps."

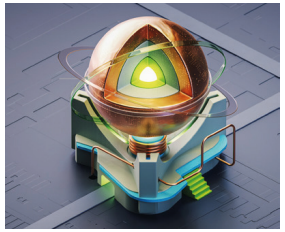
A lot of banks try to copy the way fintech start-ups work. Yet this should not be the only focus of their innovation efforts, says Timo Span, partner at Deloitte Consulting, who specialises in IT banking. "You can't ignore the core. You need to find a balance in revitalising core enterprise technologies that often work with legacy systems, and introducing new data-driven technologies, processes and products." Whereas disruptors can operate quickly and flexibly, Span emphasises that incumbents have the advantage of scale, experience and loads of (historic) data that can provide a deep understanding of their clients and their needs.

Four essential tech trends

So how can banks find this balance in revitalising their core systems and creating new products and services to become truly data-driven? In short, how can banks thrive in a digital society? Deloitte's annual *Tech Trends* report explores the landscape of emerging technologies and seeks to understand their impact on business strategy. Four of these technology trends are essential for the banking industry. This article briefly introduces these trends, while subsequent articles in this series will provide more in-depth explorations of each one.

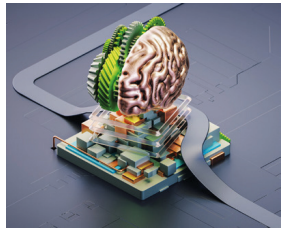


1. Core revival



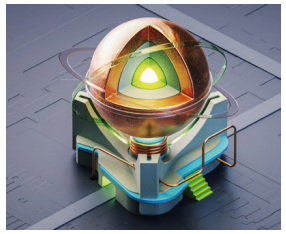
Modernising legacy enterprise systems and (partly) migrating them to the cloud is crucial to unleash a bank's digital potential. As Span states: "You can't ignore the core." A lot of banks have focused on new initiatives outside their core systems, but this is not a viable strategy for the long run, says Span. "At some point, you need to reconnect these initiatives to your core systems," he explains. "Moreover, you need to maintain your core systems and develop innovative approaches for extracting more value from legacy core assets." Revitalising core systems is a massive task, but the good news is that tools to support this process have become more easily available, user-friendly and cost-efficient in the past few years.

2. MLOps: industrialised AI



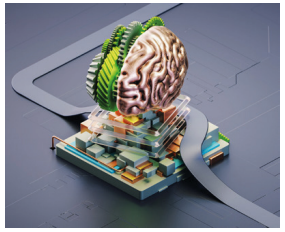
Banks have been relying on data-analytics for a long time, but with ML technologies they can radically step up their game. ML models enable a shift towards near-real time processing of data, that can help organisations efficiently discover patterns, reveal anomalies, generate insights, make predictions and move towards automated decision-making. If you aim to make ML a key driver of the company's performance, you need to alter your operations as well. This can be done with MLOps: the application of DevOps tools and approaches to industrialise and scale ML. "Several banks have already developed promising proof-of-concepts of MLOps," says Theunissen. "In the next few years, we expect MLOps to become a standard practice and an important driver for change in the banking industry."

3. Machine data revolution: feeding the machine



Legacy data systems are typically siloed and designed to support human decision-making. With the rise of new data-driven technologies such as cloud, AI and ML, organisations are working on a future in which data is easily available across all divisions. "Several banks are taking steps to disrupt the data management value chain from end to end," says Theunissen. "They are using new data capture and distributed data architecture capabilities, advanced analytics and next-generation cloud-based data stores. In the end, this will enable them to connect the dots and make real-time, at-scale, automated decisions which will radically speed up their primary processes."

4. Zero trust: never trust, always verify



The last essential technology trend for banks is related to cybersecurity. "Cyberattacks are becoming both more frequent and more sophisticated," says Span. "This requires banks to beef up their security measures." The concept of 'zero trust' assumes that no user, workload, device or network can be inherently trusted. Every access request should be validated on all available data points, including user identity, device, location and other variables. A zero-trust architecture should be part of every modern enterprise environment, says Span. "For banks in particular, their customers' trust is the most valuable asset," he explains. "This trust can only be effectively safeguarded with a zero-trust security approach."

