CGI

Experience the commitment®

BANKING. TRANSFORMED.

CGI's experts discuss:

Protecting the bank

Jerry

Jerry Norton, Vice President, Global Banking, is responsible for CGI's strategy across the wholesale and corporate markets. He also is a member of both CGI's Banking Industry Cabinet and Growth Council. Jerry specializes in industry-wide change, whether led by business or technology, and his views are sought across the global market. He brings a combination of domain expertise and technology stewardship coupled with an understanding of compliance, regulation and operational risk prevention and management. Much of his current focus is on the changing nature of business and technology in the payments market. Jerry is a regular presenter at international conferences on the major financial services themes of the day, a contributor to a number of think tanks, and is often quoted in the mainstream and trade media.

Jan

Jan Macek, Vice President, has 18 years of experience in the IT consulting sector, with 11 years of experience in senior management positions. For the past nine years, he has built up his expertise in the financial industry, specializing in the field of anti-financial crime.

Jan's CGI responsibilities include leading a team that delivers services and solutions in the Czech Republic, Slovakia and Eastern Europe, globally leading CGI's anti-crime consulting services and overseeing CGI HotScan360, which helps clients effectively fight financial crime.

As a member of the CGI Global Banking Cabinet, Jan contributes to the development and evolution of CGI's strategy in the banking industry.

CGI's experts discuss: Protecting the bank

In a series of conversations, CGI banking experts discussed four critical areas of banking transformation: modernizing, extending, protecting and digitalizing. This overview shares highlights from the "Protecting the bank" roundtable, which included Jerry Norton, who leads global banking at CGI, and Jan Macek, an expert in CGI's financial crime practice.

First, what do we mean by protection? How would you define it?

Jan: Protection involves more than keeping money safe and preventing anti-financial crime; it touches upon all parts of the bank and the banking industry. Protection today involves securing the entire banking ecosystem and the massive amounts of data that banks have on their customers.

Jerry: We know from this year's CGI Client Global Insights and our annual bank consumer survey that trust is the most critical aspect of the relationship between customers and their banks. Trust also is a key attribute in the digital world. Protection, therefore, is all about banks maintaining trust with their customers, and this is especially important when it comes to digital banking. When a bank loses trust, it loses business, and we've seen many recent instances of this in the press.

Other key aspects of protection include loss prevention and regulatory compliance. Fraud can result in huge financial losses, not to mention reputational loss. Regulation also puts a lot of pressure on banks. Effective protection addresses the challenges of each.

What are some key protect the bank challenges that banks face?

Jan: As banks become increasingly complex digital businesses, there's tremendous pressure for them to protect their entire organization and ecosystem, which impacts all of their employees, ways of working and technologies. In addition, the speed of processing today adds to the pressure, pushing banks to their limits. Customers want to make payments and decisions immediately, and legacy batch systems simply can't cope.

Jerry: Yes, and faster payments result in faster fraud.

Jan: Automation is another key challenge. Banks are automating as much as they can, as well as integrating machine learning and artificial intelligence. While managers may think automation doesn't impact their control, they're actually giving decision-making over to the machines and slowly losing control of the processes. On top of this, just a few lines of corrupted code can completely change a process, creating real havoc.

In my view, the top challenge though is the need for banks to consolidate protect the bank activities. Having multiple departments responsible for these activities is ineffective. Without a 360-degree view, banks can't see everything and deal with the continuous threats that come against them from all sides.

All of these challenges, in turn, lead to cost pressures. The daily cost for protecting the bank is increasing every year and becoming a huge issue for the CXO. When you look at it from the top and across the bank's entire organization, the cost is at almost 30% of IT budget spend. Banks are asking how they can control these costs. How can they reduce or at least optimize them?

Jerry: Correct, protecting the bank is often seen as a grudge purchase, not an income generator. Cost control is critical.

Jan: Evangelization is yet another challenge for the CXO. Every single employee, customer and partner plays an important role in the overall security of the bank. Just one small mistake by a customer, for example, can lead to a security or regulation breach that results in a huge cost to the bank. So, it's critical that a bank acts as an evangelist when it comes to protection. Currently, customers simply don't care if they wrongly enter their card in an ATM, as they expect the bank to protect them and pay for their mistakes.

What strategies and/or technologies can help banks overcome these challenges?

Jerry: Banks traditionally have examined data in subsets, but today there's a clear need for a holistic view of data, whether it's related to customers or transactions. Once a large pool of data is collected, clever pattern-matching techniques, machine learning and artificial intelligence can be employed to effectively check for false positives and improve hit rates.

