Cybersecurity at MIT Sloan
Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity
Case Study

Cybersecurity Culture at C6 Bank[1]

October 14, 2020
Dr. Keri Pearlson
Madeleine Li
Sarah Chou

In early 2018, Marcelo Kalim, Leandro Torres, and Carlos Fonseca, all former executives of Brazilian Investment bank BTG Pactual SA, seized on the opportunity to create C6 Bank, a completely online bank in Sao Paulo, Brazil, providing financial services via a mobile application alone. Building the entire operation from scratch, the team obtained approval from local regulators, built out a new office space, created the necessary IT infrastructure and designed their mobile app. Much like the start of the bank itself, its founders were able to build a fresh, new approach to organization culture to drive daily operations and their approach to work. CISO Jose Santana and CTO Nelson Novaes Neto sought to build cybersecurity values into the company's culture by taking steps to create beliefs and attitudes about the critical importance of everyone keeping C6 Bank secure. They hired Anchises Moraes as the cybersecurity evangelist, responsible for driving this culture throughout C6 Bank. The bank opened to public enrollment in August 2019, and a short seven months later, in March 2020, the COVID-19 pandemic forced many companies in Brazil to transition to a remote workforce. C6 Bank managers found themselves rebuilding their organization to accommodate this new way of work. The cyber security and the executive team wondered how to modify their approach to build a cybersecurity culture when everyone was working from home.

Background of Brazil

Banking in Brazil

The Brazilian banking industry was traditionally dominated by five large banks, split between the private and public sector. The market was incredibly concentrated. A report by the Banco Central Do Brasil (Central Bank of Brazil) shared that the two public banks held a large share of the market: Caxia held the greatest share at 31.8% and Banco do Brasil held 18.9%. In 2013, the ten major banks held over 87% of the total assets and deposits in Brazil.[2] In 2019, the five biggest banks in Brazil held 82% of the assets (as compared to the US, where the top banks held 43%).[3]

The Brazilian banking industry saw tremendous growth from 2018-2020. The landscape of banking was primarily impacted by the rise of digital services, and specifically financial technology companies, also known as fintechs. One example of a fintech was Nubank, an online credit card company founded in 2013 that influenced further growth of this market.[4] The growth

---

[2] "Banking Sector in Brazil." March 2014. https://www.emis.com/sites/default/files/EMIS%20Insight%20-%20Brazil%20Banking%20Sector%20Report.pdf

[3] "Brazilian online bank C6 reaches 200,000 clients." August 5, 2019. https://www.reuters.com/article/banco-c6-sa-plan/brazilian-online-bank-c6-reaches-200000-clients-idUSL2N2510UT

[4] "Fintechs target Brazilian banks' fat margins." August 22, 2017. https://www.ft.com/content/78058d7c-7c90-11e7-9108-edda0bcbc928

of technology and rise of fintech companies led the five major banks to improve their digital services, offering an online credit card and online payment methods in addition to traditional banking products.[5] Even with this growth however, there were still approximately 60 million Brazilians who did not have banking services.[6]

The government in Brazil highly encouraged banking industry growth, according to Nelson. He explained,

> Existing Banking regulations in Brazil are very strict. Sometimes they are difficult to follow making it challenging to get compliance and making it very difficult to launch a new bank operation in the country. On the other hand, the government wants more banks created because it's good for all to have stronger competitors. The analogy I like comes from looking at taxis and Uber. Before Uber came to Brazil, the price of a taxi was incredibly high. Then Uber came along charging considerably lower prices for a better service, so taxis improved their quality of service in order to maintain customers. The banking industry operated in the same way. If a new bank comes along offering different or better products, other banks will be encouraged to improve their services.

Cybersecurity in Brazil

Similar to other countries, Brazil experienced significant cyber threats in their financial sector in recent years. In 2018, the malware CamuBot targeted banking customers in Brazil through phishing campaigns.[7] The malware hid itself as a safe function that looked like something customers had to download. Another malware, BasBanke, targeted financial data and credit card numbers, taking advantage of the many social media users by disguising itself as an advertisement on Facebook and WhatsApp for operations such as QR readers.[8] These malware programs were difficult to recognize and nearly unavoidable for every-day users. When asked about the source and severity of cyber-attacks in the country, Nelson explained that, "criminal groups are strong in Brazil, and malware often starts there. It doesn't take much for these criminals to make a lot of money from an attack."

