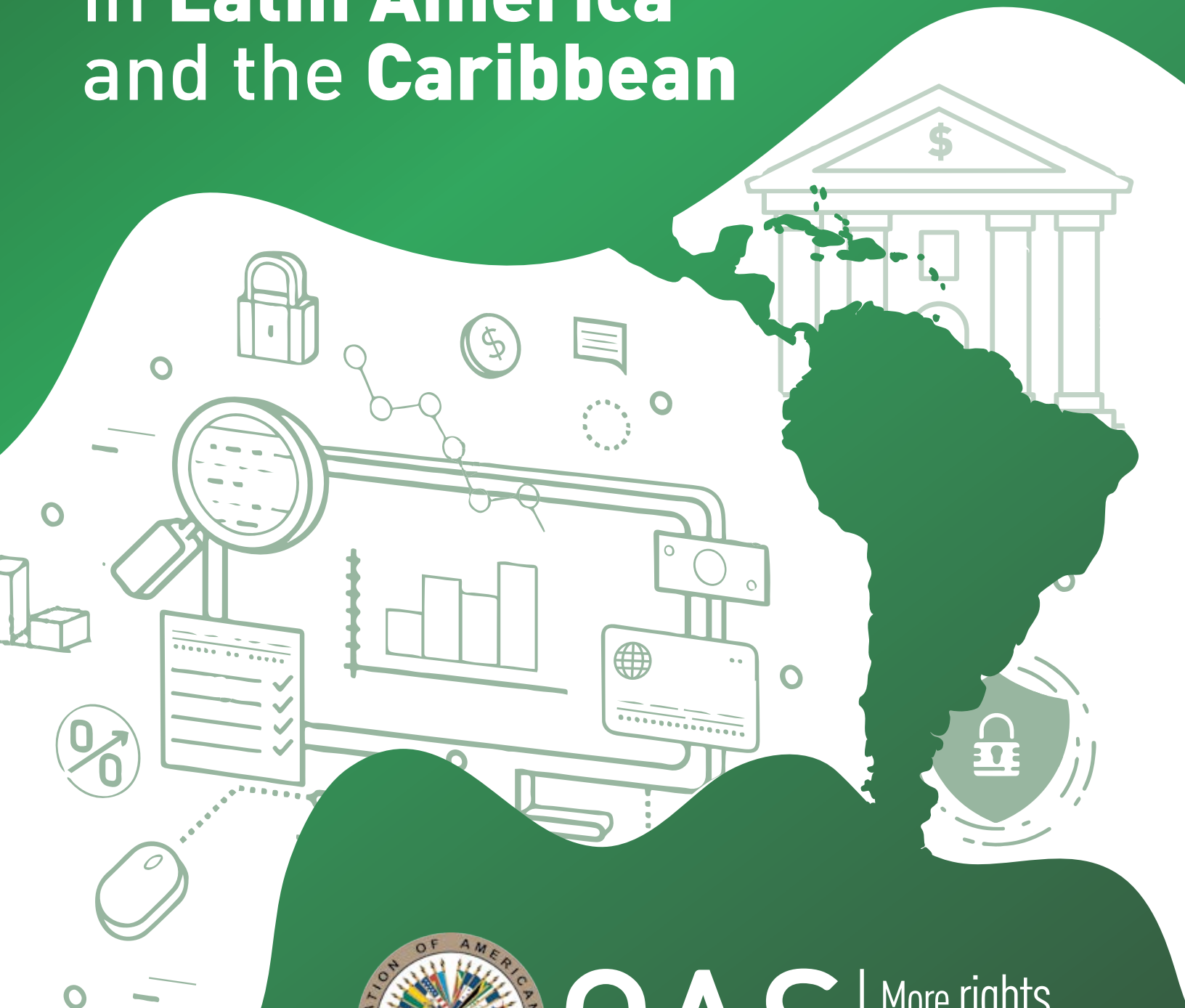
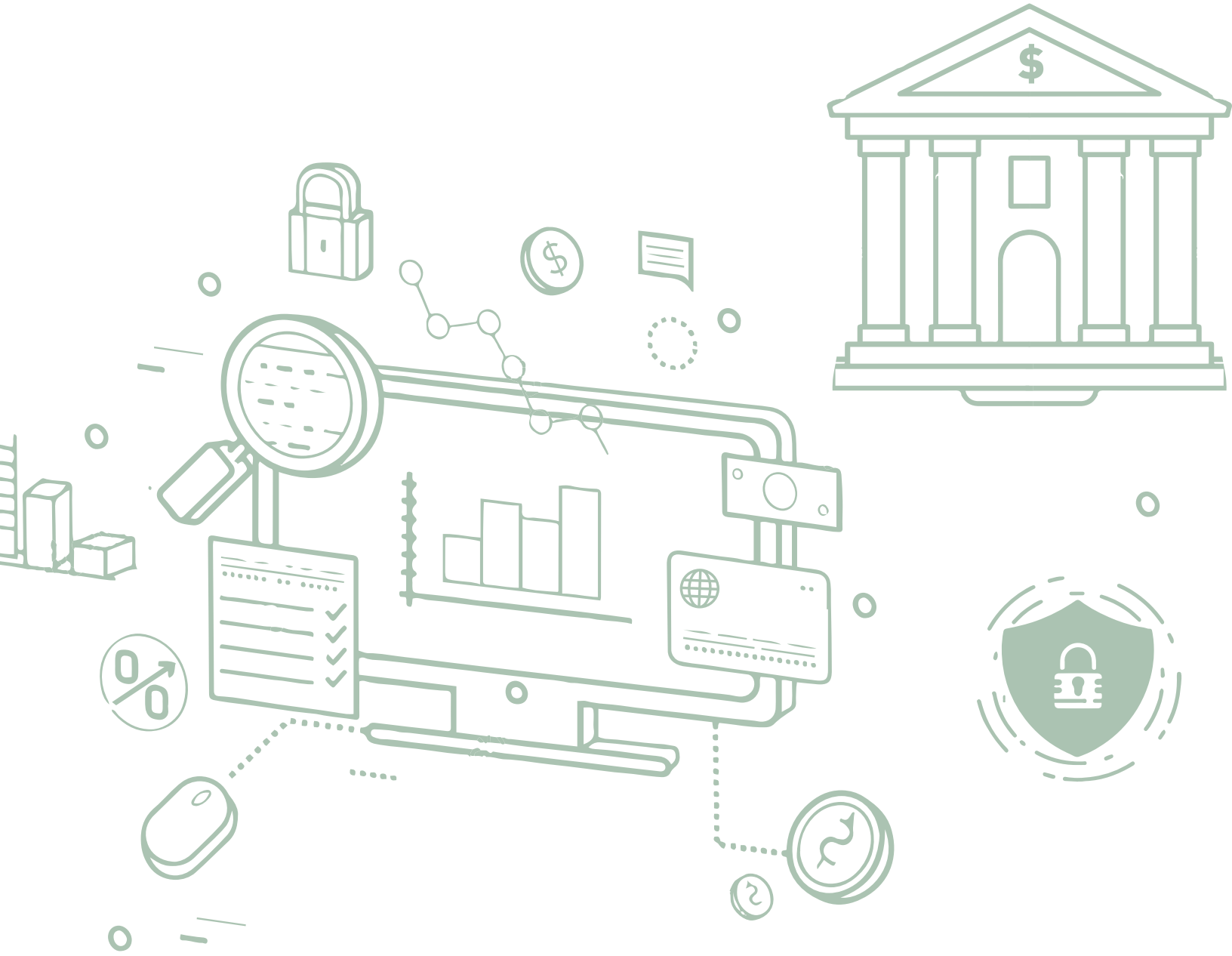
State of **Cybersecurity** in the **Banking Sector** in **Latin America** and the **Caribbean**



OAS | More rights for more people



Prepared and published by the Cyber Security Program of the Inter-American Committee against Terrorism (cybersecurity@oas.org)

Luis Almagro
Secretary General
Organization of American States

Farah Diva Urrutia
Secretary for Multidimensional Security
Organization of American States

Alison August-Treppel
Executive Secretary
Inter-American Committee against Terrorism
Organization of American States

Technical Team
Belisario Contreras
Barbara Marchiori
Kerry-Ann Barrett
Mariana Cardona
Nathalia Foditsch
Gonzalo García-Belenguer

Consulting Team
Orlando Garcés
Jorge Bejarano

Associates
Harold Coronado
Anderson Mota
José Marangunich Racchumi
César Augusto Tobón Betancur
Rodrigo Munari
José Gomes Fernandes
Fabio Moraes Benedito
Maria Teresa Tolu Brasil
Andre Salgado

This publication has been possible thanks to
the financial support of the government of

Canada

01 02 03 04

05

06

07

01

EXECUTIVE SUMMARY

This study is a contribution of the General Secretariat of the Organization of American States (OAS), which aims to provide verified information on the State of Cybersecurity in the Banking Sector in Latin America and the Caribbean. This document is yet another effort by the OAS in its task of strengthening the capacities and level of awareness in relation to the growing threats to digital security in our region.

The information in this study was analyzed in two (2) fronts. The first concerns banking entities, examining data of 191 banking entities[1] throughout the region. The other front focuses on the customers of the banking system, where the contributions of 722 users[2] in the region were studied. To conduct this exploration, the OAS, with the support of experts from the banking sector, designed specific instruments for each target group. From the observations based on the instruments used, the main findings are presented below.

Significant findings on digital security in banking sector entities in Latin America and the Caribbean:

- In relation to digital security preparedness and governance, on average, in 41% of banking entities in the region, two (2) hierarchical levels separate the CEO and the head of digital security. However, it was found that the number of hierarchical levels between the CEO and the head of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) also depend on the size of the organization. In relation to the number of areas in charge of these issues, an average of 74% of banking entities have a single area responsible for digital security.

- Regarding the support to digital security risk management (including aspects of information security, cybersecurity and fraud prevention using digital media) by the bank's top management, it is highlighted that more than 60% of the total of banking entities in the region show this i) requiring the adoption of good security practices (65%), ii) promoting training and awareness in digital security (63%) and iii) promoting digital security plans (60%).

- In 72% of the banking entities, the board of directors receives periodic reports on digital security risk indicators and management. However, 60% of those surveyed considered that convincing the organization's top management to invest in digital security solutions is moderately complex, despite the relevance of these investments, especially in terms of prevention and capacity building.

- The most implemented standards, best practices and methodological frameworks in the banking entities of the region involve ISO 27001 and COBIT standards (in 68% and 50% of the banking entities respectively).

- In terms of how teams responsible for the digital security processes are formed, it is observed that, for a typical bank in the region, these comprise, on average, seventeen (17) members. However, this value varies depending on the size of the entity.

- It is highlighted that 82% of surveyed entities in the region consider it appropriate for the team to grow in the short term, which recognizes the growing management needs on issues under its responsibility. These growing needs, in many cases, require outsourcing processes. And outsourcing

becomes the activity that is most frequently employed for the performance of security tests (65% of the total).

• In terms of capabilities for detecting and analyzing digital security events, which are vital for systematic management of this type of risk, more than 90% of banking entities in the region have implemented both firewalls and automated virus and system updates. 85% of banking entities in the region have implemented both Intrusion Detection/Prevention Systems (IDS and IPS) and Processes for Monitoring Threats and Vulnerabilities.

• Significantly, 49% of banking entities are still not implementing tools, controls or processes using Emerging Digital Technologies, such as Big Data, Machine Learning or Artificial Intelligence. These are all very important for prevention of cyber-attacks or defining suspect patterns associated with fraud, among other detection capabilities.

• The digital security risks that warrant the most attention from banking entities are: i) theft of a critical database, ii) compromise of privileged user credentials and iii) data loss.

• 92% of the banking entities report that they identified some kind of digital security event (successful attacks and unsuccessful attacks) against the financial entity. The most identified events were: i) malicious code or malware (80% of all banking entities), ii) violation of clear desk policies (63% of total banking entities) and iii) targeted phishing to access the bank's systems (57% of the total of banking entities). Also highlighted are the detection of daily malware and phishing events aimed at accessing bank systems (identified by 24% and 22% of banks, respectively).

• According to the banking entities, the events of i) phishing, ii) social engineering and iii) spyware (malware or Trojans) were the most frequently used against their financial service users, which is consistent with the statements by the users when consulted about the incidents they experienced. It is also important to note that, on average, 26% of banks detected these types of events through their own systems.

• Regarding the management, response and recovery of digital security incidents, at least half of the banking entities in the region had management, response and recovery strategies for digital security incidents.

• 37% of banking entities stated that they had been victims of incidents (successful attacks) and the main motivation for these attacks during 2017 were Economic Reasons (79% of the victim banks).

• On average, part of the digital security risk management strategies of 41% of the banks included conducting a maturity assessment. They are currently carrying out the corresponding derivative actions. Banks that fail to realize this type of assessment indicate that the main reasons are: i) insufficient specialized staff (46% of banks without the assessment) and ii) lack of budget allocation (45% of banks without the assessment).

• Regarding the communication of digital security incidents, the vast majority (88% of banking entities) offers a mechanism for their internal users (employees and contractors) to report digital security incidents (successful attacks) and 64% has a communications plan that allows to inform financial service customers when their personal information has been compromised. The majority (61% of

respondents) reports the attacks before a law enforcement authority.

• Regarding training and awareness, 82% of banking entities have preparedness, response and training plans in place, in matters of digital security for their employees and bank insourcing, which are performed mostly annually. The most effective mechanism that has generated greater awareness in banking entities, regarding digital security risks, is the development of internal information training.

• In matters concerning the impact of digital security incidents, 61% said that the digital security budget is, on average, less than 1% of the EBITDA of the previous fiscal year, 34% said it corresponds to between 1% and 5% of the EBITDA of the previous fiscal year and only 5% said that it is greater than 5% of the EBITDA of the previous fiscal year. The budget increases according to entity size.

