Part II

Digital Business 2020: Getting there from here!

Banking in the Digital Era
Regaining Consumer Trust
Cognizanti is an annual journal published by Cognizant. Our mission is to provide unique insights, emerging strategies and proven best practices that globally-minded companies can use in their quest for business and IT performance excellence.

All articles published in Cognizanti represent the ideas and perspectives of individual Cognizant associates and contributors who have documented expertise in business-technology strategy and implementation. The content of the articles published in Cognizanti represents the views of the individual contributors and not necessarily those of Cognizant. They are put forward to illuminate new ways of conceptualizing and delivering global services for competitive gain. They are not intended to be, and are not a substitute for, professional advice and should not be relied upon as such.

For more insights, and to continue the conversation online, please visit our e-community at http://connections.cognizant.com or download our Perspectives app from the Apple App Store or Google Play at http://cogniz.at/itunescognizantperspectives or http://cogniz.at/googleplaycognizantperspectives, respectively.
Amid wavering consumer confidence, changing banking behaviors, widespread hacks and new competition, here’s what traditional banks can do to rebuild trust in the digital era.

Consumer banking in the last seven years has undergone radical change. Depositing a check no longer happens at the branch or ATM but through a mobile phone. From processing payments to providing loans, financial services that were historically the sole preserve of banks are being usurped by nontraditional competitors, ranging from technology, retail and e-commerce giants, to online-only banks and digital upstarts.

Digital innovations and new consumer behaviors are significant drivers for the rise in alternative banking approaches, such as peer-to-peer lending and mobile wallets. But there is another reason that consumers are turning to new ways of making payments, storing funds, finding loans and even getting financial advice: waning trust.

According to the 2015 Edelman Trust Barometer, banking and financial services (along with the media and chemicals sectors) are the least trusted of industries, compared with technology, consumer electronics, energy, telecommunications and food/beverages. Consumer trust was deeply shaken by the industry’s dubious lending practices and questionable business decisions that helped spur the 2008 economic downturn; while trust has improved modestly since 2011, according to Edelman, cybersecurity threats have more recently dented banks’ claims of impenetrability.

Combined with new digital technologies, the trust gap spurred by the recession presented the perfect opportunity for new competitors to encroach on traditional banking territory, as consumers – especially millennials – were just as open to simple and low-cost banking capabilities provided by a mobile app or beloved brand (like Apple or Amazon). What is more, millennial customers are more likely to switch banks than previous generations, according to the Edelman study.

What can banks do, then, to regain their footing in a quickly changing industry and earn consumer loyalty once again? Here are our recommendations for banks of all sizes:
Provide proactive communications.

Banks need to make themselves heard above the noise of new competitors, mobile apps and completely new approaches to banking, such as peer-to-peer – or crowdsourced – lending. Localized and personalized marketing messages are one approach, and are particularly effective when the message is conveyed on the customer’s channel or method of choice. Amid the very real threat of cyber threats and credit card hacks, frequent and proactive communiques with customers are also essential. As an example, Citibank and American Express recently sent out security notifications and replacement cards voluntarily when the organizations detected suspicious activity, even before legitimate fraud was found. The two companies did this both as a precaution and to reassure customers that their money and personally identifiable information were in good hands. Such proactive engagement goes a long way toward building trust.

Develop an advanced analytics capability.

Big data and advanced analytics are essential tools for understanding consumer demand, anticipating customer needs and responding to those needs in the form of relevant and even personalized offerings. When banks are perceived as more relevant, it builds consumer trust. Advanced analytics techniques are especially important for understanding customer behaviors today, as consumers bank across multiple – and increasingly digital – channels. Banks need to take an “actionable analytics” approach that not only enables high-speed trading and fraud analytics but also combines analytics, big data and business process management (BPM) technologies to deliver tangible business results, including total client visualization, campaign discovery, cost reduction, revenue optimization, client churn, client acquisition and predictive analytics.

For example, analytics can be used to identify where and why transactions were abandoned, fuel location-based offerings, align customer transactions with the least expensive channel, and discover what enhances or detracts from the customer experience. (For more on this topic, read our white papers, “Making Analytics Actionable for Financial Institutions” and “Creating One Customer Journey Ecosystem that Meets All Banking Needs.”)
Nurture personalized relationships.

Advanced analytics is also crucial for creating more meaningful and personal customer relationships. In order to forge a lasting relationship, banks need to move beyond viewing customers as a series of disparate accounts, to understanding them as individual depositors and borrowers. Specifically, banks need to analyze customer interaction and transactional data from all bank channels and combine that with the customers’ other digital activities (what we call the customer’s Code Halo™), make meaning from it and then develop tailored offerings and services that suit each consumer's preferences and needs.

For instance, if the bank sees that a longtime customer’s paycheck deposits have notably increased, it could take that as an opportunity to offer a high-profile credit card. If another customer is paying multiple student loans at one time, that might indicate a positive response to an offer for student loan consolidation. Through social media, a bank could detect whether someone is planning a vacation or researching websites for a big purchase and offer a credit card with special offers for those purchase items. Or it could note that a customer toward the end of his car loan is spending time on the Web looking at new cars and insert an ad onto Cars.com for special financing rates.