The Brazilian country had a culture that influenced C6 Bank executives' approach and attitudes about cybersecurity. Even though the number of digital services and internet users continued to rise, Brazil public leaders had not really done much to educate the population on measures to teach or ensure safe cyber habits. A report in 2014 by Avant highlighted that 65% of all wireless users in the country still used the default username and password.[9] Other reports show similar statistics, such as a Symantec report that noted that most adults connected to unsecure networks and failed to delete suspicious looking emails that might include dangerous attachments.[10] Brazil was one of the lowest scoring countries for cultivating a mindset of cybersecurity, according to a 2016 report

[5] "Fintechs target Brazilian banks' fat margins." August 22, 2017. https://www.ft.com/content/78058d7c-7c90-11e7-9108-edda0bcbc928
[6] "Cybercrime: 25% Of All Malware Targets Financial Services, Credit Card Fraud Up 200%. April 29, 2019. https://www.forbes.com/sites/zakdoffman/2019/04/29/new-cyber-report-25-of-all-malware-hits-financial-services-card-fraud-up-200/#38ccaf87a47a
[7] "CamuBot: New Financial Malware Targets Brazilian Banking Customers." September 4, 2018. https://securityintelligence.com/camubot-new-financial-malware-targets-brazilian-banking-customers/
[8] "BasBanke: Trend-setting Brazilian banking Trojan." April 4, 2019. https://securelist.com/basbanke-trend-setting-brazilian-banking-trojan/90365/
[9] "Largest Cybercrime Threats in Brazil." April 8, 2015. https://techinbrazil.com/largest-cybercrime-threats-in-brazil
[10] "Largest Cybercrime Threats in Brazil." April 8, 2015. https://techinbrazil.com/largest-cybercrime-threats-in-brazil

from the Cybersecurity Observatory for Latin American countries.[11] Awareness and investment in cybersecurity in Brazil was growing but not fully mature by 2019, when C6 Bank began operations.

Background of C6 Bank

C6 Bank was founded in 2018 by a group of 25 Brazilian executives from the financial and technology industries, and received approval and licensing by the Central Bank authorities in early 2019.[12] Early on, the visionary founders realized that customers want personal financial products that met their individual needs, but with mass audience advantages and high quality. For C6 Bank, that translated into standard banking services such as demand accounts, savings accounts, credit cards, and loans, but at the low cost and personalization that was only achieved at 'scale.' This was an innovative idea for banking in Brazil. "We want to surprise customers with a true relationship and a transformational banking experience," commented Nelson.

After a beta launch with family and friends test resulted in 1000 new accounts, C6 Bank officially opened with campaigns to the general public on August 5, 2019. The bank saw strong growth in the first 9 months, with nearly 6,000 new accounts opening every single day and approximately 2 million accounts had been opened by May 2020. Customers covered 99,5% of the 5,570 Brazilian cities. Employee numbers were also growing, from just the 25 founders in late 2018 to 600 employees on launch day, mostly in technology and development.

Unlike other financial institutions in Brazil at the time, C6 Bank operated exclusively online and had zero physical branches. A number of other features also separated C6 Bank from the competition. Of most significance was the way C6 Bank bundled multiple financial services and made them available in one application on a smartphone with strong focus on the user's experience. The bank was recognized for their user experience in 2019 and again in 2020 when C6 Bank's app was selected as the banking app with best user experience for their onboarding process[13]. When asked about what made C6 Bank unique, Nelson explained (see Figure 1),

> C6 Bank is for all people in Brazil, in all segments of the Brazilian population. With lower costs and increased personalized offerings, the banking experience appeals to everyone. It is our goal to develop transparent, trusted banking relationships with our customers. C6 Bank is more than a fintech and different than the incumbent banks, so it's really in a unique position to offer the best solutions for our customers. There also isn't really a culture on how to manage money in Brazil, so we have an opportunity to educate all classes of people on how to manage their money.