Identity, onboarding and "know your customer" (KYC) are other key areas that banks need to improve. Having effective security checks in each area when the first contact occurs will prevent bad actors from the start. Of course, this isn't just about your own customers. There also are issues involved in accepting payments from other banks and networks, as well as overseas. It's critical for a bank to understand the full history of a payment or risk.

Jan: Yes, and this raises an important point, which is that anti-financial crime is not an area in which banks are competing against one another. In fact, by sharing experiences, insights and patterns, they can only benefit. It's a win-win situation. So, there's a real urgency for banks to realize this and pursue collaboration when it comes to protecting the industry and taking a collective stand against suspicious activities. Perhaps shared KYC services will play an important role.

Jerry: Yes, our clients regularly raise the need for shared services, and many banks are keen to create some type of KYC shared service. However, there are blockers. One of these is GDPR, which prohibits a bank from disclosing individual information to other banks.

Second, there's a broader regulatory concern. Many regulators are wary of shared services, thinking they leave banks off the hook in terms of accountability. Years ago, for example, we worked with a country to implement a protection-based shared service. Technically, it could work, and, through this shared service, useful insights could be generated when looking at data sets across multiple banks. However, in this instance, the regulator didn't allow the work to go forward due to accountability concerns.

Other countries may be more receptive. In the U.S., for example, some organizations are looking at the shared services concept, knowing that the increased insight and ability to protect outweighs the accountability risks.

Jan: Yes, I believe this is really important as the industry becomes more interconnected. Banks are no longer independent and isolated organizations, and they're now connected to third parties through APIs. So, protection is becoming an industry-wide issue, and it would be good to see a future solution that protects the entire banking ecosystem, as we are only as strong as the weakest link. Also, with open banking, there will be a myriad of weak links and back doors, so industry-wide collaboration will be even more important.

What role does emerging technologies play in protecting banks?

Jerry: Banks are dealing with huge amounts of data in near real time. To protect the ecosystem, they need to recognize patterns related to both known parties, such as customers, and unknown parties, such as bad actors operating incognito. Emerging technologies can, without a doubt, help banks with this mammoth task. Data analytics, machine learning, artificial intelligence, real time and cloud technologies are critical, as well as some of the ideas used in blockchain technologies such as hashing and tokenisation. Anti-financial crime solutions won't work without using some of these new technologies.

Jan: I absolutely agree on the critical role of emerging technologies in protecting the bank. As an example, I was talking to a client executive recently who asked if we could handle a wide range of different fraud sources, including digital fraud, internal fraud, trade fraud, etc. However, it's not effective to use a "silo" approach to protecting the bank. Instead, you need a lightning fast, overall view of the entire protect the bank area—not just financial crime. You need to understand what's happening in every department across the bank. The dream, therefore, of every CEO is to have a single "cockpit" view, and, for this, you absolutely need emerging technologies.

Banks are constantly under attack. They're not going to stop every attack, so protection is more about managing risk. What is an acceptable level of risk? For example, you might have a dashboard that displays upcoming risks, and, even though it's not 100% accurate, indicators can at least put a bank on alert and lead to better risk management.

Jerry: Yes, exactly, a dashboard view of risks, along with costs, would make a CEO happy.

So, emerging technologies can help to transform a bank's approach to protection. What then does a fully transformed bank of the future look like?

Jerry: Looking to the future, a fully transformed bank would be forward facing with a dashboard that helps to predict an attack rather than just respond to one. On one level, this seem too smart, but this is the artificial intelligence vision of the future. It's all about using AI to help detect something out of the ordinary and identify it as fraudulent.

Of course, this brings up issues with customers in terms of balancing trust and frustration. People have only a light tolerance when it comes to having their payments blocked. So, in a fully transformed bank, you have to achieve this without impacting the customer.

To avoid customer impact, patterns are needed. A model of each person's normal behaviour can be matched against real-time activity. The system then alerts the bank if anything unusual goes on. This should be fairly easy for normal purchasing behaviour. It's the infrequent purchases/transactions that make it hard because, as we said, customers have a light tolerance for their payments being blocked.

Jan: Absolutely, and when you have normal behaviour models for each customer, you can then roll them up to have a normal behaviour state for the bank as a whole. This normal state can be viewed on the dashboard in real time. However, this is the future, and banks aren't there yet.

What about the customers? How will they interact with their bank in the future?