The way forward

These four technology trends are crucial for banks to move forward in the digital age. But in Span's opinion, implementing them requires significant effort on the level of technology, process and organisation. "Banks are huge, complex organisations that play an essential role in our society," he explains. "They have to deal with legacy systems and they operate in a tightly regulated environment. Reviving your core systems, introducing AI – and ML-driven technologies and processes, and implementing an up-to-date, zero-trust cybersecurity architecture all entail profound transformations that will take multiple years to complete."

It requires courage to adapt and thrive in a digital age. "It's not an easy task," emphasises Theunissen. "Of course, all these transformations need to be carefully introduced, assessed and re-evaluated. But in the end, it also entails stubborn determination to pursue change and stay ahead of competition. If banks manage to successfully implement these essential technology trends, they will be ready for whatever the future holds."

TREND 1

Core revival

Series: Four essential tech trends for the banking industry

How can banks introduce futureproof technologies to keep up with their competitors? The series 'Technology trends for banks' explores four technology trends that are essential for banks to thrive in a digital society. This – the first – article dives into revitalising core systems. Tools that support core modernisation have become more sophisticated, user-friendly and cost-efficient in the past few years, which opens up exciting opportunities.

Pressure to change

Most banks are not keen to change their core systems, says Eef Gerritsen. He is director at Deloitte Consulting, focused on IT-transformations in the banking industry. "In a lot of cases, core systems of banks have been used for decades," he explains. "They are deeply engrained in the company and are intertwined with crucial business processes. This makes it understandably complex and risky for banks to change them."

Nevertheless, the banking industry is under great pressure to modernise their core systems. "First of all, banks face increasing competition from fintech start-ups," says Timo Span, partner at Deloitte Consulting specialised in IT banking. "Fintech start-ups do not carry the burden of legacy technologies and can optimally profit from new technologies. This enables them to create new products and services at lightspeed."

First of all, banks face increasing competition from fintech start-ups.

Moreover, customers are getting used to the instant results of the digital economy, and they expect their banks to keep up. Lastly, the COVID-19 pandemic has underscored the importance of being flexible and able to adapt to new circumstances, which should be supported with an adequate technical

architecture. “You can’t ignore the core,” concludes Span. “If banks want to survive, they need to ensure their core systems are futureproof.”

Replacing core systems: complex and expensive

Data-driven technologies such as Artificial Intelligence (AI), Machine Learning (ML), edge computing and quantum hold a lot of promise for the banking industry. But the current core systems of banks are mostly incompatible with these technologies. “At the moment, most data in core systems is siloed and not in the right format for real-time data processing,” says Gerritsen. “As a result, banks are not able to connect the dots and extract the most value from their data assets.”

As a result, a lot of banks have focused their innovation efforts on new initiatives outside their core systems. This allows them to experiment and create new services without the burden of legacy technologies. Although these initiatives may generate valuable insights, this is not a sustainable strategy in the long run, says Span. “At some point, you need to reconnect these initiatives to your core,” he explains. “Otherwise, you end up with hundreds of different incompatible systems, and you will miss out on the opportunity to effectively leverage your data assets.”

Other banks have set up ambitious projects that aim to replace their entire core systems for new, lean cloud-based systems. So far, these efforts have mostly failed, observes Gerritsen. “Core systems of banks are simply too big. Currently, it takes years to completely replace your core technology. At some point, the costs of such an endeavour can no longer be justified and the project is killed.” Also, replacing entire core systems holds the risk of creating legacy software of the future. “IT is developing rapidly. In five to ten years, these systems might be outdated, and you have to start all over again,” says Gerritsen. He adds that this is a serious risk for new players in the financial industry as well.

Core systems of banks are simply too big. Currently, it takes years to completely replace your core technology. At some point, the costs of such an endeavour can no longer be justified and the project is killed.

Redefine the core modernisation business case

Rather than replacing entire core systems, banks need to think carefully about which parts of their core systems should be modernised right away, and which parts can wait. “Whereas some parts of core systems should be replaced, other parts might be better off staying in business a bit longer – maybe in a leaner, more simplified version,” says Span. Avoiding replicating exceptions that have been defined and built in the past can help to prevent creating future legacy software. “It’s key to have a clear business case for every software exception and to separate exceptions from core technology to avoid issues during updates.”