• The budget allocated to digital security, by an average bank in the region, is equivalent to approximately 2.09% of the EBITDA of the immediately previous year. These resources remained unchanged for 46% of banks; they increased for 42% (where Regulatory Compliance aspects were the main reason for increase in the budget) and they decreased for 10% (the main reason for this reduction being the decrease in the bank's profits).

• The budget, as a percentage of EBITDA of the previous year, for entities that are Head offices in the country decreases as the size of the bank increases, while the budget as a percentage of EBITDA for entities that are a Branch, Subsidiary or Bank Agency in the country increases as the size of the bank increases.

• The digital security budget invests, in 43%, in Platforms and technological media, 22% in Human Resources, 22% in outsourced services and 13% in Capacity building. On average, the budget assigned to an average member of the digital security team was US$19,437 in 2017, an amount that varies depending on the size of the entity.

• On average, the return on investment in digital security is approximately 23.78%, which most believe is a return on average profitability.

• 73% said that the total cost of digital security incident response and recovery is equivalent to less than 1% of the EBITDA of the previous fiscal year and 27% said that between 1% and 5% of the EBITDA of the previous year fiscal.

• The total cost of responding to and recovering from digital security incidents for an average bank in the region represents approximately 1.52% of the EBITDA of the immediately preceding year, equivalent to US$1,913,000 per year, a sum that varies according to the size of the bank.

• The total cost as a percentage of EBITDA of the previous year increases as the size of the bank increases, regardless of whether the bank is Head Office or Branch, Subsidiary or Agency of the bank.

• Finally, with the figures obtained from the study, it is estimated that the total annual cost of digital security incident response and recovery of banking entities in the Latin America region for 2017 was approximately US$809 million.

Table 1. Main Results by Bank Size

LARGE BANKS	MEDIUM BANKS	SMALL BANKS
In 67% there is a single area responsible for digital security.	In 74% there is a single area responsible for digital security	In 79% there is a single area responsible for digital security
In 61% there are two (2) hierarchical levels between the CEO and the head of digital security	In 38% there are two (2) hierarchical levels between the CEO and the head of digital security	In 46% there is one (1) hierarchical level between the CEO and the head of digital security
The majority of large banks (27%) have a team comprising 16-30 members	The majority of medium-sized banks (48%) have a team consisting of 1-5 members	Most small banks (94%) have a team consisting of 1-5 members
26% are not implementing tools, controls or processes using emerging digital technologies	44% are not implementing tools, controls or processes using emerging digital technologies	67% are not implementing tools, controls or processes using emerging digital technologies
They were subject to attacks of all kinds of digital security events, highlighting the identification of almost all by the majority in the region	They were subject to attacks of all kinds of digital security events, highlighting the identification of some by the majority in the region	They were subject to attacks of some types of digital security events, highlighting identification of a few by the majority in the region
40% identified the occurrence of malware events daily	28% identified the occurrence of malware events daily	9% identified the occurrence of malware events daily
The majority (41%) detect between 61% and 80% of events with their own systems	The majority (28%) detect between 61% and 80% of events with their own systems	The majority (40%) detects between 0% and 20% of events with their own systems
65% say they were victims of successful attacks	43% say they were victims of successful attacks	19% say they were victims of successful attacks
73% carried out a maturity assessment and are currently carrying out the corresponding actions	47% carried out a maturity assessment and are currently carrying out the corresponding actions	21% performed a maturity assessment and are currently carrying out the corresponding actions
85% offer a mechanism for their clients to report incidents (successful attacks) to the entity	72% offer a mechanism for their clients to report incidents (successful attacks) to the entity	56% offer a mechanism for their clients to report incidents (successful attacks) to the entity
77% have a communications plan to inform their financial services clients when their personal information has been compromised	65% have a communications plan to inform their financial services clients when their personal information has been compromised	56% have a communications plan to inform their financial services clients when their personal information has been compromised

81% report the incidents suffered before the law enforcement authority	65% report the incidents suffered before the law enforcement authority	46% report the incidents before the law enforcement authority
57% said that the digital security budget is equivalent on average to less than 1% of the EBITDA of the previous fiscal year	59% said that the digital security budget is equivalent on average to less than 1% of the EBITDA of the previous fiscal year	67% said that the digital security budget is equivalent on average to less than 1% of the EBITDA of the previous fiscal year
The budget allocated to digital security equals approx. 1.86% of the EBITDA of the immediately preceding year	The budget allocated to digital security equals approx. 2.14% of the EBITDA of the immediately preceding year	The budget allocated to digital security equals approx. 2.27% of the EBITDA of the immediately preceding year
The digital security budget increased in 65% compared to the immediately previous fiscal year	The digital security budget increased in 47% compared to the immediately previous fiscal year	The digital security budget increased in 25% compared to the immediately previous fiscal year
The budget allocated in 2017 to an average member of the digital security team was US$22,713	The budget allocated in 2017 to an average member of the digital security team was US$21,766	The budget allocated in 2017 to an average member of the digital security team was US$13,927
The return on investment in digital security is approximately 24.1%	The return on investment in digital security is approximately 23.85%	The return on investment in digital security is approximately 23.33%
53% said that the total cost of response and recovery from incidents is equivalent on average to less than 1% of the EBITDA of the previous fiscal year	81% said that the total cost of response and recovery from incidents is equivalent on average to less than 1% of the EBITDA of the previous fiscal year	83% said that the total cost of response and recovery from incidents is equivalent on average to less than 1% of the EBITDA of the previous fiscal year
The total cost of responding to and recovering from digital security incidents in 2017 is approx. 1.86% of the EBITDA of the immediately previous year (US$5,253,000 in 2017 approx.)	The total cost of responding to and recovering from digital security incidents in 2017 is approx. 1.38% of the EBITDA of the immediately previous year (US$605,000 in 2017 approx.)	The total cost of responding to and recovering from digital security incidents in 2017 is approx. 1.36% of the EBITDA of the immediately previous year (US$161,000 in 2017 approx.)

Significant findings on cybersecurity from the perspective of users of banking sector entities in Latin America and the Caribbean:

•Users prefer virtual media over face-to-face media, which is consistent with the high degree of digitalization of services and the impulse to use them, since 53% of respondents review transactions and balances using smartphones more than what they consult at the bank (29%) or by telephone line (23%), and they also prefer to transfer funds through mobile banking (43%) than going to the bank (37%).

•The use of digital media shows evidence of an increase in the use of novel features or services: 20% of respondents already conduct mobile deposit operations (eg., a check amount can be deposited by capturing its image and the endorsement can be made using the smartphone camera); and about 7% of users already make cash withdrawals with ATM withdrawal options without a card (when, for example, the bank provides the option for a user that does not have the plastic card to request a token to the user's cell phone and make the withdrawal in an ATM).

• Services that were previously very common are displaced today by new options. The use of virtual payment methods with cards linked to Smartphones (27%) already exceeds telephone sales transactions (10%), and the percentage of use of Bitcoins as a means of payment (6.50%) already exceeds that of check payments (5.86%).

•Users are beginning to move from being "omnidigital" consumers, that is, people who prefer to interact digitally with their bank with no preference over the use of a laptop, a tablet or a smartphone, to preferring the smartphone. This analysis highlights the fact that in the case of youth (between 18 and 24 years old) the use of mobile devices equals that of laptops (39% in both cases), and in the following range (between 25 and 34 years old) it is very close (36% mobile and 38% portable).

• The degree of use of digital media to perform banking transactions reported by the users of surveyed banks is high, reaching 88%. Only 12% of users said they did not use digital media to carry out transactions. Distrust of the digital environment (59%) is the main motivation of those who do not use digital media to carry out their banking operations.

• With regard to digital security culture, most users (85%) knew many or all of the definitions referring to different types of cyber incidents; and they are kept informed mainly through news on websites, blogs and specialized sites (78.11%), as well as through social networks (66.73%). Only 40% of users are informed of the new cybersecurity threats by security campaigns carried out by their banking entities, which shows that they are not enough for the development of awareness about the threats targeting the weaker link of the chain, which is precisely the user. Similarly, it is certainly true that more and more information is available about new forms of attacks and security threats, and it is also true that they do not seem to be widespread in traditional media such as newspapers, TV and local radios, and users rated this type of media in fourth (4th) place as an information source.

• Regarding security measures implemented by users to prevent digital incidents, the most frequent was the use of antivirus on their computers (84.2%), followed by other security practices related to exclusive access on reliable computers (75.95%), enabling of transaction notifications via email (62.23%), preventing access using public Wi-Fi networks (59.79%), and the use of tokens

or complementary authentication means (53.09%).

• With regard to users' experience with digital security incidents that have compromised the bank's confidentiality, integrity or availability of information or their financial resources, 62.45% said they had not had this type of incident, while 27.30% said that they indeed had been affected and 10.26% answered not knowing and/or learning about the matter. Of the total number of affected users, the most frequent types of digital incidents were phishing fraud and social e-mail engineering with 49.68%, other types of compromise with 36.94% (not listed within the response options) and infection with malicious software with 35.67%. The frequency with which users express having been victims was: the majority (62.75%) suffered incidents of this nature only once, which contrasts with those who said having them once a month (22.88%) , once a week (6.54%) and daily (3.27%), which makes it clear that users are not necessarily aware of being affected by the occurrence of cyber incidents, because not all of them have adopted security mechanisms or measures which, among other aspects, allow them to be notified of this type of situation[3].

• The negative effect of the incidents suffered by users was the affectation to, or loss of, image on the bank (48.67%), in addition to the impossibility of timely access to the service (44.67%), the loss of financial resources (42.67%) and the exposure of their data to third parties (40.67%). Regarding the economic impact on those affected, 47% said they had not lost money, compared to 21% who said they had lost between US$101 to US$500, 15% said they had lost between US$10 and US$100, and 11% who registered having lost between US$500 and US$1,000. Of all the users who actually had economic loss, 44.87% said they had been repaired or totally compensated, compared to 25.64% who said they had been partially compensated and 29.49% who said they had not received any type of compensation.

• Regarding reporting mechanisms, the majority of interviewees said that the banking institution does offer a mechanism to report incidents (64.71%) and that in effect they have reported the incident to their bank (71.24%). On the other hand, also noted is that, according to the answers, only 37.25% affirms that there is a mechanism to report incidents before a governmental entity in their country, while 32.03% indicate that it does not exist and 30.72% do not know of such existence. The scenario is even more bleak when considering the low level of reporting before police or judicial authorities, given that, of the answers obtained, only 23.53% have raised the incidents before these bodies.

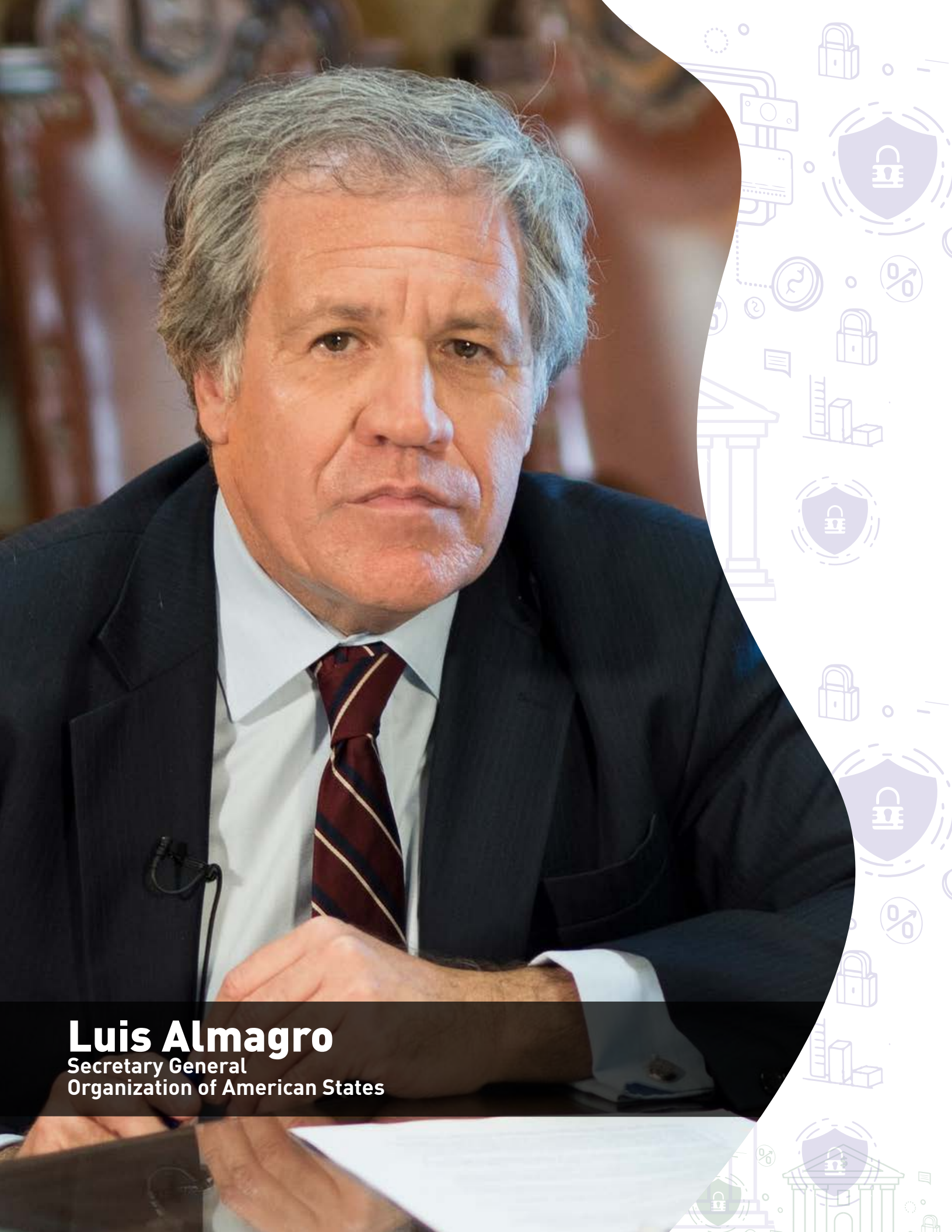
• With respect to users' perception of the evolution of risks of cyber incidents, 79.54% indicate that they have worsened in the last year, compared to 10.85% and 9.61% claiming not perceiving that increase or not knowing about it, respectively.