Using advanced analytics-driven tools, such as customer personas and journey maps, banks can personalize pricing and credit privileges based on meaningful insights, not general demographics. Well-rated banks are already doing this, and aspiring banks will need to follow suit. (For more on this topic, see our white paper, “For Effective Digital Banking Channels, Put Customers First.”)

Reinforce the digital vault.

With new types of threats, cybercrime poses a real issue for banks when it comes to customer trust. Indeed, trust seems to be the driving factor behind security spending, even greater than financial loss resulting from cybercrime.

The ongoing evolution of technology has resulted in a rapidly changing threat environment, posing a real learning curve for banks. Besides probing for the weakest link in the banking ecosystem, criminals are also developing new methods of attack, targeting new channels of communication as banks introduce them. For example, the user-friendly VISA payWave system, in which a customer swipes a card near a reader to buy something, makes it faster and more convenient to pay, but it also exposes the transaction to unauthorized users who can steal the information wirelessly.

Another example is the introduction of mobile banking and mobile applications. Both offer customers convenient channels for communication; equally, mobile threats such as mobile malware and “spim” (spam over instant messaging) are also among the fastest growing forms of cyberattack.

Evolving technologies can also help banks meet the cybersecurity challenge. Leading organizations are looking to the latest data management, monitoring and analytics technologies to anticipate potential vulnerabilities and threat vectors, as well as the impact of these threats, to determine the most appropriate, risk-based action to take.

New tools are rapidly emerging to fill existing gaps in reactive forensics (such as e-discovery solutions) and proactive analytics (such as tools that mine significant data sets to analyze patterns and support risk-based approaches). This is particularly relevant for cybersecurity, as not all threats are equally severe and must
The cyber domain is continuously evolving, providing both new opportunities and challenges for financial services institutions. To improve cybersecurity, banking organizations must elevate the topic and address threats holistically at the highest levels of the organization in a manner that they understand. In this effort, they need to:

- **Understand threats.** Just as the likelihood and impact of cybercrimes varies, so should the responses to them. For example, banks need to distinguish between attacks that are financially motivated and those that are not. In the past, malicious attacks were more the norm and were easier both to execute and defend against. With more complex layers of technology being added at an exponential rate, more recent attack vectors have concentrated on accessing customers’ personally identifiable information and passwords to conduct fraudulent banking transactions and enable broader based customer identity theft. Cybercrimes that have caused the greatest financial and reputational impact, although less spoken about publicly by banks, have been those perpetrated by bank employees themselves or through the banks’ technology partner networks.

- **Cooperate externally.** Banks are perceived as operating in silos, but greater external cooperation should enhance their cybersecurity efforts more broadly. Criminals often target weaker links in the banking ecosystem, and it would be in the banks’ long-term interests to help third-party actors improve their own cybersecurity efforts.

- **Improve awareness.** By educating everyone from end users and employees to top management, banks must continue to improve educational efforts surrounding cybersecurity.

- **Leverage data assets with advanced analytics.** Banks have enormous amounts of data at their disposal, which they can leverage with analytics tools to detect trends and create KPIs from which to proactively counter cyber threats.

- **Make risk-based decisions.** Taking a holistic view of cyber threats requires elevating the problem to an operational risk, from which better decisions can be made more quickly, and in relation to the relative risk to the enterprise as a whole.

- **Achieve innovative maturity.** As cyber threats evolve in scope and complexity, so should the financial organization’s drive and commitment to innovatively manage cyber risk, both in terms of people and technology.

- **Adopt an industry-recognized cybersecurity framework.** The National Institute of Standards and Technology (NIST) and the Federal Financial Institutions Examination Council (FFIEC) have both recently released cybersecurity frameworks that are applicable to the financial industry.7
be prioritized accordingly. Implementing analytics can help financial services institutions better understand what, when, why and how threats can potentially impact an organization, and the most appropriate action to take.

To improve customer relationships while simultaneously educating them on security risks, banks must embrace all lines of communication. In addition to external education, they also need to raise internal awareness. Indeed, “human behavior” is often cited as a key gap in cybersecurity among banks; for example, unless properly and consistently trained on security protocols, employees are often careless about their use of USB devices and public Wi-Fi connections. Danske Bank, which has over 20,000 employees across almost 10 countries, has learned from experience; when the bank introduced laptops to employees, it also made sure they were all encrypted.

In the end, achieving strong cybersecurity preparedness requires good technology, the right organizational structures, strong cooperation, legal support and investment (see Quick Take, opposite page).

Know when to insert the human touch.

Online and mobile channels are clearly the future of banking, particularly for digital natives but increasingly for all generations of bankers who seek the cost savings and convenience of self-service apps. According to a 2014 survey by Bank of America, nearly six in 10 (58%) respondents have used mobile check deposit; interestingly, nearly half of respondents in the 35-plus age category use this service. Banks need to combine a mobile-first mindset with a big data sensibility, as banking transactions ultimately shift into a customer experience that is similar to using Amazon’s or Netflix’s highly curated and individualized menu.