Span emphasises that banks should closely monitor the market, as tools that support core revitalisation are rapidly improving and maturing. In the past few years, low code/no code platforms have become more sophisticated, user-friendly and cost-efficient. They are increasingly getting ready to transform core systems. Cloud vendors are making major improvements and are getting more fit for core replacement as well. “These developments result in compelling business cases for banks, in which migrations can be cost-neutral or even lead to cost savings,” says Span.

It’s key to have a clear business case for every software exception and to separate exceptions from core technology to avoid issues during updates.

Other examples include tools that scan core systems to see what types of codes need to be replatformed or removed. Some of these tools enable the automatic replacement of certain types of outdated code. Other tools can identify the business rules in the current core system and automatically reuse those in new systems. “These tools help to reduce complexity. They allow you to continue with your current core system, but in a faster and leaner form,” explains Gerritsen. He points out that in the context of core modernisation, these tools represent a game-changing breakthrough, as they not only contribute to better and faster core systems, but they are also improving over time as they leverage AI and ML to automate aspects of the code extraction process.

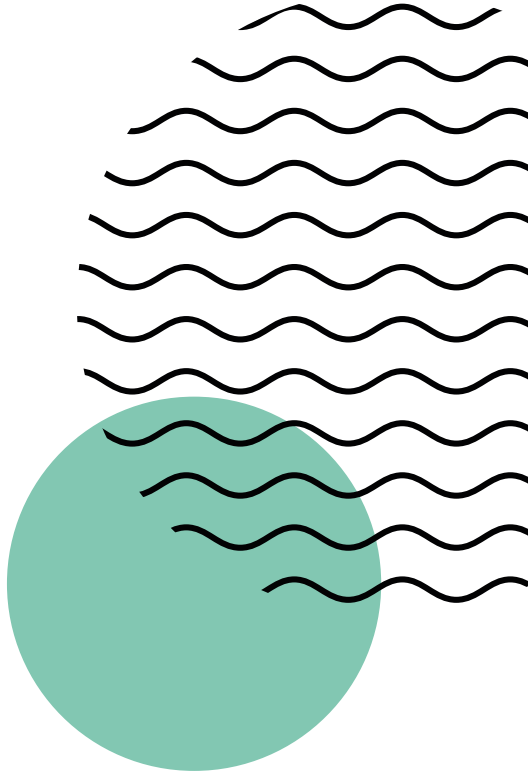
The way forward: think big, start small

Revitalised core systems that allow for flexibility and real-time data processing will create a lasting foundation for future innovation and competitive advantage. As tools that support

core revitalisation are improving and maturing, banks have the opportunity to redefine their core modernisation business case and make this future a reality.

Yet, banks should not rush the transition to a cloud-based core system. “Revitalising core systems is a massive undertaking that shouldn’t be underestimated,” warns Span. “Start with a clear strategy about which parts of your core systems need to be replaced, removed or improved. As the market of tooling is developing rapidly, timing is important. In some cases, it is better to wait a little longer.” The work of improving legacy core assets is not a one-time task but an ongoing opportunity, says Span. “When it comes to core revitalisation, it is best to ‘think big, start small’,” he says. “One step at a time, you will pave the way to faster, leaner and futureproof core systems.”

Read the report: *Core Revival*



MLOps: Industrialised AI

Series: Four essential tech trends for the banking industry

How can banks introduce futureproof technologies to keep up with their competitors? The series 'Technology trends for banks' explores four technology trends that are essential for banks to thrive in a digital society. This article explores the application of DevOps tools and approaches for Machine Learning, better known as MLOps. MLOps helps banks to scale ML models, lower operational costs and deal with urgent data management challenges such as accountability, transparency and ethics.

The promises and challenges of ML

Banks have been relying on data-analytics for a long time, but with Artificial Intelligence (AI) and Machine Learning (ML) technologies they can radically step up their game. "AI and ML are widely seen as key drivers to unleashing a bank's digital potential," says Riona Arjoon, manager at Deloitte Consulting, with a focus on data and analytics in the financial services industry. "All the banks are experimenting with AI and ML."

Yet despite the growth in ML adoption, few organisations manage to realise the broader, transformative benefits of AI and ML. In a survey among nearly 750 business decision-makers, only *8 percent* considered their companies' ML programs to be sophisticated. "A lot of ML projects do not get beyond the proof-of-concept phase," says Leon Kortekaas, director Cloud Engineering at Deloitte. "They struggle with a lack of expertise and production-ready data, as well as immature development and deployment processes."
AI and ML can transform the way business is done, but only if organisations reshape their operations and structurally embed AI and ML throughout the company, he concludes.