C6 Bank's primary goal was to "transform the banking experience" by distinguishing itself from traditional Brazilian banks. Opening an account at C6 Bank took less than 5 minutes to set up, whereas it took much longer at traditional banks. One way C6 Bank was able to do this and avoid fraud was by cross-checking personal information with other databases instantly. Further, customers felt more control of their banking experience since the C6 Bank app gave them the option to personalize nearly everything, from the color and the name printed on their credit card

[11] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf
[12] "A New Era For Blockbuster Bank M&A." February 8, 2019. https://www.spglobal.com/marketintelligence/en/news-insights/blog/a-new-era-for-blockbuster-bank-ma
[13] This report is available online in Portuguese: https://idwall.co/analise-de-mercado-bancos-digitais-s1-2020/

to the set-up of the application's navigation page. The app was also designed to be highly user friendly. The bank's website highlighted the company's dedication to clarity and transparency. Transferring money between accounts or making payments from an account was simple, further impacting the customer experience. Customers needing assistance could reach customer service at any time, 7 days a week, 24 hours a day. To further build trust and confidence, C6 Bank had back up processes using human operators in the event the application was not working. C6 Bank sought to be known as the bank with simple solution for customers (See Figure 2). [14]

The bank's products and unique offerings were influenced by the core ideals and values of the founders. Even the name, C6 Bank, took its inspiration from the sixth element in the periodic table, carbon, which has 6 protons, 6 neutrons and 6 electrons and can bond with other carbon molecules easily and seamlessly. The carbon atomic structure is also the inspiration for many elements of C6 Bank; Their offices have many hexagon shaped tables, door openings, windows, and other physical elements. Their work is driven by 6 ideal that are displayed on a hexagon created by one of the founders, Luiz Marcelo "Teco" Calicchio (See this framework in Figure 3). The six ideals are:

- Authorcracy- a word shaped by C6 Bank executives to represent and to advocate power to individuals' own ideas.
- Breaking the status quo- the idea of being different than the traditional Brazilian banks
- The art of disagreeing- refers to understanding the origins and reasons for the idea you are about to disagree with
- Good humor/mood- creating an environment where people like to work and bring their positive outlook to work.
- Respect/Ethics/Transparency- the bank will operate in a manner that reflects respect of individuals (customers and employees), transparency (to insure stakeholders really know what is taking place), and ethics (operating in a manner consistent with doing what is right for the customer/employee). This last ideal is purposely at the base of the hexagon to indicate it is the base of everything else.
- *Frescobol,* a reference to a Brazilian paddle-ball-like game where everyone works together to keep the ball in the air. This ideal refers to everyone helping out and no one person tries to take credit or 'win'.

Leaders envisioned a bank that was also a way of life, embodying the ideals and values of the generation of customers they targeted. By articulating their values in this way, they hoped to invite customers into their business in a new and engaging way.

Company Corporate Culture

The general culture at the bank reflected Brazilian society--relaxed, non-traditional, open and friendly. Their offices were located in a new, 8-story building in the heart of Sao Paulo. The office space was designed by award winning architects at Perkins&Will to reflect the company values and bring the feeling of a silicon-valley startup. (see Figure 4) There were no cubicles, and all team members worked at open tables. There were break out spaces, stocked kitchens, areas for relaxing and socializing, and more. Their offices were decorated with graphics and signs on many of the walls and hallways. For example, building pillars displayed one the company's core values (see Figure 5).

Though a more traditional organizational hierarchy existed to run the business, the open culture included many activities that crossed department and hierarchical levels. For example, all employees regardless of role attended a weekly all hands meeting, called "open mic," a place to

[14] https://www.c6bank.com.br/

share announcements, to introduce new hires and to discuss critical company issues. In one meeting, all C6 Bank employees openly discussed the company's culture and idea sharing. Any employee could suggest a topic for discussion and have it added to future open mic meeting. Frequently, topics about cybersecurity were brought up by the cybersecurity team and presented by Anchises. At the end of the meeting, all employees were encouraged to send questions or topics that would be discussed at future open mic meetings. Additional group activities to build a shared culture included a "6 min meetings" hosted on the last Friday of every month for a couple months in 2019 and organized by HR, where employees could talk about any topic they wanted to discuss. Frequently topics were not related to bank operations; employees frequently talked about hobbies, vacations, and good restaurants.

Cybersecurity at C6 Bank

From the very beginning, cybersecurity was incorporated into the bank and its operations, plans and strategies. The first employee Nelson hired at C6 Bank as a CTO, was a member of the security team. The Chief Information Security Officer (CISO), Jose Santana (Figure 1), elaborated,

> From the very beginning of the bank's online operations, we had attempts at fraud, hacking, and social engineering. In fact, one of our executives had his credentials stolen early on and we had to figure out how to make sure no damages were done. We had to figure out our security posture and plan for security issues from the very start.