However, when problems arise with these self-service channels, reputable banks need to know – using customer Code Halos – when individual customers prefer to engage with a service representative and provide that capability at the tap of a call button.

Consider a rebirthing strategy.

In some cases, a bank’s reputation is too ingrained for it to be perceived in a new light, and in those cases, a re-branding strategy is the best course of action. For instance, some banks have created a “bank within a bank,” reinventing their brand by developing a startup operation that can act more quickly and aggressively than the legacy institution can, enabling it to compete with new nontraditional competitors. When taking this approach, banks can use the startup to target a particular demographic or banking specialty.

An example is BRE Bank, which launched mBank in 2000, a pure-play online bank. After a rapid rise to Poland’s biggest online bank and third largest retail bank, mBank expanded into the Czech Republic and Slovakia in 2007. In 2012, BRE invested $31 million in a complete redesign of the bank to accommodate the new trends in real-time marketing, personal financial management, mobile banking and social media. At that point, it officially changed its name to mBank and adopted the online bank’s brand, focus and look-and-feel.

Looking Forward

With all the changes that have occurred since the 2008 downturn, more turbulence is ahead for consumer banking. The key to remaining relevant amidst the constant change is rebuilding consumer trust. By making consumers the centerpoint of their strategies and operations – and focusing on convenience, personalization, security and digital approaches to banking – banks can be heard above the noise of new competitors and provide an experience that inspires customers to return, again and again.

Note: Code Halo™ is a trademark of Cognizant Technology Solutions.
Footnotes


5. In April 2013, Charles Blauner, the chair of the Financial Services Sector Coordinating Council (FSSCC), wrote in a letter to the National Telecommunications and Information Administration: “Financial services are built upon trust from our clients, trust between our firms and the trust required to ensure the proper functioning of markets, execution of transactions and protection of information.”

6. According to the 2013 Internet Security Threat Report from Symantec, there was a 58% increase in mobile malware compared with a year earlier, and a 32% increase in the number of reported vulnerabilities in mobile operating systems during the same timeframe.

7. In February 2013, President Obama issued an executive order for NIST to develop a voluntary framework for reducing cyber risks to critical infrastructure (http://www.nist.gov/cyber-framework/). The FFIEC developed the Cybersecurity Assessment Tool to help institutions identify their risks and determine their cybersecurity preparedness. The assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.


Author

Steven DeLaCastro leads Cognizant’s Banking and Financial Services business unit’s global “Bank of Tomorrow … Today™” digital banking program. With a wealth of expertise in bank technology and operations, software, services and consulting, he has held the titles of Chief Information Officer, Chief Operating Officer, Senior Vice-President, Managing Director, General Manager, EMEA Sales Director, Regional Country Manager, Partner and Managing Partner. Steven holds an M.B.A. and a BSc. in business administration with concentrations in operations, finance and psychology. He can be reached at Steven.DeLaCastro@cognizant.com | LinkedIn: www.linkedin.com/pub/steve-delacastro/0/240/309.
About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world's leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work.

To learn more about Cognizant, please visit: www.cognizant.com.

U.S. Headquarters:
211 Quality Circle
College Station, TX 77845
Tel: +1 979 691 7700
Fax: +1 979 691 7750
Toll Free: +1 855 789 4268
Email: inquiry@cognizant.com

India Operations Headquarters:
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com

China Operations Headquarters:
Cognizant Technology Solutions (Shanghai) Co.
Zhangjiang Hi-tech Park
Building No. 5, No.
3000 Longdong Avenue
Shanghai, Pudong China 201 203
Phone: +86 21 6100 6466
Fax: +86 21 6100 6457
Email: inquirychina@cognizant.com

Global Delivery Centers:
Budapest (Hungary), Buenos Aires (Argentina), Guadalajara (Mexico), London (UK), Manila (Philippines), Shanghai (China), Toronto (Canada); Chennai, Coimbatore, Kolkata, Bangalore, Hyderabad, Pune, Mumbai, New Delhi, Cochin (India); Bentonville, AR; Boston; Bridgewater, NJ; Des Moines, IA; Minot., ND; Phoenix, AZ; Tampa, FL (U.S.).

Regional Offices:
Atlanta, Boston, Chicago, Dallas, Los Angeles, Norwalk, Phoenix, San Ramon, Teaneck (U.S.); London (Canada); London (UK); Frankfurt (Germany); Paris (France); Madrid (Spain); Helsinki (Finland); Copenhagen (Denmark); Zurich, Geneva (Switzerland); Amsterdam (The Netherlands); Hong Kong, Shanghai (China); Tokyo (Japan); Melbourne, Sydney (Australia); Singapore (Singapore); Bangkok (Thailand); Kuala Lumpur (Malaysia); Buenos Aires (Argentina); Dubai (UAE); Manila (Philippines).