MLOps: DevOps meets Machine Learning

MLOps, which means applying DevOps tools and methods to ML, is the answer to these challenges. "About fifteen years ago, DevOps

transformed the way many IT teams delivered applications and services," explains Arjoon. "By standardising and automating application development, deployment and management, organisations dramatically improved development efficiency, delivery schedules and software quality." Now, organisations are getting ready to apply DevOps principles to ML. "This may have similar revolutionary effects and will help to realise the transformative benefits of AI and ML," says Arjoon.

Like DevOps, MLOps features automated development pipelines, processes and tools that streamline ML model development and operations. "It's an automated sequence to structure your modelling, deployment and management that allows you to get fast feedback," Kortekaas explains. "It makes the process more transparent and efficient." Structuring the application of ML models will allow companies to reduce operational costs and scale more quickly, says Kortekaas. He adds that cloud services help to make ML and MLOps easier to use for companies, as they reduce the complexity of having to manage the analytical services and infrastructure yourself. "MLOps creates a highway for ML that everyone can use safely, rather than lots of small dirt tracks."

It's an automated sequence to structure your modelling, deployment and management that allows you to get fast feedback.

Another principle of MLOps is the collaboration between experts in multidisciplinary teams. "Together, data scientists, ML engineers, business analysts and IT-operations professionals design, develop, operate and maintain ML applications in production," says Arjoon. "Multitalented teams help to create efficiency, scale and business value."

Detecting fraud, improving efficiency, and new services

TMNL, a collaboration of five Dutch banks, already uses MLOps as standard practice. It deploys AI and ML to monitor payment transactions for signals that could indicate money laundering or the financing of terrorism. "At TMNL, the entire data infrastructure is cloud based, which makes it easy to leverage ML," says Kortekaas, who currently leads the IT track at TMNL from Deloitte. "Tech, business and IT people work together and own the model end to end."

Other useful cases of deploying ML in the banking industry include models to automatically decide whether a consumer of a company is eligible for a loan or a mortgage. "At one bank, we reduced the response time to loan requests from small and medium business owners from several weeks to a couple of minutes with the use of ML," tells Kortekaas. Arjoon sees opportunities in banks through

creating personalised customer experiences. "Customer service agent augmentation is an example where natural language processing algorithms and sentiment analysis can be applied to better understand customers behavior and offer products and services which better suit their profiles."

MLOps to promote trust

Whereas the technical and business opportunities of AI and ML are developing rapidly, Kortekaas observes that companies are lagging when it comes to ensuring governance challenges such as accountability, security and ethics. "ML models are becoming easier to use for people without a technical background," he says. "This opens up amazing opportunities, but also results in a higher risk of data leakage."

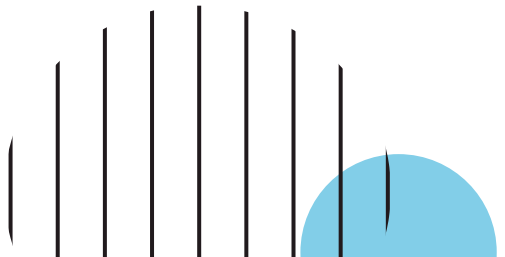
MLOps helps to mitigate these risks and address data management challenges such as accountability and transparency, regulation and compliance, and ethics. "By standardising and automating ML models you can embed ethical, regulatory and cybersecurity requirements in the MLOps pipeline," says Arjoon. For instance, banks can provide consumers insights into automated decisions. If you deny someone a mortgage based on an AI model's outcome, you can explain it to a customer. "With MLOps, you can set up your AI and ML models in such a way that every modification is recorded," says Arjoon. "This helps to make your model auditable."

The way forward

MLOps enables multitalented teams to work together more efficiently and to get more done in a standardised manner. By creating automated development pipelines, processes, and tools that streamline ML model development and operations, banks can scale ML models and reduce costs. Moreover, MLOps allows AI and ML teams to promote trust by embedding accountability and transparency, regulation and compliance, and ethics.