• Finally, another of the important findings of the study is that 67.08% considers that the existence of risks derived from cyber incidents does affect their decision to use digital media in this sector, or not, which puts the spotlight on the importance of strengthening the management of digital security risks, comprehensively, so that users and companies find a digital environment that generates trust for all.

The detail of the study that can be seen in subsections 4 and 5 of this document develops the aforementioned findings in depth together with many other aspects that may be of interest. Likewise, the annexes included offer additional information useful in the framework of the object of study.

02

FOREWORD



Luis Almagro

Secretary General
Organization of American States

The General Secretariat of the Organization of American States (OAS), through the Cyber Security Program attached to the Secretariat of the Inter-American Committee against Terrorism (CICTE), promotes and coordinates cooperation among the OAS Member States and, among them , the Inter-American System and other organizations in the international system, in order to access, prevent, confront, and respond effectively to threats to security, in order to be the main point of reference in the Hemisphere to develop cooperation and capacity-building in the OAS Member States.

The financial sector, and banking in particular, has been one of the sectors with the highest digitization rates. Every day a greater number of clients of the financial sector are users of electronic banking, they carry out transactions by Internet or payments through mobile devices. This adaptation of the business models and the exploitation of digital channels aim to make the most of the advantages of technologies, the flip side of which is the appearance of new risks that must be prevented in order to mitigate possible attacks and fraud situations to which the sector is currently exposed and, of course, its users.

In the same vein, the aim of this study, prepared by the OAS, is to present the results and analysis on digital security incidents (including aspects relating to information security, cybersecurity and fraud prevention using digital media) that were apparent after conducting the corresponding surveys within various banking entities in Latin America and the Caribbean and their users, as well as the impact in the region. This document structures a study on cybersecurity in the banking sector in Latin America and the Caribbean.

One of the main inputs of this study was the survey conducted in banking entities, which provided information that made it possible to better understand the way they manage digital security risks and their impact. Likewise, the surveys to users served as the source to obtain data on the type of operations established and their use of digital media, their digital security culture, as well as the degree of impact suffered as a consequence of digital security incidents.

The study is divided into two parts as follows:

- **Part 1)** Cybersecurity in the entities of the banking sector in Latin America and the Caribbean: The instruments offer information in three sections. The first offers information on the profiles of the banking entities' characteristics; the second refers to aspects associated with the management of digital security risks, and the third is concerned with aspects related to the impact of the incidents on them.

- **Part 2)** Cybersecurity from the perspective of the users of the entities of the banking sector in Latin America and the Caribbean: The survey instruments offer information in three sections. The first provides information about the characteristics of the users; the second deals with aspects associated with the digital security culture and the third refers to aspects related to the impact of the incidents.

In addition to the specific results obtained with the aforementioned instruments, we have had important contributions from representatives of the most important organizations in banking in Latin America and the Caribbean, as well as from international level organizations that contribute to

high impact issues in the sector. It is a privilege for the organization to have contributions from such relevant organizations as the World Economic Forum (WEF), the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the Financial Action Task Force on Money Laundering (FATF), the Latin American Banking Federation (FELABAN) and the Caribbean Association of Banks (CAB) that, with their articles, allow us to have significant elements to contextualize the challenges of addressing cybersecurity for banking in Latin America and the Caribbean.

Based on the above, as well as the research conducted founded on different references addressed in the study, the intention is to offer conclusions and recommendations relevant to the banking sector and its users, as well as to governments and their regulatory bodies in order to have a more reliable and secure digital environment for the services offered by this vital sector for the region.

03

CONTRIBUTIONS

3.1 World Economic Forum: The Cybersecurity Threat Landscape in Latin American & Caribbean Banks

Troels Oerting
Head of the **World Economic Forum** Global Centre for Cybersecurity

Sean Doyle
Global Leadership Fellow; Project Lead, Governance and Policy, **World Economic Forum** Centre for Cybersecurity

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

In 2018, headline-making attacks on banks in Mexico and Chile made it clear that Latin American financial services are a target of foreign criminal and state-supported hackers. Along with this relatively new international attention, the resources of home-grown Latin American cybercriminals are also likely to grow, with clear evidence that Latin American-developed specialist malware is being adapted for the export market.

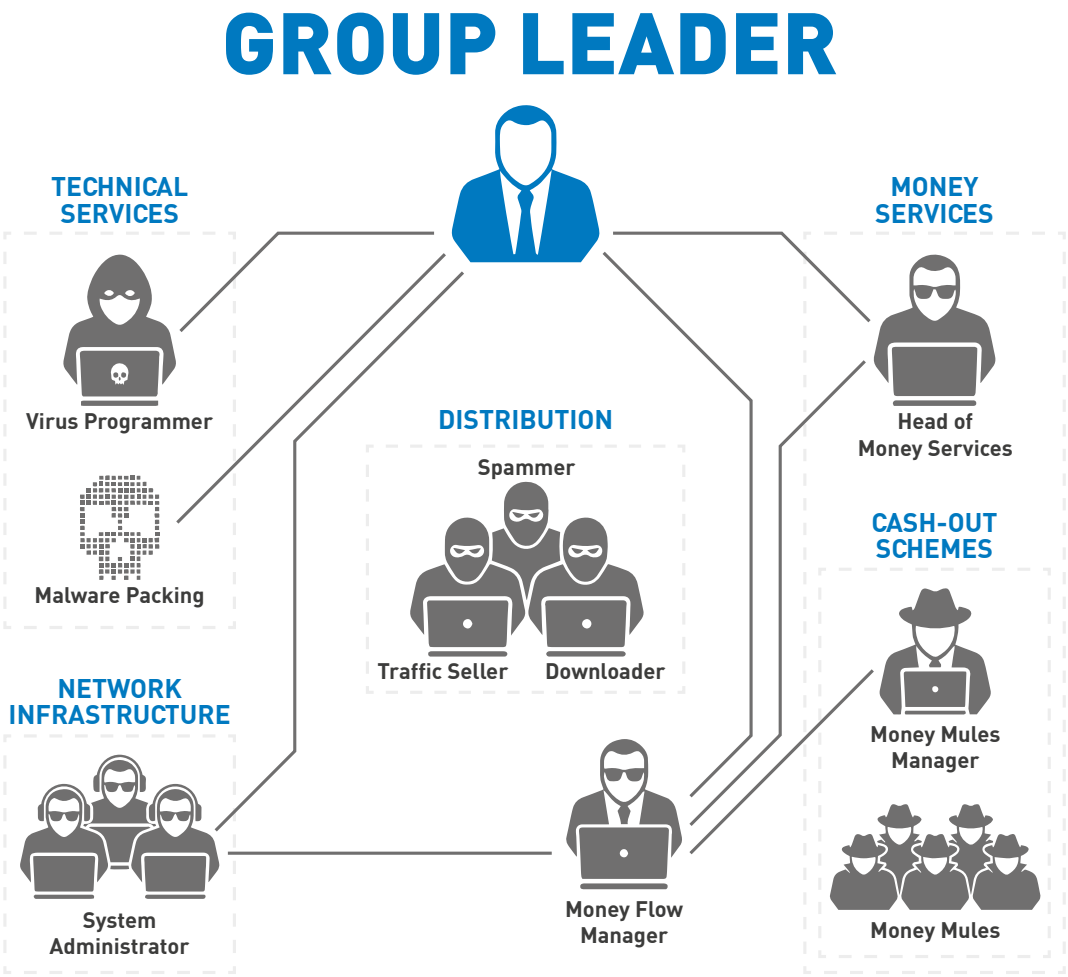
Cybercriminals are organized, well-funded and geographically unrestricted. Thieves no longer need to enter a bank branch, or even the country in which their target is located. Sophisticated criminals will attack whichever bank provides the greatest return on investment, regardless of where it is based. Therefore, all banks should take care that they have sufficient technical resources, adequately trained staff and appropriate procedures to defend against cybercriminals and ensure that the business is sufficiently resilient. In Latin America and around the world, cyber resilience requires engagement from board-level down to branch level.

While individual efforts to improve security are vital, cybercriminals also identify weaknesses in the ecosystem of a country or region's banks, such as common practices in payment processing, or commonly used software. Consequently, an attack on one bank is likely to lead to similar attacks on many banks in the region. For this reason, efficient sharing of information between banks, and between banks and state-agencies, is an important factor in increasing resilience across the system and lowering the financial and reputational cost of attacks.

Cybercriminal groups

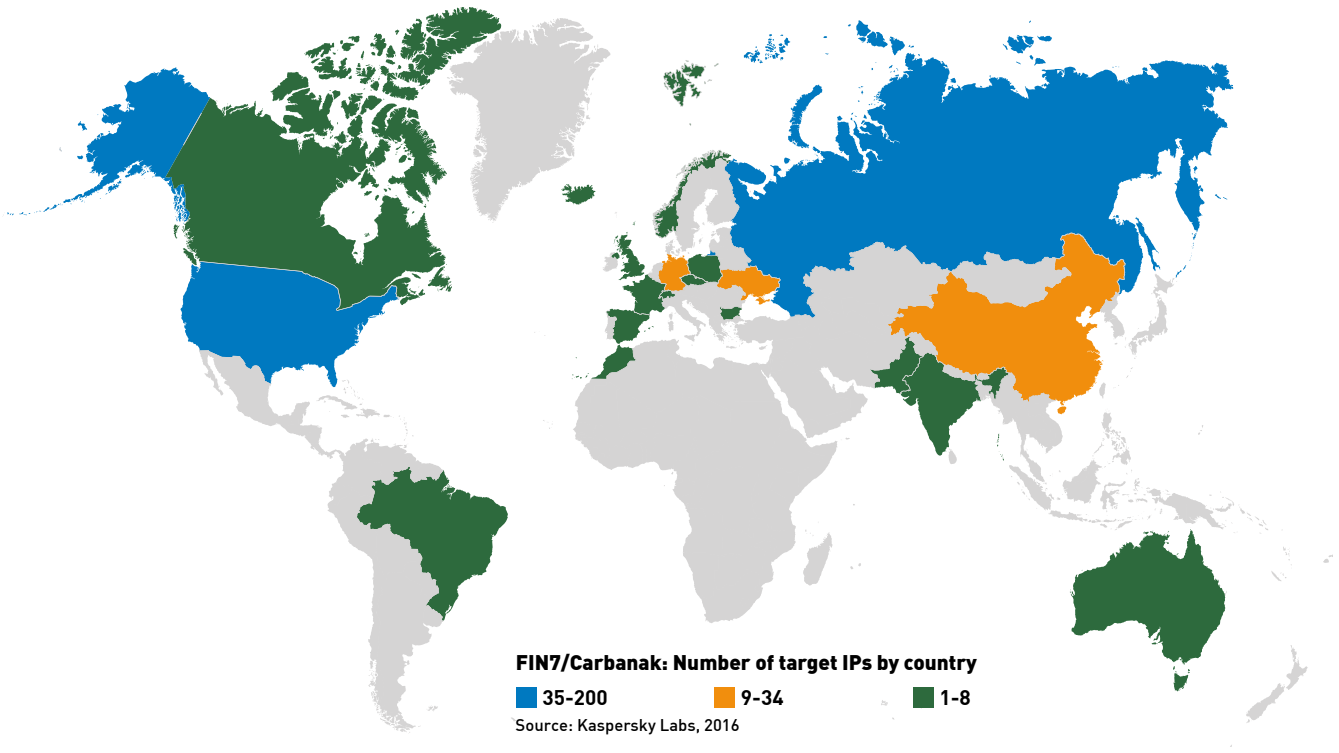
Increasingly, cybercriminal groups targeting the financial system are highly specialized and have acquired expertise in core banking systems, common bank work systems as well as the methods to infiltrate and subvert them. These groups are typically disciplined, with effective operational security, standardized operations, sophisticated techniques, access to high-end software development resources, a deep knowledge of the targeted networks and an ability to sustain activities inside a bank's network for a period of months.[4]

Image 1: Typical Cybercrime Group Organization



This sophistication allows such criminals to strike globally. The image below provides an overview of jurisdictions targeted by just one set of cybercriminals, the Fin7 (aka Carbanak) group. Fin7 is assessed to have stolen at least USD 1 billion from financial services operators in the period 2013-2016, before expanding its targets to include a range of other sectors in 2016-2018.[5]

Image 2: Jurisdictions in which banks were targeted by the Fin7/Carbanak group



When police forces began arresting Fin7 members in March-August 2018[6] it required cooperation across the United States, Ukraine, Germany and Spain, among others. The geographical spread of both targeted banks and the individuals undertaking the attacks makes it difficult for individual banks to prepare effective defences when acting on their own and complicates law enforcement efforts to track and arrest criminals after a successful attack.