Since core ideals of the bank included transparency and ethics, gaining trust was critical for the bank to be successful. The founders knew that and that drove a deep and fundamental desire to build cybersecurity into every aspect of operations. According to Jose Santana, this focus on ensuring the company's security at all levels from the beginning created a key aspect of the company's culture. Jose shared his thoughts,

> Everyone at C6 Bank is responsible for cybersecurity. It's in the mind of every Csixer[15]. We are building the whole company with everyone helping to keep the company secure from the beginning. This is different than other companies who build a cyber culture within an established culture. We are building the company's culture and cybersecurity culture together. Frankly, there is no difference in our culture and our cyber culture; there is only C6 Bank culture and cybersecurity is a part of it. This is our employee mindset.

The cybersecurity organization at C6 Bank had five major teams (see Figure 6 for the organization structure of the security team reporting to Jose). The five teams included:

1. Cyber Defense Center- included the cybersecurity operations team, who monitored, investigated and handled all incidences, threat intelligence, etc.
2. Engineering- consisted of security architects who supported the product development team. The team was also responsible for establishing information and cloud security best practices.
3. Cyber governance, risk, compliance, and access- focused on risk management, audits, and compliance within the company. The team also managed the access control and user identity to C6 Bank.

[15] "Csixer" is how C6 Bank's employees refer to themselves.

4. Applications security and offensive security- defined requirements, controls, tests and solutions to aid and respond to threats from a potential hacker. The team also ran security checks on C6 Bank applications and infrastructure, including penetration tests.
5. Cyber Culture and Awareness- built and evangelized the information security culture (headed by culture evangelist Anchises Moraes).

Security Strategy

Building a security strategy was critical for C6 Bank, and they relied on best practices from the banking and other industries. Since the roots of the founders of C6 Bank were primarily from financial services companies, they knew a lot of colleagues in the industry with whom they shared information about breaches and vulnerabilities. Breaches were newsworthy stories and this provided a foundation for discussions among financial industry professionals. External security and banking industry events, vendors, academics and professionals were all resources that influenced the security strategy. They also followed standard security reference models such as the ISO[16] and NIST[17] models to structure security plans. In addition, traditional and more recent security concepts were adopted. One approach included in their core design was the concept of zero-trust, which start with the premise that no one is trusted. This means that there is no 'perimeter' to penetrate because every access attempt must be accompanied with appropriate credentials and identification. At no time is authorization passed between components of the system; user must be identified and authenticated each time.

Managing risk was key to their security strategy. C6 Bank used a 3-layer risk control model:

- First was the operations/technology/information security layer: End points of their network were hardened. All possible layers of defense were employed including bug bounty program, antivirus software, identity management and firewalls. All software was kept up to date and patched with the latest versions. Controls were put in place.
- Second was their risk and compliance layer: Every process was examined closely and tested regularly to insure everything was following compliance policies. Further any risks that were identified were required to have a plan to reduce, eliminate, or mitigate it.
- Third was their internal audit layer: Auditors were used to insure the environment was secure through processes to validate and insure vulnerabilities were appropriately managed.

Security was the bank's number one priority when building products, as noted by Jose who remarked that "the goal of the C6 Bank product design strategy was to mesh security with our agile development process." The process for developing products incorporated deep testing of vulnerabilities due to potential threats, and critical components of security were designed and tested in each phase of the development process.

To heighten security, C6 Bank built their own mobile banking app with proper controls and shields. Customers could not access the C6 Bank online banking system using standard browsers, they had to use the C6 Bank mobile application downloaded from the official iPhone or Android store. There was no host website available to use; customers who went on the C6 Bank website were

[16] https://www.iso.org/isoiec-27001-information-security.html – ISO 27001 is the international standard for best-practice information security management. It is a rigorous and comprehensive specification for protecting and preserving your information under the principles of confidentiality, integrity, and availability.
[17] https://www.nist.gov/cyberframework – The NIST Cybersecurity Framework is a voluntary framework primarily intended to manage and mitigate cybersecurity risk for critical infrastructure organizations based on existing standards, guidelines, and practices.

directed to a download page for the app, rather than have access to the bank's services. Though this did not leave the company immune to malware attacks, it added a level of security to their online banking operations.