Last but not least, automating the more mundane tasks with MLOps will give AI and ML professionals more time for exploration and innovation. "MLOps makes the work more fun interesting," says Kortekaas. "This is an important factor to attract and retain scarce tech and data talent." In the forthcoming years, MLOps will become a standard practice and an important driver for change in the banking industry, says Arjoon. "Several banks are thinking about MLOps on a strategic level," she says. "Now it is time to make it a reality."

Read the full report *MLOps: Industrialised AI*



Machine data revolution: feeding the machine

Series: Four essential tech trends for the banking industry

How can banks introduce futureproof technologies to keep up with their competitors? The series 'Technology trends for banks' explores four technology trends that are essential for banks to thrive in a digital society. This article delves into the machine data revolution that is needed to support Artificial Intelligence (AI) and Machine Learning (ML) models. New technologies can help banks to disrupt the end-to-end data value chain and create a future-ready foundation for an era of automated decision-making.

The need for a new data architecture

It's no secret that new data-driven technologies such as cloud, AI and ML have tremendous *opportunities to unleash the digital potential* of the banking industry. "AI and ML technologies can create automated, real-time and at-scale decisions, which can dramatically improve results for the banks and their customers," says René Theunissen, partner at Deloitte Consulting specialised in enterprise technology for banking. "As financial institutions collect lots of data, and have been collecting data for a long time, they are – in theory – well-positioned to deploy data-driven technologies."

Yet at most banks, the enterprise data architecture is not designed to support rapid and consistent development of AI and ML. "Banks often rely on legacy technology and data models. Their data architecture is siloed and designed to support human decisions," explains Benedikt Kratz, director at Deloitte Consulting with a focus on data strategy, architecture and management in the financial industry. "If banks want to become truly data-driven, they have to implement automated, machine-based decisions in their primary processes," Kratz continues. "This entails reorganising their data architecture end-to-end."

Human vs. machine decision-making

Banks currently perform lots of data analytics, but mostly to support human decision-making. The data architecture of banks reflects this way of working. “Data is often organised in manually crafted spreadsheets with clean tables and rows,” explains Kratz. “This is convenient for humans but not optimal for the deployment of ML and AI models.” Moreover, data is stored in legacy systems that have been used for a long time and is siloed in systems that do not interact.

Machines, by contrast, can extract low levels of statistical significance across massive volumes of structured and unstructured data. They work around the clock and can make decisions at scale and in real time. “AI and ML allows banks to automate parts of their primary processes,” says Theunissen. “For instance, AI and ML models can make real-time decisions on whether a loan or a mortgage should be granted. This asks for a new data architecture, in which data is easily available in open-standards across all divisions.”

Unlocking the bank’s data goldmine

Fintech start-ups enter the market without the burden of legacy systems and can optimally profit from cloud, AI and ML technologies. However, they do not have the scale, experience and amount of (historic) data that can provide a deep understanding of customers and their needs. “Traditional banks are sitting on heaps of potentially valuable data,” says Kratz. “Now, it’s time to unlock their data goldmine by enabling themselves to put AI and ML models at work.”

Reengineering data value chains to support AI and ML’s possibilities is a complex task that can take up years, says Theunissen. “It touches every part of the value chain, including how you capture, store and process data.” New technologies and approaches can support this process, including advanced data capture and structuring capabilities, next-generation cloud-based data stores, and analytics to identify connections among random data. Together, these tools and techniques can help organisations turn growing volumes of data into a valuable asset to support automated decision-making.

Fundamental transformation, step by step

Reorganising the data architecture of banks requires a clear strategy, planning and management. “A first step is to understand what kind of data you have, how it’s stored, what the quality is and how it can be valuable,” says Kratz. “This is already a massive undertaking. For instance, ABN AMRO is in the

midst of modernising their data architecture, and they discovered that they are currently deploying more than 3,000 systems."

The next step is to prioritise: what parts of the data architecture need to be updated first, and why? "You cannot do it all at once, so you have to decide where to start," says Kratz, who adds that compliance and business value are particularly important in this respect. Subsequently, banks have to define the data and ensure that it can be reused in different platforms.

A first step is to understand what kind of data you have, how it's stored, what the quality is and how it can be valuable.