Latin American and Caribbean banks

While public reports of sophisticated cyber-attacks on Latin American and Caribbean banks are less frequent than those in North America, Europe and Asia, recent evidence shows that the region's relative tranquillity is coming to an end. In mid-2018, banks in Mexico were targeted by groups with the characteristics of state-supported Advance Persistent Threats (APTs).[7] Also in 2018, at least one bank in Chile was robbed by an organization with significant capabilities, though it is unclear whether this is best attributed to cybercriminals or more advanced APTs.[8]

ATM attacks:

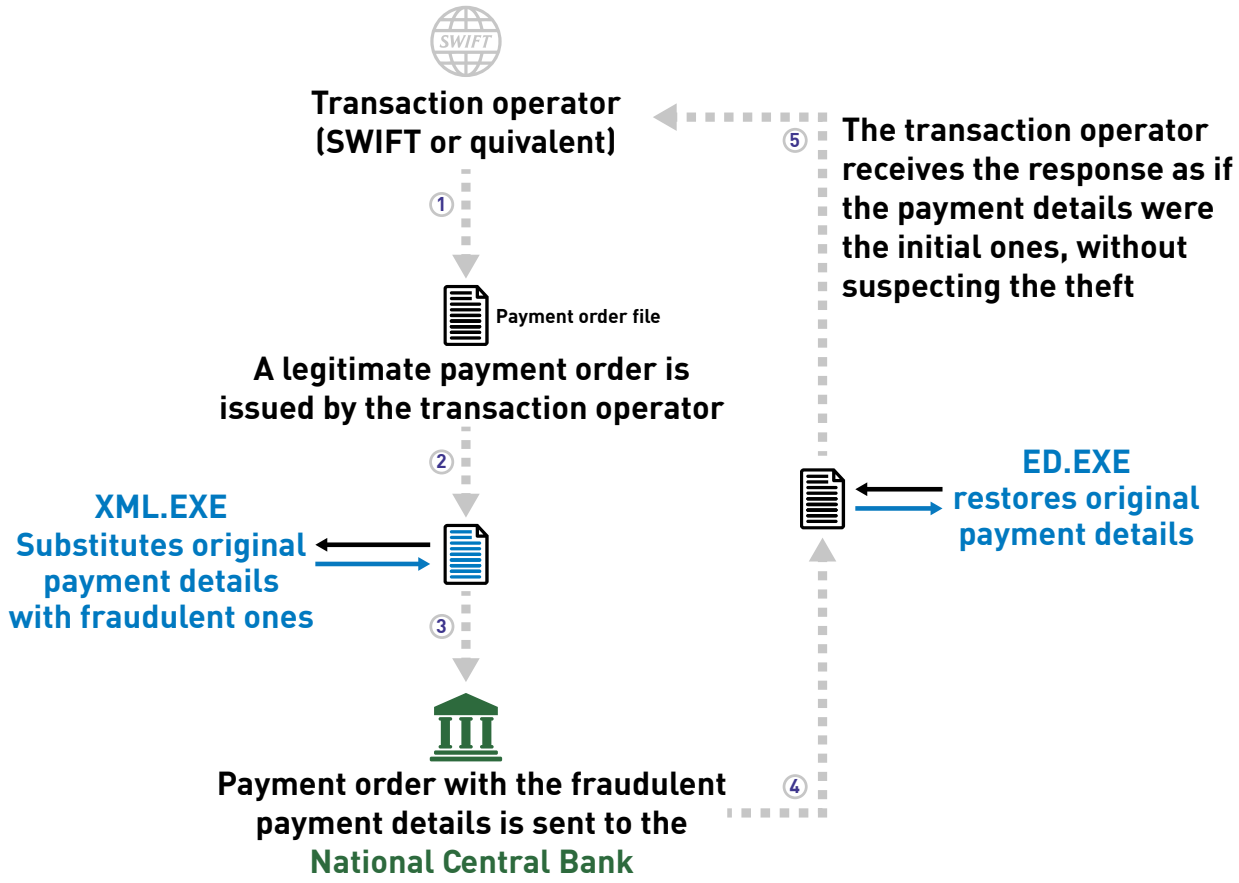
Besides being a target for international criminal groups in the near future, Latin American banks have their local sophisticated attackers to contend with. ATM attacks are an area in which Latin American cybercriminals sit among global leaders. Latin-American developed ATM exploits, such as the Ploutus family of malware, have proven so effective and adaptable that Latin-American criminals have successfully marketed this software for export. For example, in early 2018 the Internet of Things (IoT) specialist security firm Zingbox reported that variations of Ploutus malware were being sold under licence to criminal groupings in the USA. This operation was so sophisticated that the licensing system was reported to include additional client services such as workforce training.[9]

These two examples, Fin7 and ATM attacks, show how criminal activity proven effective in targeting banks in one region will eventually find its way to Latin American and Caribbean markets, just as Latin America-developed Ploutus ATM-malware has made its way to North America.

The New Attack Surface for Latin America: Payment Systems

Breaches of payment systems such as SWIFT, or national variants such as Mexico's SPEI, happen across all regions. These attacks rely on weaknesses in banks' systems architecture and processes and are not usually due to weaknesses in the payments infrastructure itself. For example, SWIFT, responding to an attack on a Latin American bank in March – April 2018, stated it was unaware of "evidence that SWIFT's own network or core messaging services have ever been compromised. Rather, in each of the incidents customers first suffered security breaches within their local environments.[10]

Image 3: Anatomy of an attack on payments systems



Exploitation of these relatively weak endpoints seem to be the next trend in cybercriminal activity. In late 2017, the private-sector information security firm Group-IB found indications that sophisticated cybercrime groups specializing in financial services attacks, such as the Russian-speaking "MoneyTaker" group, were gathering intelligence on cross-border payment systems used by banks in Latin America as well as North America.[11] It seems clear that this intelligence is being gathered by criminals in order to launch future attacks against Latin American or Caribbean banks, perhaps to achieve similar results to the cybercriminals who did subvert the SPEI payment system in spring of 2018.[12] This attack was itself similar to the alleged exploit of the transfer network of UniTeller, compromised by an East Asian group in June 2016.[13]

Additional targeted attacks are likely in the near future, particularly as systemic, sector-wide defences in North American, European and Asian markets continue to improve through enhanced cooperation and more effective regulation.

Conclusion

In the face of sophisticated adversaries, cybersecurity must now be viewed as a common good dependent on a high minimum standard across the sector and across borders.

The cost incurred by cybercriminals to prepare and execute an attack is diminishing and the risk of being arrested remains low. Consequently, the World Economic Forum Centre for Cybersecurity assesses that attacks of a low to mid-level sophistication will grow in volume while the expertise of a limited number of non-state Advanced Persistent Threat (APT) groups will continue to increase.

To counteract this, banks can first concentrate on getting the technical, workforce and governance basics of cyber-security right. This often requires taking cybersecurity out of a siloed area of the business and spreading responsibility to the board-level, who can ensure that cybersecurity is a core consideration when the business thinks about products, services and how it plans to grow.

As the sector most heavily targeted by cybercriminals, banks in Latin America and the Caribbean have the potential to access a detailed picture of cyber threats and attack vectors. The opportunity to undertake strategic analysis of emerging threats is greater than in almost any other sector and could significantly improve identification and containment of attacks if banks work together to do so.

Criminals operate across borders and can either steal or purchase information on banks' internal networks and operating procedures. This information asymmetry leaves banks at a disadvantage. There is no perfect solution to this problem but there are examples which might be adapted from other regions.

In the US, the Financial Services Information Sharing and Analysis Center (FS-ISAC)[14] is a successful forum for collaboration between banks and between banks and government agencies. In Europe, Europol's Cyber Crime Centre[15] acts as a point of intelligence gathering, analysis and distribution for law enforcement across the EU. Individual projects, such as the "No More Ransom"[16] project led by the Dutch Police and supported by the private sector, have lowered the attractiveness of European companies and organisations for ransomware attackers. In the UK, a small number of banks joined with law-enforcement to create the Cyber Defence Alliance[17] to increase the difficulty of attacking multiple banks with the same techniques.

Each of these models is unique but all point to the right kind of solution for Latin America – only through greater partnership between banks and between the financial sector and regulators and law enforcement can we even begin to combat this problem. The World Economic Forum Centre for Cybersecurity stands ready to help build defence capacity and foster these partnerships.

3.2 SWIFT: Nine cyber security best practices that will help you protect your institution

Juan Martinez
Managing Director, Latin America & the Caribbean at **SWIFT**

While the financial services industry is among the most advanced sectors in its use of IT, and it has hugely invested in its IT security systems, it remains a clear target for cyber criminals – and that threat is growing. As such, the industry is constantly on the lookout for ways to manage the risks they face, all in the knowledge that a cyber breach can happen at any time to any institution.

The World Economic Forum (WEF) has cited cyber-attacks as a top global risk. Its analysis shows that, across the globe, the good guys are not winning the fight by any stretch of the imagination – cyber-attacks were in the WEF's top ten risks in 2016; they moved to the top five in 2017; and in 2018 they feature in the top three risks to the global economy.[18]

While no system can be perfectly secure, there are a number of best practices that banking sector organisations can employ to protect themselves from the complex methods deployed against them. Here are nine cyber security best practices that are applied in highly secure institutions:

1. Secure your environment

Embedding security in the design of your network architecture should be a core principle of your approach. This should also include physical security measures, such as limiting access rights to sensitive areas to authorized personnel, and ensuring you have processes in place to actively control and monitor who is accessing these areas. In addition, those authorized personnel must be properly screened and trained.

2. Know and limit access

After constructing these defenses to guard against intruders coming through the front door, you must put in place operating procedures and processes to limit and protect administrator and system privileges. Having locked down these privileges, a rigorous implementation of strong ID management is required with strict

and actively managed profile and password rules to ensure basic access controls.

3. Detect and respond

Preventative measures will only go so far; detection and response are equally critical. Vital to your awareness and ability to respond in a timely fashion, is having adequate intrusion detection capabilities, delivered through a series of triggers and trip-wires to initiate alerts to suspicious activity.

4. Know your adversary

Ensure that you are constantly gathering threat intelligence about your adversary as it is vital in protecting against it. Threat intelligence plays a key part in assisting software development and updates to anti-virus applications.

5. Limit your exposure

You should only do business with trusted counterparties and maintain relationships with those that you trust. Monitoring any changes in relationships and removing any non-current relationships is another way in which can limit your exposure to potential threats.

6. Implement security controls

Engaging in regular security benchmarking and security audit exercises enables you to detect gaps and lapses in your security controls. To help the industry, SWIFT, in conjunction with industry experts, has published a set of security controls based on the latest cyber-threat intelligence. These controls reflect good security practices and should also be applied beyond SWIFT-related infrastructure as they can help strengthen your operational environment.

7. Know your counterparties

Your understanding of potential counterparts' credit and compliance risks is key to your decision-making around whether and how you do business with them. Cyber considerations should also be an integral part of these routine Know Your Customer (KYC) processes.

8. Implement business controls

By deploying further business controls you can take timely preventive and corrective action against suspicious activity. For instance, by filtering outgoing messages against a tightly configured set of rules you can screen your outgoing payments to detect illicit or unusual message flows. Being able to detect such out-of-policy messages before they are sent may alert you to a potential compromise, allow you to take immediate remedial action, and ultimately prevent fraudulent transfer requests even leaving your organisation.

9. Plan for incident response

Security is not an absolute status, preparing for the worst is as important as defending against it. You must develop and institute a recovery policy to ensure that you are equipped to respond quickly to fraudulent activity. If fraudulent or suspicious activities are detected, appropriate measures must be taken immediately. With the right processes in place, you have an opportunity to minimise fraud loss and/ or to increase the likelihood that funds will be recovered.

Equally, it is important to ensure your understanding about the internal actions you must take when responding to an incident, as well as rehearsed processes to support them. Those behind the cyberattacks are deploying increasingly creative techniques to access critical user information, such as obtaining administrator rights for operating systems, manipulating the software in memory, and altering the legitimate functionality to resist two-factor authentication, etc.

How SWIFT is reinforcing the security of the financial industry

SWIFT, as a global member-owned cooperative and the world's leading provider of secure financial messaging services, is committed to playing an important role in reinforcing and protecting the wider ecosystem safety through the SWIFT Customer Security Programme

(CSP), which launched in 2016. The CSP aims to improve information sharing throughout the community, enhance SWIFT-related tools for customers, and provide a customer security control framework. Through the programme, we also share best practices for fraud detection and enhance support by third party providers.
In developing and rolling out the CSP, we regularly communicated and consulted with regulators and have been – and remain – heavily engaged with our customers all around the world. Drawing on our community's advice and input, we have set up expert, consultative and working groups. We have also conducted numerous webinars, workshops, roadshows, round tables, and training sessions, drawing more than 14,500 SWIFT community members, in our bid to raise awareness, to build competence, and to transfer skills.

We have made measurable, tangible progress in helping our customers gear up against the evolving threat. Attacks have been detected and prevented thanks both to increased awareness on the victims' parts, to the alertness of their counterparts, and thanks to the tools we have developed.

While no system is totally secure, there are ways in which institutions can best protect themselves from the complex methods deployed against them – including securing their local environment, managing security risk in interactions with counterparties, sharing relevant information, and acting in a timely manner on the security risk information they receive.

The adversaries are prepared to invest a large amount of time planning and preparing their attacks. Knowledge, determination and collaboration are essential ingredients to achieve cyber security resilience.

3.3 FATF: IMPLEMENTING EFFECTIVE LEGISLATIVE FRAMEWORKS TO COMBAT MONEY LAUNDERING IN THE GLOBAL DIGITAL ECONOMY

Santiago Otamendi
President (2017-2018)
Financial Action Task Force on Money Laundering (FATF)

Crime is a fact of the human species, a fact unique to this species.[19] As long as there are people seeking financial gain from crime, it is necessary to separate the income from the underlying crime. Money laundering helps organized crime flourish, which, in turn, threatens civil security and endangers stability and economic growth.

The role of FATF is to understand the risks of money laundering and terrorist financing, to develop and promote global policies and standards to counteract these risks, and to evaluate countries vis-à-vis these standards and thus contribute to security.

The first step is to develop an effective legislative framework to prevent and punish money laundering, protecting the integrity of the financial system. This framework should provide countries with sufficient authority to identify, evaluate and understand how criminals wash the proceeds of their crime.