Engaging Everyone in Cybersecurity Training and Awareness Programs

Training and awareness of the importance of cybersecurity started when employees were hired, regardless of their role or standing at the bank. The message was delivered to all employees, including individuals in departments such as marketing or human resources. From day 1, employees participated in onboarding activities and presentations about the bank's culture and keeping the bank secure. Employees learned the bank's security policies and regulations and participated in training programs that focused on ethics and risk management. In general, the onboarding process ensured that every employee was familiar with cyber threats and how to handle potentially risky situations. Upper management did not just endorse the training, they were active participants as well. They took the same training when they onboarded and participated in cybersecurity activities as part of their management responsibilities.

The C6 Bank cyber culture plan also included activities to reinforce the messages from the training sessions. C6 Bank managers employed "recycling." Recycling were activities that constantly reminded employees of policies, regulations, and other concepts from learned in training such as reporting suspicious emails or creating complex passwords. Cyber issues and breaches in the news were also incorporated into the communications campaigns to keep everyone informed and prioritizing the safety of the bank. Some employees eventually move into specialized cyber training, on topics such as PCI compliance and the Brazilian Personal Data Protection Regulation (Lei Geral de Proteção de Dados Pessoais – LGPD) that comes into effect in 2020.

The third part of the cyber plan incorporated an aspect of "fun" into this traditionally serious subject matter. Under the moniker "integrated awareness," thematic campaigns such as "cybersecurity week," "data privacy day" or "Ada Lovelace day" focused on strengthening the company's awareness of cybersecurity, as well as other relevant technical topics. IT and security teams hosted public events in partnership with local technical communities such as meetups and hackathons. They established relationships with a larger community of professionals in Sao Paulo through hosted breakfasts, public talks or happy hours, kid mentor programs, blog posts on important cyber news, and contests. The bank managers also employed and encouraged the use of tools to promote safe practices such as phishing exercises, web-cam protectors, and shredders placed closed to printers. These tactics seemed to work. One executive commented,

> One time an iPhone was stolen and the thief sent notes to several people in the bank encouraging they to share the credentials to unlock the phone. The thief was clever and disguised the way he asked for this information, but no one fell for it. No one gave him the credentials.

Behaviors were reinforced with simple rewards and recognitions. In a phishing test sent to a random group of 100 employees, 20 reported their suspicions to the cyber team. To recognize these individuals for reporting the email, the cyber team rewarded them with a cookie. While the reward was simple, the impact was great. Future phishing test success rates improved and employees reported that getting a cookie was a welcome reward.

On the other hand, when employees exhibit behaviors that might open up vulnerabilities for the bank, managers imposed consequences that focused on education rather than punishment. The offender would be required to meet with the security team to help identify the security controls that were missed, and to be reminded of the company policies learned through onboarding or subsequent lessons. Further, the security team would reiterate the risks to the bank should this behavior continue. For example, in the same phishing test mentioned previously, two people accidentally clicked on the tainted email, one of which sat next to the security team's desks. Rather than punishing her in formal employee evaluations, the C6 Bank team used respectful humor to reminded her of her mistake. This had the effect of delivering the important message but without harsh consequences and was well received, since humor is a big part of the C6 environment. When asked about consequences to employees should they display behaviors that open up vulnerabilities, Jose stated that "we just want to share information in an easy and fun way. That is consistent with our company values. Negative consequences might also get the job done but it's not the C6 Bank way."

Executive Involvement and Participation

Executives played a big role in promoting the culture of cybersecurity. Since everyone at the bank was new, executives came from many different backgrounds and some were unrelated to technology. They initially thought cybersecurity was something that the IT department handled. But the C6 Bank culture required executive participation in keeping the bank secure. Because of the focus on security, all executives was the benefits from of cybersecurity activities and that sparked further executive engagement. The executives were offered webcam covers and many asked for more to give to their colleagues, friends and families. Furthermore, executives were continually made aware of security issues in the news and that helped reinforce the need to keep C6 Bank secure. For example, when the WhatsApp breach occurred, it was a major topic of discussion at several C6 Bank meetings, driving consensus about avoiding its use for C6 Bank business communications. Executive involvement sent a clear message to the organization that cybersecurity was a priority.

