Digital Identity:

Fulfilling Consumer Cravings for Elevated 'Digital Experience'

By Sophie DECOCK, Country Manager VMware Belgium & Luxemburg

The business-consumer relationship has been challenged by a world gone digital. As organisations work to discover their digital identity, growing consumer expectations are placing online experiences under a microscope.

Evidence (conducted in a research via online surveys via YouGov in UK, France, Germany Italy and Spain with a minimum of 1,000 respondents in each country) shows that many people are digitally curious, with 42% of Europe's consumers who think the increased presence of digital experiences in their daily lives is exciting rather than scary. Data also shows 46% of people are using a specific brand service because of its superior digital offerings in the market. This is great news for organizations out there who are currently rethinking, adapting or creating their next digital strategy move.

However, despite this digital appetite, consumers have been left feeling underwhelmed in the online services they've been served up; a judgement business cannot afford to ignore.

As digital connectivity continues to improve the quality of leisure, work and daily living, today's consumer is increasingly reliant on the functionality of their tech, and the possibilities it provides.

And with this comes the opportunity for businesses to increase the diversity of their digital services – but in a way that separates them from the competition.

Has the App become the new bank branch?

Time is finally up for financial services firms failing to create the engaging digital experiences that consumers have been crying out for. Almost half of European consumers (42%) prefer to engage with banks via apps rather than in person with members of staff, while more than a third (36%) believe their smartphone is more important than their wallet in powering financial transactions (rising to 47% of 18-24 year olds).

In a fiercely competitive market, that has seen traditional and challenger firms battle it out to win customer attention, almost half (46%) of consumers prioritise easy to consume apps and digital services when choosing a financial services provider. Only a third (34%) of consumers believe the financial services firms they interact with now deliver an improved digital experience compared to before the pandemic.

After the great 'digital switch' of last year, consumers are rightly demanding more from an industry where the battle for the best customer experience means success or failure to businesses in the financial services sector. In this new battleground, the most successful firms will be the ones that are becoming digital at the core – where they can adapt and innovate faster to create better user experiences, without compromising security, in the process. Those firms who have a digital-first posture, have everything to play for.

La Banque digitale européenne Advanzia Bank poursuit son success story

Advanzia Bank, la banque digitale européenne spécialisée dans les cartes de crédit et les solutions de paiement, annonce une nouvelle année de croissance continue et de fort développement des bénéfices. Avec 1,9 million de titulaires de cartes de crédit dans son portefeuille, la banque a enregistré un encours brut de 1,9 milliard d'euros et a atteint un revenu net de 100 millions d'euros.

Roland Ludwig, CEO d'Advanzia Bank, commente : «Advanzia a poursuivi son success story en 2020, malgré des circonstances des plus défavorables. Non seulement nous avons maintenu notre activité, mais nous avons également pu nous développer sur tous nos marchés et offrir une stabilité de service à nos particuliers, clients professionnels et établissements financiers. Les résultats d'Advanzia démontrent le succès de notre souscription prudente des risques de crédit et notre agilité à adapter les stratégies marketing pour améliorer la performance du portefeuille dans un environnement changeant».

Acquisition et transfert du portefeuille de cartes Capitol achevées avec succès

Avec l'acquisition et le transfert du portefeuille de cartes Capitol de Catella Bank, Advanzia Bank a consolidé sa position de fournisseur leader de services de cartes professionnelles pour les banques et les établissements financiers. La banque accompagne désormais 89 banques dans 12 pays, avec une présence croissante en Europe.

De bonnes performances sur les marchés établis de la banque

En Allemagne, le plus grand marché de la banque, la «Gebührenfrei Mastercard Gold» a terminé l'année avec un encours brut de 1,6 milliard d'euros et 1,6 million de clients. Les produits de la banque ont fait preuve d'une grande résistance en 2020 et ont continué à surpasser le marché. En France, la part de marché croissante de la «carte ZERO» a conduit à un encours brut de 134 millions d'euros à la fin de l'année. Grâce à son positionnement unique en Autriche, la banque a lancé un programme co-brandé pour ses clients professionnels et a terminé l'année 2020 avec encours de 109 millions d'euros pour la «free Mastercard Gold». Ces trois marchés ont contribué activement aux bénéfices d'Advanzia en 2020.