Since the issuance of the first group of FATF Recommendations[20] in 1989 to help countries combat money laundering, which later introduced standards to counter terrorism financing, governments around the world have made significant progress in implementing a strong financing system against money laundering and against terrorism (AML/CFT). As countries implement safeguards to detect, prevent and punish the laundering of money from criminal activities and the flow of funds related to terrorism, terrorists and criminals continue to adapt and find ways to bypass these safeguards to continue financing their criminal activities.

One of the strengths of the FATF is its ability to respond to the changing risks of the financial system, raise awareness of new or evolving threats and update, if necessary, its standards accordingly so that countries continue to have the strongest possible tools to protect the integrity of the financial system.

During the 30 years of existence of the FATF, technological innovation has had a significant impact on our society and our daily lives. The financial landscape has also changed, introducing services and products that did not exist only 10 years ago.

For centuries, the traditional banking structure has dominated the financial services market. Today, digital innovation has introduced alternative products and new ways for customers to manage their assets and financial transactions. Financial innovation has delivered efficiencies and it has the potential to increase financial inclusion by offering digital solutions to clients who do not have access to regular banking services, particularly in low-income regions. However, this also means new risks that must be mitigated to ensure that the services are not abused to launder money or finance terrorism.

The number of financial service providers continues to grow. Traditional banking service providers have responded by introducing competitive financial innovations to maintain their customer base. They have invested heavily in developing the necessary experience and innovative technology to compete with the new financial technology service providers (Fintech). Financial innovation has had an impact on the way financial services are delivered and also introducing new financial products, such as crypto-assets.

Crypto-assets (sometimes called virtual currencies or crypto-tokens) can be decentralized, they are practically impossible to be the target of attacks, and are anonymous. These features are attractive to many, including those who wish to use them for money laundering and terrorist financing. Crypto-assets involve a variety of business models, often with many parties operating from different jurisdictions. The segmented and cross-border nature of the industry makes regulation difficult. There has been a wide range of government responses to crypto-assets. Some governments classify them as currencies. Others classify them as basic products. Others have chosen to ban them altogether. This has resulted in a patchwork quilt of different regulatory approaches. This lack of common focus on the part of governments negatively impacts transparency and creates spaces for abuse by criminals and terrorists.

The transnational nature of crypto-assets requires a global regulatory approach. The FATF has identified opportunities to improve its understanding of the potential risks of money laundering or terrorist financing and is working to develop a more consistent strategy to manage these risks, while supporting responsible financial innovation and promoting financial inclusion in accordance with the AML/CFT requirements.

The FATF recognizes the enormous potential of financial innovation and supports responsible development that does not increase the risk of money laundering and terrorist financing. Artificial intelligence and machine learning technologies have the potential to contribute significantly to an effective AML/CFT policy. However, challenges persist, such as gathering in one place all the relevant information needed by banks, public authorities and technology developers, in a way that does not compromise privacy and confidentiality.

The FATF is closely monitoring these problems and is directly involved with the financial technology and regulatory technology (Regtech) communities. After all, the fact that the products they develop are considered to protect the integrity of the financial system and are not considered vehicles to move funds linked to crime or terror is also to their advantage.

In 2015, as part of a phased approach to monitor progress in financial innovation and its impact on FATF standards, our entity issued the

Guidance for a Risk-Based Approach to Virtual Currencies.[21] This guide focuses on the use of its standards relevant to convertible currency converters, that is, the point of intersection with the regulated system.

Since then, the FATF has increased its understanding of financial innovation and possible vulnerabilities related to money laundering and terrorist financing. With the support of the G20, the FATF will now review its standards to identify where they might need to be adjusted or strengthened to provide countries with updated tools to implement them, within their national legal, regulatory and operational frameworks.

The FATF is dedicated to more than just establishing global standards to combat money laundering and terrorist financing. Like the Organization of American States (OAS), FATF member states hold each other accountable.

The global financial system is as strong as its weakest link. Therefore, it is essential that there be a comprehensive implementation of robust and effective AML/CFT measures. The FATF has established, through nine (9) FATF-style Regional Bodies (FSRBs), a network of 204 countries that have committed at the highest political level to fully and effectively implementing the FATF Standards. The FATF and each FSRB assess the effectiveness of their members' implementation of the FATF Standards using universal procedures[22] based on the FATF assessment methodology.

The robust FATF peer review program (the mutual evaluation process[23]) is now in its fourth cycle, focusing on the effectiveness of the AML/CFT systems of the countries evaluated. Previous cycles showed that countries often adopted a 'check box' approach when implementing AML/CFT measures. They sometimes reached a high level of technical compliance with FATF standards, but their measures did not always deliver the expected results to be considered effective, such as successfully prosecuting criminals for these crimes and confiscating their illegal profits.

The current cycle of evaluations has a double focus. Technical compliance, that is, making sure that laws, regulations and operational measures are working, is still important. These measures are the pillars of a solid framework for dealing with financial crime. However, an effective AML/CFT framework is based on a country's identification, understanding and evaluation of the specific risks of money laundering and financing of terrorism it faces. The Americas face risks different from those faced by the northern countries of Europe or Asia, so the measures, which countries must implement to ensure that funds connected to crime or terrorism are kept outside the financial system, are different. This risk-based approach is essential. It allows a country to use its resources efficiently, focusing them on the areas where the risks are highest.

In a peer review of the FATF, a country must be able to demonstrate that the action it is taking is delivering the expected results. Each evaluation gives the assessed country two sets of ratings that reflect the extent to which a country has implemented the technical requirements of the FATF Recommendations and the level of effectiveness of its measures. More importantly, the evaluation provides clear recommendations on the country's priority actions. A robust follow-up process ensures that countries take the necessary measures to address the deficiencies revealed in their evaluation and hold those who do not take the necessary steps to strengthen their systems accountable.

To help achieve strong, sustainable and inclusive economic growth, promote greater inclusion and reduce inequality, the FATF should continue to focus on financial inclusion, in line with the FATF Standards and the G20 High-Level Principles for Digital Financial

Inclusion. In addition, it is clear that the elimination of risks and de-commodification by global banks can lead to financial exclusion and increase the risks of money laundering and financing of terrorism faced by society, including the increase in the use of cash and of unregulated channels.

Innovation is bringing many positive developments to the way we live, work and manage our assets. Financial innovation, in particular, improves financial inclusion for those who do not have access to traditional financial products, which are often vulnerable communities in high-risk regions.

Now more than ever we have to work together to make sure that criminals and terrorists do not benefit from financial innovation to hide their identity and carry out their illicit activities undetected. The FATF will continue to monitor new developments and will work with other relevant organizations to mitigate the risks of AML/CFT. It will continue its dialogue with the Fintech and Regtech communities to increase understanding and knowledge, and ensure that financial innovation is developed considering the vulnerabilities of money laundering and terrorist financing.

The FATF will work to develop a more consistent approach to manage the vulnerabilities of financial innovation and to reduce gaps that are emerging as a result of different regulatory frameworks in different countries.

3.4 FELABAN: CYBERSECURITY IN LATIN AMERICAN AND CARIBBEAN BANKING

Santiago F. Rodríguez V.
President
Latin American Committee on Banking Security

Latin American Banking Federation (FELABAN)

Banking security has gradually evolved, founded on technological advances, to face the risks and threats to banking in the provision of its financial services.

Criminal modalities have been increasingly refining over time and have sought vulnerabilities to banks financial services to their clients. The first computer attacks began in the 90s with the start of the Internet.

Users do not have an adequate awareness of the use of the Internet. Dependency on suppliers begins without establishing adequate security measures, and the information begins to be stored in removable devices, also, with few security measures. This situation is used by cybercriminals to search for vulnerabilities.

In the 2000s, attacks began to target the tools responsible for protecting information, the use of social networks began to spread massively, the security risk derived from disgruntled employees (insiders) appeared, and online fraud began to occur.

In 2010, Security Management took off, where regional banking began implementing solid plans for information security awareness; the legal departments sought legislation to protect critical infrastructures; greater control was installed, related to privacy of information to prevent leakage; and information encryption tools started being used.

The above-mentioned evolution of the three factors, Technology, Financial Services and Risks, gave way to Cybersecurity, using risk detection and threat to Information Security, being basically provided by frequent computer use.

From here on, in the case of Latin America and the Caribbean, the main computer risks in banking were credit card cloning, identity theft in non-face-to-face purchases and phishing. The latter term was used to describe a model of computer abuse in which a cybercriminal is posing as a financial institution to obtain confidential customer information in a fraudulent manner. However, by this date there have already been important advances in terms of cybersecurity and preparedness to combat cybercrime. The chip technology was incorporated into debit and credit cards and the use in online purchases of a security token.

This was compounded by the appearance of a black market for the sale of account numbers, cards and passwords that originated mainly in Russia, but which sought alliances with cybercriminals in the different Latin American and Caribbean markets.

These cybercriminals expanded their business in the region, because they detected that the infrastructures were vulnerable and that the banking entities acted in a reactive manner, with which preventive efforts were scarce.

The banks in the region are facing a technological breakthrough that has not stopped, continues and continues stronger than ever. In this field, we are already experiencing and facing challenges such as digitalization, which represents a challenge for the financial sector, both for its business and for its security. The financial system has become an indispensable way to have access to basic satisfactions and development opportunities. There are different studies that conclude that access to financial services improves the quality of life of people and drives the economic development of countries. Innovation and technology have taken up the challenge of developing new schemes and ways of giving greater and better access to finance, but accompanied by a strong security scheme, with the aim of minimizing the different forms of cybercriminals.

Given these profound changes in the demand for financial services, banks in the region are responding to the challenge of digitalization and cybersecurity, with different approaches and at different speeds, since not all banking entities understand the same meaning of transforming themselves for be a digital bank. But what is digital banking? The literature does not offer a concise definition of this new concept that, in any case, considers issues such as the generation of supply, distribution and sale of financial products and services through digital channels, the exploitation of the latest technologies to better understand the customer and anticipate their needs in an agile and convenient way, the omnichannel or the possibility of the client communicating through all the channels (analog and digital) with their bank or the automation of services. In general, digital banking is expected to put the needs of the final customer before the creation of products, this being the center on which the offer is defined.

In this sense, traditional banks in the region that are betting on digital banking are going through a transformation that allows them to position themselves in the new ecosystem.

This positioning in the digital banking ecosystem must be accompanied by a security scheme, this being a reality that determines the strategies set by financial institutions at a regional and global level. The client defines their priorities by demanding a different, immediate and digital experience, but with a backup of their information and transactions. The combination of these worlds, digital banking, customer experience and security, reveals the experience of secure digital customer, essential at present and in all sectors of the economy, but particularly relevant in the construction of the future banking sector.

Attackers have become sophisticated and increasingly seek precise objectives and offer a high economic reward, rather than large-scale attacks to the largest possible number of users.

The fight against cybercrime in the region during 2016 took big steps, as resources were increased to Cybersecurity. However, in the face of greater investigation and protection against threats, cybercriminals continued to change their way of acting and expanded their objectives, often with higher budgets than those charged with defending.

Globally and regionally, 2017 was a complicated year for Cybersecurity, where banking in the region had to face large-scale cyber attacks and threats against computer security such as Ransomware, WannaCry and Petya.

Dmitry Bestuzhev, director of the Research and Analysis Team for Latin America at Kaspersky Lab, points out that "the security of a bank is not a static strategy, but needs to evolve and adapt constantly, based on intelligence obtained on trends, new threats and the latest security techniques to keep the network truly secure."

For these next years one of the main risks for banking and that will be a challenge for Cybersecurity in the world and in the region, will be the Internet of Things, which is described as a world where things are connected and capable of share data.

GARTNER (Gartner Inc. is a consulting and information technology research firm) calculates that the number of Internet of Things devices connected to the Internet in 2025 will exceed 75 billion. Each of these devices with its own operating system, usually a simple firmware with a small microprocessor capable of performing the simple tasks necessary for the operation of the device, its own IP address and always connected.

Many millions of these devices will work with vulnerable firmware, some more than others. There is no perfect security, in the short term there seems to be no interest in maintaining responsibility for everything that is being manufactured to be connected to the internet. With 75 billion devices and accessories online, many of them easily damaged and used to carry out attacks, we will face a real bomb.

To face and defend against this type and other types of risks, cybersecurity teams must use artificial intelligence, but at the same time cybercriminals could also use it; that is, they could manipulate what are now friendly bots and turn them into lethal weapons to violate and penetrate the security schemes of financial institutions.

In the same way to face this avalanche of cyber attacks, the banks in the region are perfecting their security schemes that among the main efforts is the implementation of a response team to Digital Security Incidents (CSIRT), a team with the responsibility of receiving, review, analyze and respond to all that report and activity related to information security problems.

Another measure to mitigate the cyber-attacks in which we are already working is Digital Surveillance, which allows us to be proactive and preventive, in order to be prepared to face and solve the greatest security challenges in the digital world. That is to say, to be the eyes and the ears in the ecosystem, to manage and face the increasing volume of cyber attacks to the financial system of the region.

A similar measure to the Digital Surveillance in which security teams already work in the region, are the techniques of obtaining, analyzing, elaborating and disseminating data in open sources, where hidden relationships can be discovered, monitoring of cybercrime modalities and analysis of patterns In addition to extraction of information not visible at first sight and that serves for decision making.

Trends in financial services in the region show a strong outlook of evolution, adoption of technology and greater awareness in Cybersecurity.
The new attack vectors will gradually grow and an appropriate management scheme will be necessary in response to the threats accompanied by a multidisciplinary security team, organized, integrated and incorporated within the digital transformation teams, to face the cybercrime modalities.

The attacks will have a wide scope and cybercrime will continue to be professionalized, because it is becoming more organized.