Even the top executives set an example. The executive committee did not want to be the weakest part of the bank's cybersecurity strategy, so they asked the cyber team to keep them constantly updated with cybersecurity news. This enabled top executives to engage in random conversations with other C6 Bank team members about cyber issues and common best practices, such as not having a conversation that included confidential information in the elevator or in any public space. This set an example of the priority the C-level executives put on cybersecurity.

Using the Local News to Make the Point

Employees at C6 Bank were deeply interested in keeping up with the latest news and had frequent discussions about topics of interest. Anchises leveraged this interest to keep cyber news front and center, too. For example, after the WhatsApp hack in May 2019, the cyber team used the incident as a teaching moment for the rest of the company, making the vulnerabilities to the bank clear to everyone. Executives reinforced the message to replace WhatsApp with a more secure application since phones and computers could easily be infected by the malware embedded in the WhatsApp breach. Anchises, as the cyber evangelist, regularly initiated communications campaigns using emails, posts on the intranet, and broadcasted videos on TV screens in the cafes to highlight cyber content, reinforce cyber policies, and to encourage cyber secure behaviors.

In one humorous example, Anchises placed reminders about the dangers of using WhatsApp on Post-It notes and posted them in some bathroom stalls. This had the desired effect of catching employee attention; many employees took photos and shared them with their friends further spreading the important cyber security message. Since Post-It notes were effective in spreading that key message, Anchises incorporated it into his next communications plan about managing passwords. He planned to create Post-It notes with commonly used passwords and post them around the building to highlight the importance of using unique, more complicated passwords for security. Unfortunately, the COVID-19 Pandemic in 2020 forced Anchises to put this campaign on hold.

Employees regularly took an active role to ensure that all risks were managed, even taking steps that went beyond their individual role in the bank. Anchises explained,

> If I see a computer left on or open for anyone to access, I open a word document, type a note on it, and then lock the computer screen. This is a friendly way to remind the employee to not to leave their screen open next time. One time, I found a computer in an empty meeting room, so I brought it to my desk and sent a message in Microsoft Groups for someone to come and claim it. If there's a document on a printer with any important information, I make sure to bring it to the person or to shred it.

Collaboration across the company was a major goal for the cyber team at C6 Bank. The team promoted the idea that all departments should engage with cybersecurity efforts, and the company had already seen benefits. For example, the legal team at C6 Bank frequently came to the security team for help; when they needed support with their contracts, they checked with the cyber security team to ensure that they were following safe practices. They also involved the security team during contract negotiations to be sure that contracts contained appropriate policies and practices. In addition, the marketing team initiated and posted security messages on the company's intranet. When an employee received a suspicious email message, they regularly asked cyber team to check it out and make sure it did not contain malware. The cybersecurity team regularly observed behaviors that indicated the awareness plans were working

Measuring Effectiveness

The campaigns, executive involvement, rewards, consequences and other activities designed to reinforce the idea that security was important to C6 Bank appeared to be impactful. However, specific and measurable performance metrics to evaluate and communicate the success of the cybersecurity culture were needed. As of December 2019, approximately 93% of employees had gone through cyber training but that was not a complete indicator of the success of these efforts, which expanded beyond training. The page views of intranet posts, the number of incidents occurring and reported, the data from the phishing exercises, and training completed were the only metrics available. Anchises planned to work with the cybersecurity team to create and collect data for additional meaningful metrics for measuring security awareness effectiveness. This was an emerging priority for the bank.

The Impact on C6 Bank from the COVID-19 Pandemic

In March of 2020, the COVID-19 pandemic hit communities all over the world. The Brazilian economy, like many world economies, struggled during this time.[18] When asked about the impact of the pandemic in the banking sector in Brazil, Anchises remarked,

> Many banks were forced to close their physical branches to adhere to social distancing rules and had to move their workforce to their homes. Local economy shrank since many Brazilian workers lost their jobs, resulting in loss of income and putting their financial lives at risk. The lack of income made Brazilians visit banks looking for low-interest loans. There were specific low-interest loans offered by Brazilian banks to government employees and retired persons. The closure of bank branches and increased demand for loans and access to governmental unemployed insurance program (similar to US stimulus checks) drove up demand for banking services, particularly for an online bank that was able to complete all transactions remotely and had zero transaction fees. C6 Bank saw higher levels of growth in customer enrollment. Indeed, C6 Bank grew 150% between January and July 2020. But we were impacted in other ways. We had to rethink our own office space utilization and our operations as we implemented social distancing for our own employees, moving 90% or more of our CSixers to home.