La numérisation et la croissance comme priorités stratégiques

La deuxième année d'activité de la banque en Espagne a été stable malgré une forte influence de la pandémie, avec 66 100 clients de carte de crédit «Tarjeta YOU», encours brut de 30 millions d'euros à la fin de 2020, et une entrée réussie sur le marché de ses programmes de cartes de crédit co-brandées. La banque est convaincue que les investissements réalisés pour l'entrée sur le marché entraîneront de fortes évolutions à l'avenir.

Face aux défis posés par la pandémie en 2020, Advanzia Bank a continué d'assumer son rôle vital de fournisseur de cartes de crédit dans l'écosystème des paiements.

La banque a également gagné des parts de marché et a franchi des étapes importantes dans son parcours de transformation numérique en introduisant des solutions de paiement mobile sur tous ses marchés et en lançant des applications mobiles pour ses clients. Avec l'introduction d'une infrastructure basée sur le cloud et le déploiement de son API Gateway, la banque a posé les fondations de sa croissance future.

La feuille de route pour 2021 et au-delà se concentre sur la transformation numérique en créant une plateforme bancaire centrée sur le client et une expérience client unifiée et omni-canal. L'accent permanent mis sur les possibilités de croissance par la diversification des marchés, les accords de partenariat et les acquisitions de portefeuilles reste une priorité stratégique essentielle en 2021 également.

Research in Finance

On Cybersecurity risk planning

With the development of financial technologies known as FinTech, Cyber risks have become one of the major operational risks faced by financial institutions. For the new emerging sector of FinTech credit, recent research by the Committee on the Global Financial System and the Financial Stability Board (CGFS-FSB (2017)) indicates that Cyber risk is the major operational risk. It is important, however, to realize that Cyber risks differ from typical operational risks. As pointed out by Kashyap and Wetherilt (2019), Cyber risks are special in the way shocks occur as well as their potential impacts after occurrence of those shocks. The specificities of those shocks thus call for specific public policies and regulatory adaptations.

Broadly speaking, there exist two types of Cyber attacks. The first category disrupts computer systems. The second affect the data by gaining access, eventually corrupting data. Both types of attacks, however, share common characteristics that differ from standard operational shocks. First, the Cyber attacks typically have malicious intentions with the aim of inflicting maximum damage. This might influence the timing as well as the targeting of multiple systems at the same time. Second, the likelihood of a high-impact event is rather a question of time than whether it occurs. Third, the eventual "invisibility" and the time to detect the occurrence of the attack. If the attack is not immediately noticed, data might have been corrupted and compromised long time before the attack is contained. Fourth, as pointed out by Lewis (2018), new technologies reduce the cost of attacks (the budget of the attacker) but increase their impact.

Given the systemic nature of Cyber risks, the resources allocated by firms might not be sufficient as they take only into account "private risks" and not the systemic component that takes effect through externalities. Private firms that are profit-driven typically focus on private costs due to data breaches but tend to neglect externalities. This has led to inefficient cybersecurity markets, as only a fraction of social costs are taken into account. In that case, the government plays a significant role in achieving investment efficiency. Such an efficiency can potentially be restored by regulation and/or incentive mechanisms.

Bagchi and Bandyopadhyay (2018) suggest that a coordinated security architecture where governments invest in intelligence and firms in safeguards, is much more efficient than firms taking decision on a standalone basis. Those types of optimal decision-making problems are addressed in a new emerging literature called "Economics of Cybersecurity". This literature broadly shifted from the analysis of private cost studies to social cost studies. Ransbotham and Mitra (2009) seems to be the first paper to have introduced strategic interaction into cyber defense. In a more recent paper, Nagurney and Shukla (2017) analyze the value of cyber information sharing and cooperation for cybersecurity investments. Simon and Omar (2020) analyze optimal cybersecurity investments in supply chains without and with information coordination in case of strategic and non-strategic attackers.