3.5 CAB: Challenges in the Promotion of a Cyber-Secured Caribbean Financial Services Industry.

Joanna Charles
Presidenta
Asociación Caribeña de Bancos (CAB)

CARIBBEAN ASSOCIATION OF BANKS
Keeping the Industry Proactive, Protected and Profitable

Global and regional financial systems continue to become increasingly interconnected thus resulting in significant economies of scale, increased efficiency and lower transaction costs for consumers. Interestingly, it is widely believed that the financial services sector is the most lucrative target for cyber-attacks. As banks progress to bridge the technological gap, so too, cyber criminals exploit these advances to orchestrate increasingly sophisticated attacks. Indeed, the World Economic Forum (WEF) 2018 Global Risks Report identifies Cyber threats[24] as one of the four main risks to focus on. How then do regional indigenous banks manage this dynamic risk?

The answer to this question may be difficult to grasp, in a landscape where cyber threats are continuously changing and evolving, and technology is constantly redefining the way banks conduct business. Additionally, the unique characteristics of the Caribbean banking landscape presents its own navigational challenges. The regional financial space can be divided into three broad categories: foreign banks -which are branches or subsidiaries of much larger North American banking groups-, large indigenous banking groups, and small indigenous banks.[25] The prevailing operating climate is one of a cash intensive economy with a changing customer base, advances in new financial technology and risks from derisking by correspondent banks.[26]

The disparity in the sizes of financial institutions in the Caribbean, highlights the fact that in most cases a 'one-size-fits-all' approach cannot be employed, and cyber security solutions may have to be tailored to the needs of each individual bank. However, the similar economic climate in which the banks operate presents unique opportunities to take a collaborative approach to addressing cyber risks. The Caribbean Association of Banks (CAB) has strategically positioned itself to facilitate this collaboration and promote the sharing of best practices. The CAB was established in 1974 and currently represents seventy-eight (78) member institutions. The CAB's Membership spans from the Bahamas in the north, to Guyana and Suriname in the south and comprises both the English and Dutch speaking Caribbean.

Caribbean financial institutions are fully cognizant of the importance of a cyber resilient organization and the catastrophic consequences of a cyber breach, which includes damage to the bank's reputation, loss of customer trust and loyalty, and severe legal and regulatory penalties. Mitigating

these risks creates additional demands on the limited resources of smaller Caribbean banks; resources which also must be used to address issues such as compliance with ever-changing national, regional and international regulatory requirements and a sensitive correspondent banking climate. Nevertheless, Caribbean banks are placing great importance on each step of the cybersecurity cycle, which can be defined by prevention, detection and response; and are taking necessary measures to combat and mitigate cyber threats.

These measures may take many forms. Generally, they should be enabling factors for cyber resilience in the bank and may include steps such as[27]:

1. Establishing the right Governance structure to make cyber security a board level priority and developing leading indicators to identify gaps early;

2. Identifying the financial institutions' risks to security by defining their risk appetite and cyber profile, implementing effective monitoring mechanisms and constantly assessing the threat landscape;

3. Identifying and protecting critical business processes; and

4. Improving collection, analysis and reporting of cyber intelligence and aligning cyber security to business processes.

Financial institutions need to ensure that numerous safety nets and levels of monitoring are in place in the event of a breach, as regardless of how prepared they are, gaps exist which cyber criminals would most likely exploit. For example, while CAB's members hold routine cybersecurity training for their staff incidents of phishing are still being report.

Harmonization of cyber security, data privacy and Information and Communications Technology (ICT) legislation are a critical component in facilitating the development of a cyber secured financial services industry. While the CAB notes the progress that the CARICOM has made in this regard, there is need for a greater sense of urgency and political will to implement the necessary harmonized legislations. The lack of harmonization of legislation inhibits the ability to effectively leverage the best practices of other financial services institutions in the region; it limits the sharing of ideas and the possibility of consolidation of key functions to effectively navigate the cyber threat landscape. To some extent, these inefficiencies limit the pooling of resources and expertise which could be allocated towards more robust cyber security structures.

Additionally, the need to develop greater capacity of cyber security professionals in the region cannot be understated. It is important to foster an enabling environment which will facilitate the development of these professionals in various sectors such as law enforcement, financial services, telecommunications and other critical public and private economic organs. Educational programmes to develop the expertise of cyber professionals and to raise awareness of financial services professionals to the importance of cyber security, is likewise a key strategic component to addressing this regional threat.

In this regard, the CAB has actively been engaged in educating its membership on the need for cyber threat mitigation and resilience. Several CAB Conferences have featured panels and presentations by prominent companies, on the need for cyber security and how financial institutions can effectively manage their cyber risks. These presentations facilitate open dialogue between CEOs, managers, technical personnel and cyber security experts, and creates a platform on which regional banking leaders engage cyber security professionals.

In addition to the annual CAB Conference, CAB organizes conferences for its affiliate- the Caribbean Association of Audit Committee Members- and likewise prominently features cyber security as a major topic of concern to raise awareness on all fronts.

The new European Union's General Data Protection Regulation (GDPR) is another area in which the CAB has brought training and awareness to the Region. Non-compliance with this regulation results in fines up to two percent (2%) of global turnover or ten million Euros (whichever is greater) for a first level breach, and up to four percent of global turnover or twenty million Euros (whichever is greater) for a high-level breach. Cognizant of the serious implications this regulation has for regional financial institutions and how they deal with data privacy and cyber security, the CAB hosted a webinar on GDPR for the industry, as well as a panel discussion at the CAB's CEOs Forum, which was facilitated by its Service Members Deloitte and Hitachi Systems. Additionally, the CAB made a presentation to the CARICOM's Council for Finance and Planning (COFAP) so that regional Government heads would be aware of the issue and draft a necessary regional response.

To aid regional financial institutions to gauge their level of "cyber security readiness", the CAB circulated the Cyber Resilience Review (CRR): Self- Assessment Package developed by the Carnegie Mellon University and the Government of the United States and encouraged members to complete the assessment to ascertain where their deficiencies or gaps existed.

The CAB also provides Group Insurance Protection to regional financial institutions through its partnership with Howden UK Group Limited. Howden offers protection to Caribbean financial institutions within the CAB Comprehensive Crime, Cyber Crime & Civil Liability Policy. Currently, Howden offers coverage between USD 2,000,000 and USD 20,000,000 per member bank. Since 2012, Howden has settled (100%) on claims which include, fraudulent payment instructions, plastic card skimming, ATM theft and cyber-crime.

The Caribbean financial services industry has by no means been insulated from cyber threats, and while regional banks are continuing to expend resources to ensure continued digital operations and competitiveness, they are also investing in mechanisms to mitigate cyber risks. In light of this major threat confronting the financial sector in the Region, the CAB fervently believes that it is opportune for all stakeholders to play their part and implement the enabling mechanisms to mitigate cyber risks, thereby ensuring the continued growth, stability and security of the Regional financial industry.

04

CYBERSECURITY IN BANKING SECTOR ENTITIES IN LATIN AMERICA AND THE CARIBBEAN

According to the Global Risk Report of the World Economic Forum 2018, large-scale cyber-attacks and leaks or massive thefts of data are considered among the five (5) most likely risks in the next decade globally. *"The risks of cybersecurity are also growing, both in prevalence and in disruptive potential. Attacks against companies have almost doubled in five years, and incidents that once were considered extraordinary are becoming increasingly common"*. (WEF, 2018).

Bearing in mind that the financial services sector–which includes the banking sector–is considered one of the economic sectors with the highest degree of digitalization, relying heavily on Information and Communication Technologies, especially the Internet; given the growing relevance of the digital environment on the banking entities' activities in the Latin America and the Caribbean region, and its high dynamism and impact on other economic sectors, in recent years this situation has brought with it a set of risks, threats, vulnerabilities and incidents of various types, to which both these organizations and their users have been exposed.

According to the information gathered by the Latin American Banking Federation (FELABAN), the volume of bank assets (without discounting the liabilities of the entities) in Latin America reached US$4.2 trillion as of December 31, 2017. Additionally, the net profits (earnings) accumulated by the banking system as a whole in the region as of the same date were US$53 billion, up approximately 13.9% from the previous year. According to FELABAN, *"as of December 2017, the banking system in Latin America increased its assets at a rate of 2.53% per year. 2017 turned out to be a year of recovery for the main economies that suffered the consequences of a recession or a slowdown in the economy. The slight regional economic recovery in 2017, coupled with a favorable environment for international finance, a controlled domestic inflation, and prudent management by bank managers has resulted in benefits that are well worth mentioning."*

In order to prepare this Study on the State of Cybersecurity in the Banking Sector in Latin America and the Caribbean, the General Secretariat of the Organization of American States (GS/OAS) has developed an instrument to procure information on the related aspects and on digital security incidents (including aspects of information security, cybersecurity and fraud prevention using digital media) in banking entities and their impact in the region.

In particular, the instrument presented a catalog of questions classified into three (3) sections:

- Characterization of banking entities
- Digital security risk management
- Impact of digital security incidents

In order to ensure the confidentiality of the information both for the people responsible who answered the survey and for the organizations to which they belong, it is important to bear in mind that the GS/OAS did not request any information that could be identified at a personal or at the organization level. All answers were compiled, analyzed and distributed at the aggregate level, that is, by theme blocks, without it being made available to any person or institution in detail.

Additionally, and for greater clarity during the processing of the instrument, participants were informed that the sum of successful attacks and unsuccessful attacks suffered by the institution during a period of time would be considered a digital security event. Also, the total successful attacks suffered by the institution during the same period of time would be considered a digital security incident.

4.1 Characterization of the Banking Entity

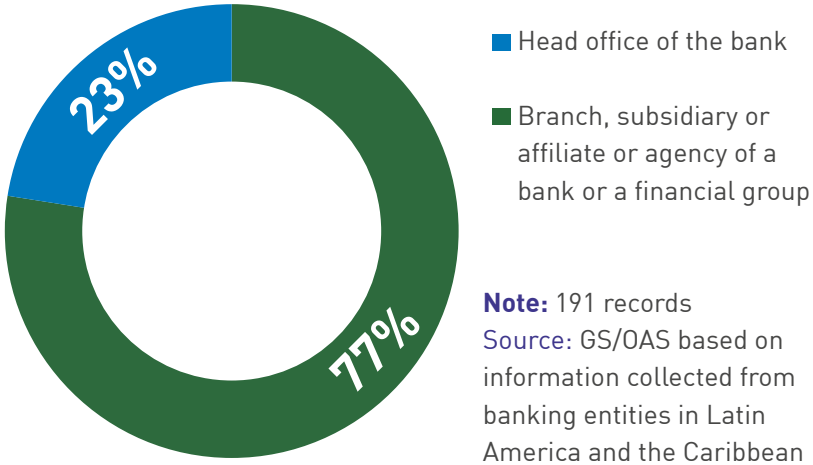
Out of a total of 552 responses delivered during the publication period of the information collection instrument (months in the first 2018 quarter) and based on the detailed review, a database was established with records of 191 banking entities in nineteen (19) countries of the Latin America and the Caribbean region. It is estimated that the sample of banking entities appearing in the results of this study reached bank assets of US$1 trillion and net profits of US$10.5 billion as of December 31, 2017.

The instrument's questions targeted being answered by the local banking entity employing the respondent official (i.e., the bank that operated in the country where he/she was located), even where the institution was the parent company of the bank or a branch, (affiliate or subsidiary) or agency of a bank or a financial group. For clarification purposes, each question detailed the scope of application. 651-7180 x115

Consequently, 23% of the banking entities interviewed were the bank's parent company, while 77% were a branch, subsidiary (affilliate or subsidiary) or agency of a bank or a financial group.

Graph 1. Head Office or Branch, Subsidiary or Agency of the bank

In order to classify the banking entities of the Latin America and the Caribbean region by size, the methodology introduced in the 2014 study by the Inter-American Development Bank (IDB) and the Latin American Bank Federation (FELABAN) was taken into account. A Small Bank is considered an entity with less than 300 employees, or if it has more than 300 employees, it has up to 10 branches. A Medium Bank is a bank that has between 301 and 5,000 employees and between 11 and 150 branches; and a Large bank is a bank that owns more than 150 branches.



Note: 191 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Following is the classification of the 191 entities, considering the bank's number of employees and branches employing the official who filled out the questionnaire (in the country where he/she was located). For example, the total sample shows that 57 banks have less than 300 employees and up to 10 branches; and that 23 entities have more than 5,000 employees and over 151 branches.

Table 2. Distribution of banking entities by number of employees and branches

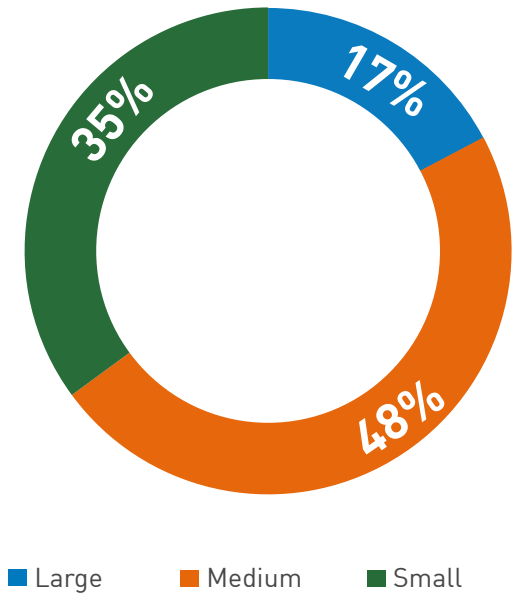
Number of Employees	Number of Branches				
	Up to 10 branches	From 11 to 50 branches	From 11 to 150 branches	More than 151 branches	Total
Up to 300 employees	57	10			67
Between 301 and 999 employees	16	22	2		40
Between 1,000 and 4,999 employees	5	17	29	8	59
More than 5,000 employees	2			23	25
Total	80	49	31	31	191

Note: 191 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

With the above information, bank entities were classified by size as follows: 35% of the sample is considered small banks, 48% are medium banks and 17% are large banks. This classification is paramount since all the analysis, conclusions and recommendations regarding the management of digital security risks and the impact of digital security incidents in this chapter bear in mind the size of the organization.