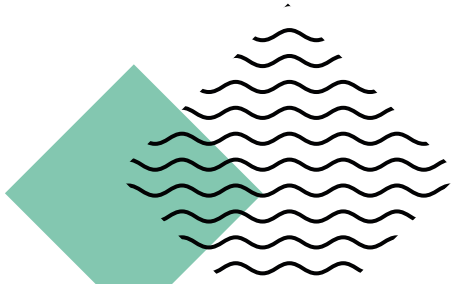
Last but not least, banks need to ensure that *ethics are embedded* in their new data architecture and that adequate governance is in place. "AI and ML models work with estimations; their outcomes need to be 'good enough'," explains Theunissen. "Although they can make decisions at scale, it doesn't mean that the results are flawless." Banks make impactful decisions, such as who gets access to loans and on what terms, and they need to be able to explain and defend their decisions. This can be done implementing these requirements in the design of the new data architecture.

What's next

There are lots of examples of banks already deploying AI and ML models. Theunissen mentions an example of a tool to assess whether an SME is eligible for a loan, which reduced the processing time from a week to only 15 minutes. "Tools like these are disrupting the market," he says. "However, these are mostly small initiatives and often do not transcend the proof-of-concept phase. Now, it's time to create a futureproof data architecture that enables deploying AI and ML models at scale."

Reorganising the data value chain to get ready for the AI and ML revolution is a long, complex, but exciting journey. "The current data architecture of banks brings a lot of hidden costs in manual labour," says Theunissen. "Modernising the data architecture is a massive undertaking. But in the end, it will bring enormous benefits in the form of efficiency, cost reductions and smarter decisions."

Read the full report: *Feeding the Machine: Machine Data Revolution*



TREND 4

Zero Trust – never trust, always verify

Series: Four essential tech trends for the banking industry

How can banks introduce futureproof technologies to keep up with their competitors? The series 'Technology trends for banks' explores four technology trends that are essential for banks to thrive in a digital society. With shifting enterprise environments and the introduction of data-driven technologies, banks need to fundamentally reassess their cybersecurity standards. A Zero Trust approach allows banks to effectively futureproof the security of their digital assets.

Safeguarding trust

A bank's most valuable asset is customers' trust. However, this trust is at risk when it comes to cybersecurity. According to Sandra Mavimbela, Manager Cyber Strategy at Deloitte Cyber Risk Services, cyberattacks in the banking industry are becoming more frequent and more sophisticated. "Cyber criminals are always looking for new weaknesses to exploit," she explains. "Because of their size and the fact that they handle valuable transactions, banks are interesting targets."

Essential IT and data management modernisations in the banking industry can result in new cybersecurity risks. *Reviving core systems*, *cloud migration*, *the introduction of automated decision-making models*, and remote office technology are examples of developing and shifting enterprise environments that generate vulnerabilities. The growth of smart devices, 5G, edge computing, analytics and artificial intelligence results in more data and connections, and also leads to an increasing attack surface.

"Banks have heavily invested in cybersecurity and most banks currently have decent cyber threat response systems," says Lourens Bordewijk, Director Risk Advisory at Deloitte Cyber Risk Services. "But as enterprise IT environments are developing rapidly and cyber criminals are always adjusting to the new circumstances, it's important that security departments keep up with the fast-changing threat and IT landscapes."

Cyberattacks in the banking industry

The IT infrastructure of banks can be divided in customer-facing frontend systems and internal backend systems. “Hackers try to attack both,” says Mavimbela. Common attacks on frontend systems are fraud on online channels, such as phishing scams in which people are tricked into clicking on a link with malicious software. “No matter how sophisticated your security systems are, humans are often the weakest link in the system,” Mavimbela explains.

Attacks on the backend systems of banks are less frequent but can have a high impact. A notorious example is the Bangladesh Bank cyber heist, in which hackers issued fraudulent transactions via the SWIFT network to illegally transfer close to 1 billion US dollars. Another example is the SolarWinds Supply Chain Cyberattack, in which hackers exploited a software update and got access to 18,000 SolarWinds customers, including many in the financial services industry.

No matter how sophisticated your security systems are, humans are often the weakest link in the system.

“Supply chain attacks are not new, but on the rise again and particularly worrisome because these attack vectors have been overlooked in the past and were not always covered during system design,” says Bordewijk. “With adequate precautions such as threat modelling during system design, segmentation and monitoring of untrusted third-party software, the impact of these cyberattacks can be easily prevented, detected and contained.”