Paul and Wang (2019) analyze the optimal balance between prevention safeguards and the detection & containment safeguards, using robust optimization in the face of cybersecurity uncertainty. This opens the door to applications of decision-theoretic models. Thus, Paul and Zhang (2021) analyze the interplay of government, firms and cyberattacks in a two-stage stochastic programming problem where part of the decision can be made after information is revealed. The focus is on strategic resource allocation aimed at minimizing social costs due to data breaches from cyberattacks. The government plays a role via intelligence investments. The intelligence by governments can provide information about potential future threats and systemic risks. The goal is to minimize social costs of a cyberattack.

The total social costs are composed of the following elements:
- Intelligence investment by the government
- Detection investment by firms
- Containment investments by firms
- Deprivation cost due to detection delays
- Deprivation cost due to contained delays

Intelligence by governments will help with forecast accuracy concerning future cyberattacks. Such information needs to be selectively communicated. Firms face different resource allocation strategies, called the cybersecurity portfolio mix. They can invest in prevention and/or more towards detection and containment mechanisms. The former decrease the risk of attacks, whereas the latter reduce time to diagnose an attack and reduce net losses.

The authors implement a case study by calibrating the model involving the different decision makers based on real data. The decision-making problem is formulated as a two-stage stochastic programming model. Governments and firms make strategic decisions about intelligence and detection investments in the first stage. The attacker then attacks and firms then implement further containment investment decisions in a second stage.

The positive externalities of the cybersecurity investments influence the optimal decisions of the firms' cybersecurity portfolio mix (detection versus containment and prevention) as well as government investments.

The computational study leads to the following conclusions:
- The attackers' budget (means) mainly impacts the second stage containment investment by firms
- The externality potentially reduces government intelligence investment
- Firms budget allocation prioritize detection investment over containment investment
- It is effective to spend more on intelligence given the reduction of social costs related to cybersecurity.

As to our knowledge, Paul and Zhang (2021) is the first paper to address such optimal decision-making in a coordinated security architecture. Their calibration of the cyber breaches is calibrated on past data form the Ponemon Institute (2017). Given the importance of cyber risks for the new FinTech industry, it can be expected that financial markets indexing such risks will rapidly develop. As explored in Verlaine (2020) this opens the door to the use of structured financial products to extract information, not only about past potential threats, but future expected threats using elicitation techniques with information theoretic concepts.

Dr. Michel VERLAINE
ICN Business School
Head of the Finance and Risk Management Master specialization in Berlin
https://www.icn-artem.com/en/berlin-campus
Michel.verlaine@icn-artem.com

Bagchi, A. and Bandyopadhyay, T. (2018) "Role of intelligence inputs in defending against cyber warfare and cyber terrorism", *Decision Analysis* !%(3), 133-194.
Cambridge Center for Risk Studies (2016) "Managing Cyber Insurance Accumulation Risk"
Committee on the Global Financial System and Financial Stability Board (2017) "FinTech credit: market structure, business models and financial stability implications", *CGFS papers May*.
EIOPA (2018) "Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies", Publications office of the EU.
G-7 Cyber Expert Group (2017) *Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*, October. Washington DC: G-7.
Kashyap, A. and Wheterilt, A. (2019) "Some Principles of Regulating Cyber Risk", *American Economic Review Papers and Proceedings 109*, 482-487.
Lewis, J. (2018) *Economic Impact of Cybercrime—No Slowing Down*. Santa Clara McAfee.
Nagurney, A. and Shukla, S. (2017) "Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability", *European Journal of Operational Research*, 260(2), 588-600.
Paul, J.A. and Wang X. (2019) *Socially optimal IT investments for cybersecurity*, Decision support systems.
Paul, J.A. and Zhang, M. (2021) "Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker", *European Journal of Operational Research*, 291, 349-364.
Ponemon Institute (2017) "Cost of data breach study: global overview".
Ransbotham, S. and Miktra, S. (2009) "Choice and chance: A conceptual model of paths to information security compromise", *Information Systems Research*, 20(1), 121-139.
Simon, J. and Omar, A. (2020) "Cybersecurity investments in the supply chain: Coordination and a strategic attacker", *European Journal of Operational Research* 282(1), 161-171.
Verlaine (2020) "On the Extraction of Cyber Risks Using Structured Products", Proceedings of the Decision Sciences Institute Annual Meeting, pp. 944-965, Virtual US meeting.