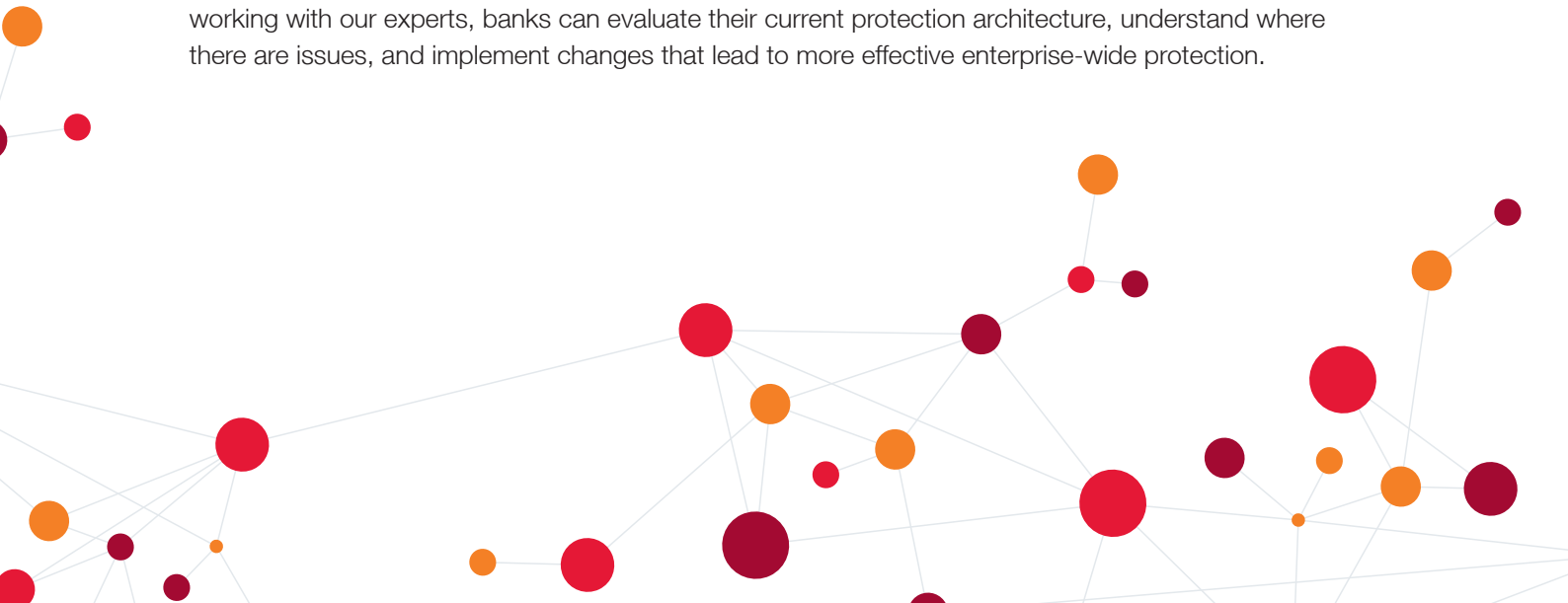
Jerry: It's all about interacting electronically, immediately and with more rigorous security checks done behind the scenes. For the customer, the journey will be easier and more seamless.

Jan: We all know that security checks are one of the biggest frustrations for customers, partners and employees. A few years from now, I imagine banks will deploy sophisticated cyber solutions for authentication and onboarding. Again, artificial intelligences and biometrics will play a critical role here, not only to tighten security but also to ease journeys across the entire ecosystem for all.

Finally, what are some key recommendations for banks?

Jerry: My first recommendation is to acquire a holistic view of data. Put in place a protection architecture that looks at and manages customer data holistically across all transaction streams. This is a big challenge, but, once properly implemented, it generates big opportunities.

Jan: Absolutely, and, on a similar note, they also should consolidate departments that currently deal with protection in silos. In doing so, they can make gains from acting as a harmoniously aligned business. By working with our experts, banks can evaluate their current protection architecture, understand where there are issues, and implement changes that lead to more effective enterprise-wide protection.



A partner for transformation

Since our founding in 1976, CGI has been at the heart of transformation in the banking industry. Today, we support more than 500 financial institutions worldwide, helping to deliver a broad range of digital IT and business strategies, services and solutions. Our deep understanding of the complex global challenges banks face coupled with our strong local relationships enable us to build long-term partnerships that drive success.

CGI's Digital Transformation Practice is anchored around helping clients create a more agile business, one that can continuously respond to changing market and customer needs. CGI has built its practice around providing the end-to-end capability that clients need to enable their transformation and agility. We have more than four decades of experience in helping leading organizations across the world, move forward with their innovation and transformation agendas while helping them elevate their legacy infrastructures.

If you're interested in learning how we can support you on your transformation journey, contact us today. One of our consultants would be happy to help you.

Banking.transformed@cgi.com