Graph 2. Distribution of banking entities by size
(large, medium and small)

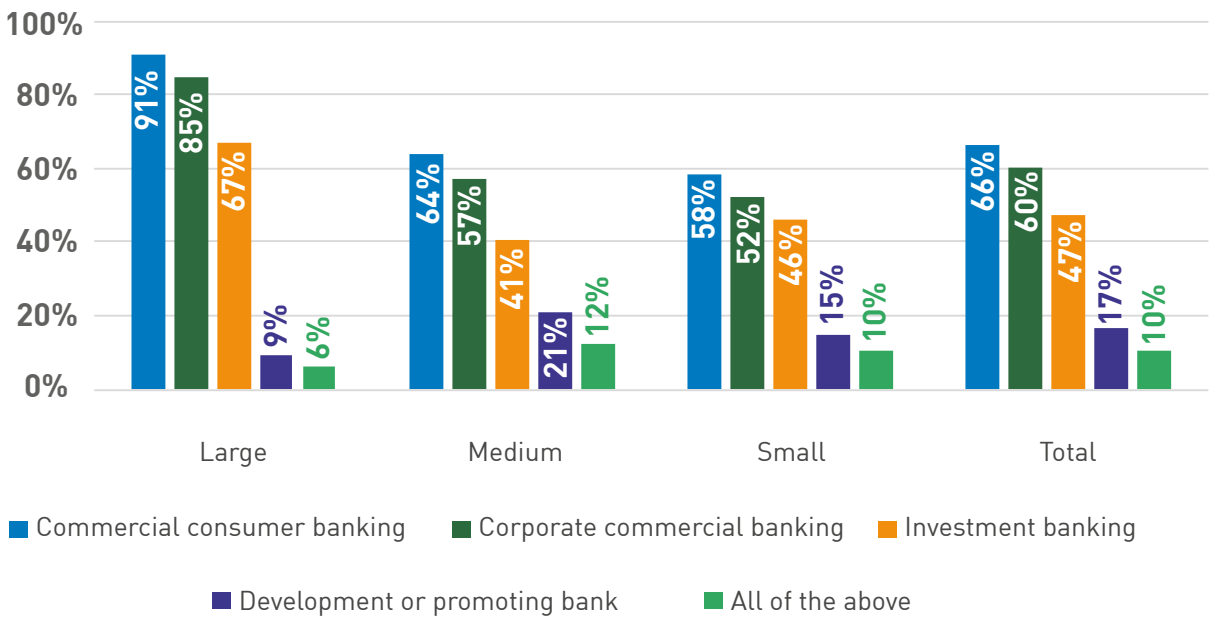


Note: 191 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Thus, it can be seen that 66% of the total number of banking entities interviewed provided commercial consumer banking services (in the country where the employee who responded the instrument was located), 60% of the total provided commercial corporate banking services, 47% of the total provided investment banking services, 17% of the total provided development or promoting banking services and 10% of the total provided all the previous services.

When analyzing by bank size and by type of banking services, some particular situations can be seen. For example, while 91% of large banks provide commercial consumer banking services, only 58% of small banks do so, or while only 9% of large banks provide development or promoting banking services, 21% of medium banks provide such services.

Graph 3. Type of banking



Note: 191 records

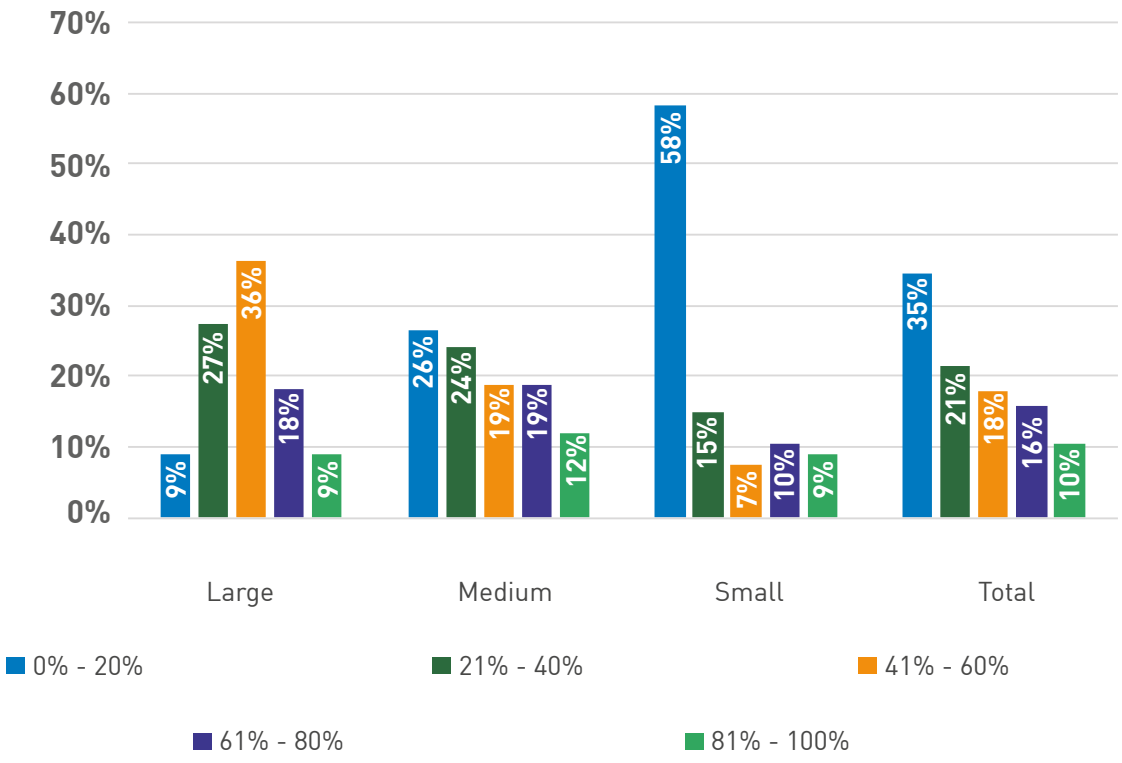
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Considering the ownership type of the bank which employs the official who answered the survey (in the country where he/she was located), it can be seen that 79% of the total sample refers to private banks (100% private capital), 13% are public banks (100% public capital) and 8% are mixed banks (comprising both public and private capital). When analyzing by bank size, only 3% of large banks are public banks while 20% of medium banks are public. Similarly, while 15% of large banks are mixed banks, only 3% of small banks have capital made up of both public and private capital.

Now, 77% of the banking entities interviewed (in the country where the employee who responded to the instrument was located) have the majority of the social capital of national origin, while 23% of the banks have capital with the majority of foreign origin resources.

When analyzing the percentage of operations performed at the bank using remote transaction channels (Internet, electronic transactions, ATMs, automatic payments, mobile telephony and audio response) of the bank's total operations during 2017, it is noted that 35% of the banks in the sample conducted 10% - 20% of their operations through remote transaction channels. When analyzing by bank size, it can be observed, for example, that only 9% of large banks performed 10% - 20% of their operations through remote transaction channels, while 58% of small banks had operations in that range.

Graph 4. Percentage of transactions that were carried out through remote transaction channels



Note: 191 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

As the bank grows, operations expand through remote transaction channels in the region and, therefore, its presence in the digital environment, its digital security risks and its need to strengthen its digital transformation strategy also increase. *"With 85% of banks identifying the implementation of a digital transformation program as a business priority for 2018, investment in technology to boost efficiency, managing evolving risks and taking advantage of growth opportunities will be critical to sustainable success"* (EY, 2018).

4.2 Digital security risk management

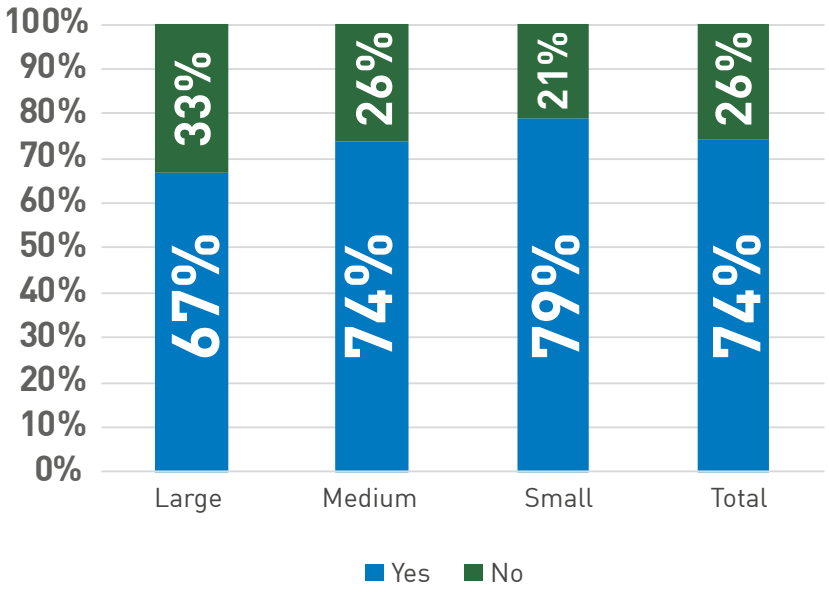
As part of the study of banking entities, a series of questions were asked regarding the management of digital security risk. These questions were asked with the purpose of evaluating the main aspects and issues related to the following topics:

- Preparedness and governance
- Detection and analysis of digital security events
- Management, digital security incident response and recovery
- Reports of digital security incidents
- Training and awareness

4.2.1 Preparedness and governance

Most of the banking entities interviewed (74%) mentioned that in their organization and in the country where the official who answered the instrument was, there is a single area responsible for digital security (including information security aspects, cybersecurity and fraud prevention using digital media). It is worth noting that as the bank grows, the areas responsible for digital security increase, since 79% of small banks have a single area as opposed to 67% of large banks.

Graph 5. Single area responsible for digital security in the bank

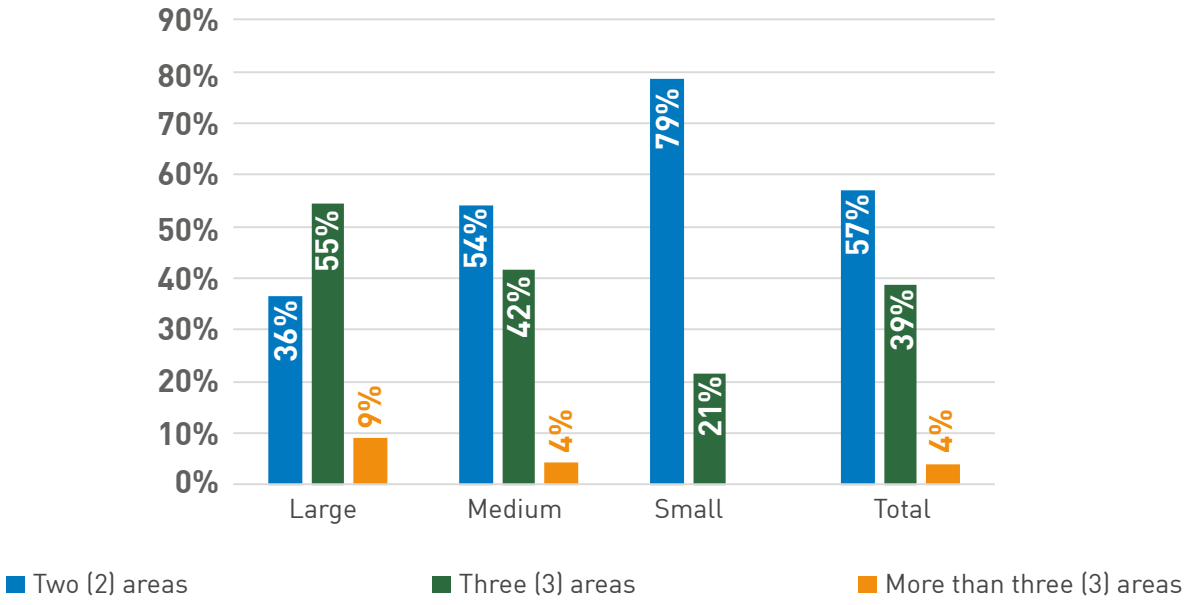


Note: 191 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Thus, of the total number of banking entities that mentioned that there were several areas with the highest responsibility for digital security (49 out of 191), it is concluded that the number of such areas depends on the size of the organization. For example, when analyzing the situation for large banks, it can be observed that 36% have two (2) areas, 55% have three (3) areas and 9% have more than three (3) areas. On the other hand, 79% of small banks have two (2) areas, while the rest (21%) have three (3) areas.