Zero Trust: technology companies provide best practices

In a lot of organisations, cybersecurity investments are prompted by incidents. Zero Trust, on the other hand, entails fundamentally reassessing the approach to cybersecurity of the organisation and the skills, processes and technology that support it. “Zero Trust is not one solution, but a set of controls and design principles that guides decision-making in your security architecture and that you instil in your organisation,” explains Mavimbela.

The concept of Zero Trust is to always treat your infrastructure as if it’s breached. It assumes that no user, workload, device or network can be inherently trusted. Every access request should be validated on

all available data points, including user identity, device, location and other variables. This can result in both tightening existing cybersecurity measures and procedures, and implementing additional ones. Further simplifying, integrating and automating the security technology stack are also part of Zero Trust, and help to improve the efficiency of security teams and streamline security processes and operations.

Technology companies such as Google, Microsoft and Netflix have already integrated a Zero Trust approach to cybersecurity throughout their organisation. For banks this is harder to achieve, since they often do not have a unified IT landscape and have to deal with legacy systems from different mergers and acquisitions. However, technology companies do provide best practices that banks can implement, such as least-privileged access, micro-segmentation, and automated detection of unusual behaviour based on trust scores. “Banks already do this to some extent, but there are more high-impact Zero Trust controls that banks can implement,” Mavimbela explains. “The more you can standardise and automate, the more your security teams can focus on the more complex issues.”

The way forward: implementing Zero Trust step-by-step

The move towards Zero Trust requires significant change effort and planning. “Zero Trust is not a one-click solution,” warns Bordewijk. “In fact, it might take decades before banks have fully integrated Zero Trust throughout the organisation and it might be too expensive.” This means that banks need to prioritize where impactful security improvements are most needed. “Start with a pilot,” recommends Bordewijk. “For example, try to implement several high-impact Zero Trust controls for the new cloud environment or for critical payment systems on-prem.”

Zero Trust is not one solution, but a set of controls and design principles that guides decision-making in your security architecture and that you instil in your organisation.

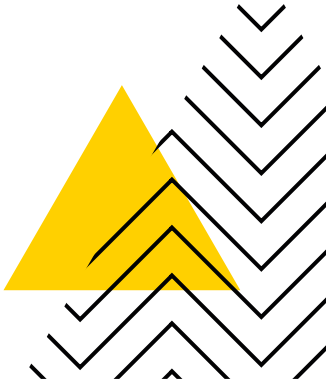
Start with identifying the attack surface, model relevant security threats and agree on the scope of the project, says Bordewijk. Optionally, perform a red team exercise to measure the current risk exposure. Then, several high-impact and best-practice Zero Trust controls should be considered, such as validating and strengthening endpoint security and measuring their health and risk-score, implementing strong, adaptive

authentication (e.g. for identities, devices, services and applications), micro-segment assets at risk, tailored monitoring, least-privileged access and encryption to critical data sets, and only allow access from trusted/ secured devices. Afterwards, security tests or red team exercises will be performed to measure the realised riskreduction.

It can be tempting to wait with implementing high-impact security controls until it's too late. "That's why it is important to continuously measure the attack surface and effectiveness of critical security measures and demonstrate their value to the board of the organisation," says Bordewijk. This helps to develop a business case for your security programme and contributes to an effective security architecture that can be reused in other parts of the organisation.

Ultimately, each bank that adopts Zero Trust will need to determine what approach best suits their unique environment. This includes balancing risk profiles with impactful controls to be implemented. Adoption and standardisation of impactful Zero Trust controls can help the security department to keep up with the increasingly changing threat and IT landscapes, says Bordewijk. "High-impact Zero Trust controls should become part of every modern enterprise (cloud) environment."

Read the full report: *Zero Trust: Never Trust, Always Verify*



Contact

René Theunissen
Partner
+31621272952
rtheunissen@deloitte.nl

Harmen Meijnen
Partner
+31882884258
hmeijnen@deloitte.nl

Eef Gerritsen
Director
+31882882904
egerritsen@deloitte.nl

Leon Kortekaas
Director
+31882885221
lkortekaas@deloitte.nl

Timo Span
Partner
+31882885164
tspan@deloitte.nl

Riona Arjoon
Manager
+31882884208
rarjoon@deloitte.nl

Lourens Bordewijk
Director
+31612581585
lbordewijk@deloitte.nl

Sandra Mavimbela
Manager
+31882883063
smavimbela@deloitte.nl

Deloitte.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.