COVID-19 forced many companies to find ways to social-distance their employees, and many scrambled to create a work-from-home (WFH) workforce. C6 Bank was able to adopt the WFH strategy since its systems and infrastructure were relatively new and already utilized the cloud environment. In addition, all employees had near-brand new laptops with the latest software on them. Anchises elaborated,

> Before the pandemic, employees were already fully-equipped to work from home, so we were prepared for this new way to work. However, managers preferred to have employees physically in the office, because collaboration was easier and managing a team was easier in person. But our team members were able to make the transition to WFH pretty easily. In fact, right after the transition, C6 Bank saw an increase in productivity from its employees.

In early 2020, Anchises had prepared a number of monthly cybersecurity awareness campaigns, including hiring a Brazilian robotics company to deploy a robot to wander C6 Bank headquarters with a tablet for employees to check their password strength. However, once the pandemic began, most of these campaigns had to be scrapped. No one was in the office, so office-based activities and communications (such as the plans to expand the use of Post-It notes) would be ineffective if not impossible.

Instead, Anchises was tasked with keeping C6 Bank employees informed about novel cybersecurity threats related to the at-home workplace and finding new ways to deploy his campaign to keep C6 Bank secure. One way he did this was by utilizing the company intranet: C6 Bank already had created a page filled with news and announcements, including curated news articles of pandemic-related information. Anchises added articles that reminded employees about cybersecurity practices. An additional section was created to cover WFH and videoconferencing best practices and security recommendations.

---

[18] "Brazil govt cuts 2020 GDP forecast to -4.7%, the biggest fall since 1900." May 13, 2020. https://www.reuters.com/article/us-brazil-economy-forecast/brazil-govt-cuts-2020-gdp-forecast-to-4-7-the-biggest-fall-since-1900-idUSKBN22P2ZJ

The new ways of working during the Pandemic were largely based on digital interaction among its employees over email, text messages via online communication tools as WhatsApp and Microsoft Teams, and video-conferences, but quickly vulnerabilities were revealed in some of these traditional communications technologies. For example, when issues arose regarding the security of Zoom, a popular video conferencing platform, C6 Bank quickly banned Zoom from all company devices and encouraged the use of Microsoft Teams. “Open mic” meetings continued, but were moved to running weekly on Teams. These included company updates and the usual discussion of company culture and critical issues, but they were increasingly peppered with security items. For example, after he alerted C6 Bank employees that cybercriminals were messaging employees and customers through Instagram Direct to gain personal information, Anchises reported that employees regularly sent screenshots of their direct messages for verification that the messages were safe and the Instagram profiles were legitimate. Furthermore, C6 Bank teams continued to hold regular “Happy Hours” after work hours, where employees chatted and drank together, but these moved to remote engagement over Teams to extend the camaraderie of its in-person workplace to the virtual world.

While they used to be part of the IT team, the cybersecurity team at C6 Bank became an independent vertical organization reporting directly to the executive team. This was envisioned to continue after the pandemic. Executives also moved the fraud prevention operations from the Risk & Compliance team to the Cybersecurity team. During the course of the pandemic, C6 Bank built a war room, where the executive team met regularly through videoconferencing, and requested weekly reports from the security team regarding new threats to the company, its employees, and its customers. They continued to make cybersecurity a priority and took extra effort to stay informed.

Next Steps for the C6 Bank Cybersecurity Culture

During September 2020 the Brazilian law known as the Lei Geral de Proteção e Dados Pessoais (LGPD), which closely matched GDPR (the EU’s personal data protection law), came into effect. As a result, the security team was rapidly transitioning C6 Bank’s products and infrastructure to be in compliance with the LGPD. This was a collaborative effort led by a Privacy Committee composed by representatives of different teams, including IT, Security, Legal, Compliance, Product, and Software Development, and others. The strategy included specific training for C6 Bank employees in this new law, which would give them a “Cybersecurity Hero” designation.

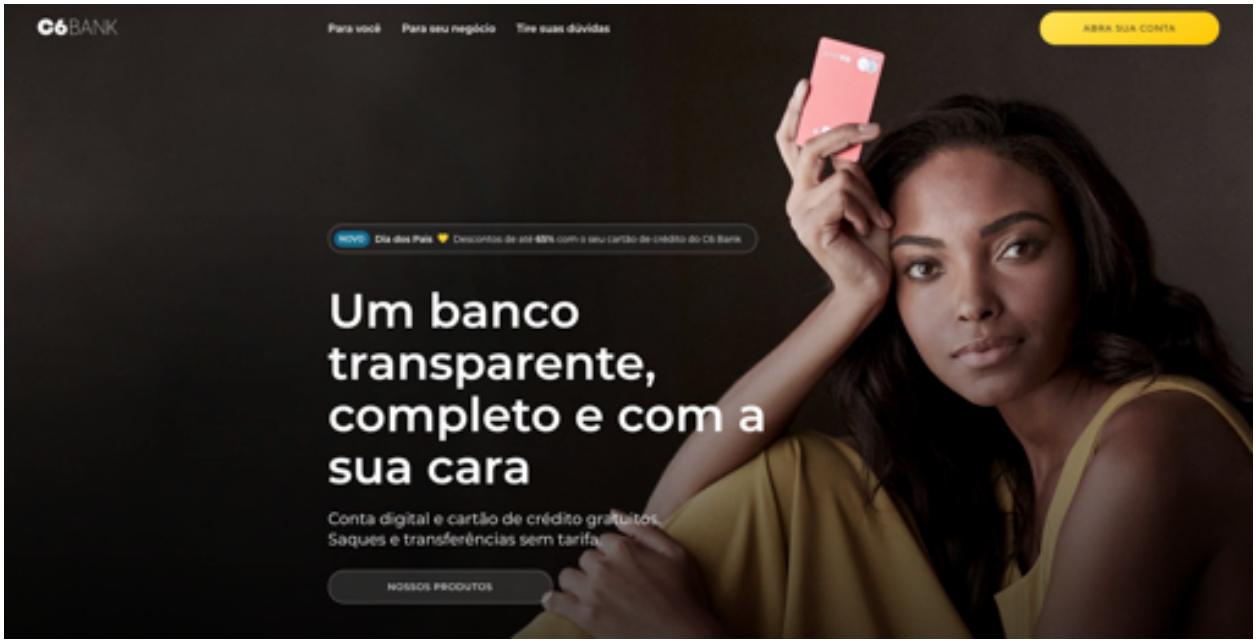
The work environment was expected to be very different going forward. After the pandemic, the executive team planned to allow remote working to continue, giving employees the choice of whether to continue to work remotely or return to the office, which would create a hybrid workforce. Other impacts were anticipated from the aftermath of the pandemic, but they were not well-known as everyone focused on the chaos and uncertainty the pandemic generated.

One thing was certain: cyber threats and vulnerabilities would continue, and the Bank would need new approaches and methods to keep themselves, their customers and their systems safe. C6 Bank wanted to plan ahead. With support from HR and Marketing teams, the cybersecurity team wondered what steps they should take to reinforce a culture of cybersecurity in the anticipated new hybrid work environment. Anchises wondered what kind of communications messaging he, Marketing and HR could create to keep both remote and in-person workers engaged in this new work environment.

Figure 1: Role and Employees at C6 Bank Mentioned in this Case

Chief Executive Officer (CEO)	Marcelo Kalim
Co-Founders	Marcelo Kalim, Teco Calicchio, Leandro Torres, Carlos Fonseca
Chief Technical Officer (CTO)	Nelson Novaes Neto
Chief Information Security Officer (CISO)	Jose Luiz Santana
Cybersecurity Evangelist	Anchises Moraes

Figure 2: C6 Bank Website Landing Page



Approximate Translation to English: A transparent and personalized bank. Free digital account and credit card. Withdrawals and transfers have no fees.

Figure 3: C6 Bank "Carbon" Culture Model

Figure 4: Photo of one of the office spaces at C6 Bank

(credit for photo: Perkins&Will, https://perkinswill.com)

Figure 5: Painting on C6 Pillar in Office

Translation: “Ethics”
(Credit for this photo: Keri Pearlson)

Figure 6: Cybersecurity Teams at C6 Bank