Graph 6. Areas responsible for digital security in the banking entity where there is no single area



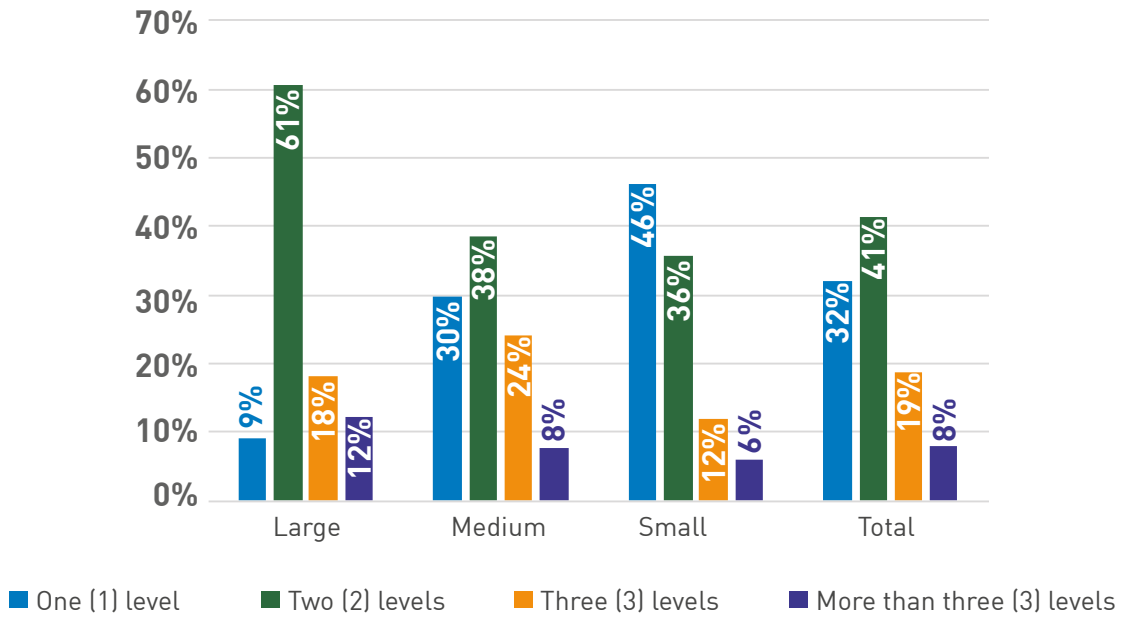
Note: 49 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Understanding that the Chief Executive Officer (CEO) of the bank would be considered the head of the bank in the country (Level 0 or Level A) and based on the results obtained, it is concluded that the hierarchical levels that exist between the CEO and the head of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) also depend on the size of the organization in the region. For example, in 46% of small banks, the head reports directly to the CEO, that is, the person is only one (1) level underneath, while only 9% of large banks would have such a situation. In 61% of large banks there would be two (2) levels between the CEO and the head of digital security. As the bank grows, the number of hierarchical levels between the CEO and the person responsible for digital security increases.

When analyzing the total sample, it can be seen that in 41% of the banks in the region there are two (2) hierarchical levels between the CEO and the head of digital security. This average situation corresponds with other related studies such as ISACA (2018) which concludes: *"43% of respondents say that their security function informs a specific level C security position."*

Graph 7. Number of hierarchical levels between the CEO and the head of digital



Note: 191 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

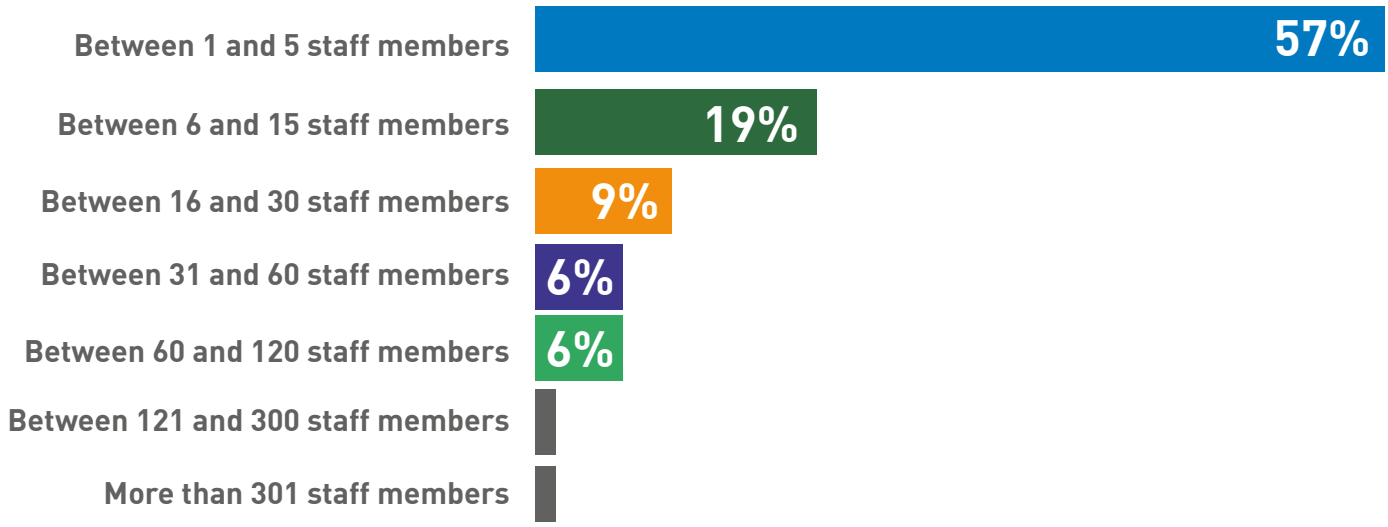
In the banking sector of the Latin America and the Caribbean region, the most common name of the position held by the head of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) is Information Security Officer (ISO). However, in most large banks (42%) the name given is Chief Information Security Officer (CISO), while in 23% of medium banks the position is called the Information Security Manager (ISM).

An important aspect regarding the preparedness and governance of digital security is the outsourcing of activities related to digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) by the organization. On average and without distinction by size of bank, the services most procured by banking entities in the region from an entity outside the organization are: *Security Testing* (65% of the total), *Monitoring of Security Infrastructure* (37% of the total), *the Monitoring of Security Controls* (20%) and *Cloud Security Services* (19% of the total).

The results for the banking sector in the region are consistent with other studies of organizations at a global level. For example, the CISCO study (2018) concluded from the sample analysis that *"among security professionals, 49% said they subcontracted monitoring services in 2017; (...) 47% outsourced incident response in 2017"*. Now, regarding outsourcing services by banking entities, it is important to recognize that such action could increase the exposure to digital security incidents: *"Almost half of the security risk of organizations occur because they have multiple providers and security products"*. (CISCO, 2018)

With regard to the size of the team that manages processes associated with digital security (including aspects of information security, cybersecurity and fraud prevention using digital media), on average a bank in the Latin America and the Caribbean region has a team consisting of seventeen (17) people. When estimating said personnel by entity size, the following is observed: a team of forty-nine (49) people on average in a large bank, a team of sixteen (16) people on average in a medium bank and a team of four (4) people on average in a small bank. Compared with other studies at a global level, the conclusion of the CISCO study (2018) stands out: *"In 2017, the median number of security professionals in the organizations was 40, a significant increase over the 2016 median of 33".*

Graph 8. People comprising the total teams that handle processes associated with digital security



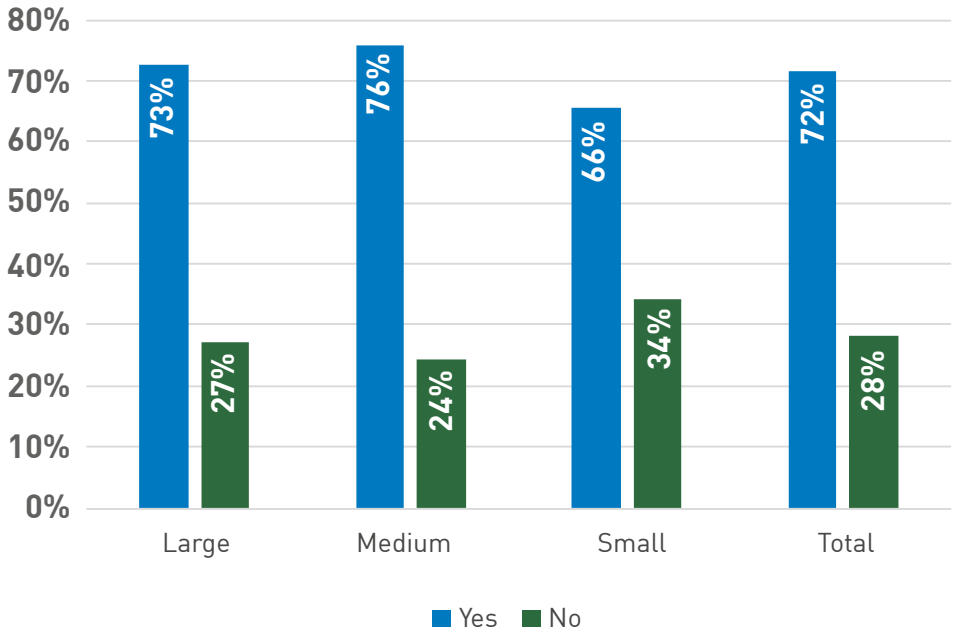
Note: 191 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Despite the presence of teams responsible for digital security in this type of organization, 82% of banking entities in the region consider it appropriate for this team to grow in the short term. It is highlighted that 15% of large banks, 16% of medium banks and 22% of small banks consider that the size of team should be maintained.

As part of the governance model of banking entities, the board of directors of 72% of banks in the region receives periodic reports on digital security indicators and risk management (including aspects of information security, cybersecurity and fraud prevention using digital media). Notable is the difference between large/medium banks and small banks, where 66% of the latter keep this practice.

Graph 9. Does the board of directors of the banking entity receive periodic reports on indicators and digital security risk management?



Note: 191 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Knowledge of digital security risk management, by the decision-makers in organizations, and especially in the banking sector, is fundamental in order to prioritize efforts and allocate resources efficiently. This has been recognized by several cybersecurity studies on the subject at the international level:

- *"Bank leadership teams recognize that cybersecurity is a fundamental priority, particularly in terms of protection against external attacks". (EY, 2018)*

- *"CEOs around the world identify cyber threats as the most concerning business threat. (...) 87% of global CEOs say they are investing in cybersecurity to build trust with customers". (PwC, 2018).*

- *"Cybersecurity remains a high-risk concern, for 84% of executives and directors, followed by compliance risk (49%) and strategic risk (38%)". (BANKDIRECTOR, 2018)*

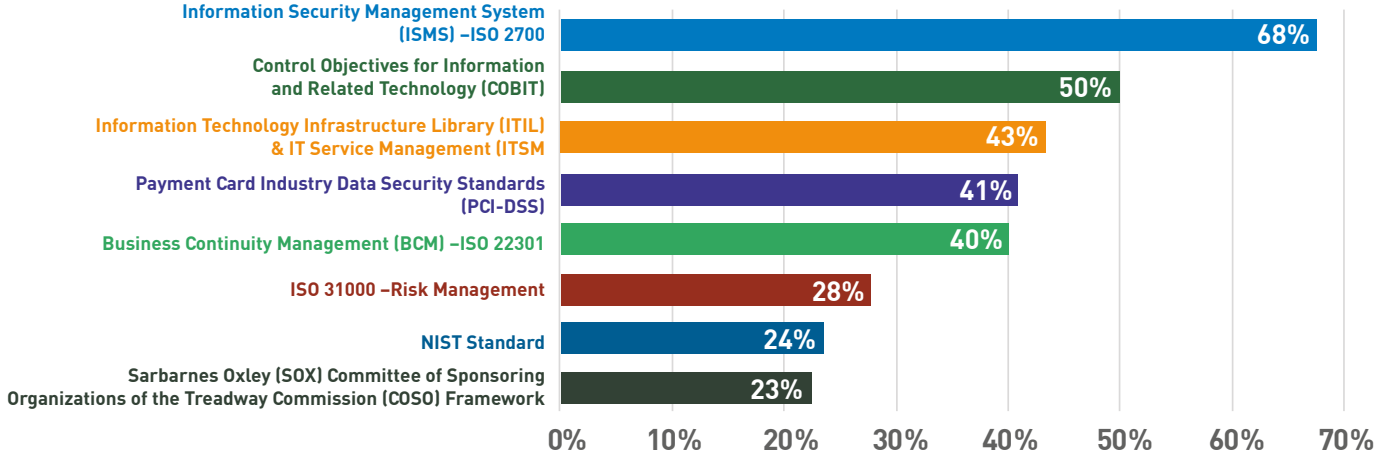
According to the results, the management of digital security management (including aspects of information security, cybersecurity and fraud prevention using digital media) in most of the banking entities in the Latin America and the Caribbean region is prepared in the framework of a *Risk Committee* (39% of the total). In the banks of the region there are also other levels of strategic management in relation to the subject such as the *Security Committee* (23% of the total) or a *Technical or Technology Committee* (21% of the total). This situation is similar to the one analyzed by BANKDIRECTOR (2018) in a study of US banks for 2017, where it was found that 34% of banks in that country manage digital security within the framework of a Risk Committee, 29% in the framework of the Board of Directors, 19% in the framework of a Technical or Technology Committee, 15% in the framework of an Audit Committee and 4% in another instance.

Regarding support for digital security risk management (including aspects of information security, cybersecurity and fraud prevention using digital media) by the bank's top management, it is highlighted that more than 60% of the total number of banking entities in the region show this: i) by requiring the adoption of good security practices (65%), ii) by promoting training and awareness in digital security (63%), and iii) promoting digital security plans (60%).

The role played by the top management and the board of organizations regarding digital security is fundamental. Globally, EY (2018) found that *"90% of the banks surveyed globally consider the improvement of cybersecurity and data security as the main business priority"*. In Latin America and the Caribbean this study finds that for most of the banking entities in the region (60% of the total), convincing the top management of the organization is moderately complex, while only 19% of organizations consider it highly complex. It is important to highlight the conclusion of ISACA (2018): *"Organizations have a little more confidence in the support of senior management and the board regarding security efforts compared to last year. 69% percent of participating organizations believe that the board of directors has given adequate priority to information security"*.

Lastly, in matters of preparedness and governance, the efficient adoption of security frameworks and/or international standards on digital security by banks in the region is worth highlighting. 68% of all banking entities mention that they have adopted *the Information Security Management System (ISMS)* – ISO 27001 standards, 50% of the total have adopted *Control Objectives for Information and Related Technology (COBIT)*, 43% of the total has adopted *Information Technology Infrastructure Library* (ITIL) & *IT Service Management (ITSM)* and 41% of the total have adopted *Payment Card Industry Data Security Standards* (PCI-DSS).

Graph 10. Security frameworks and/or international standards adopted



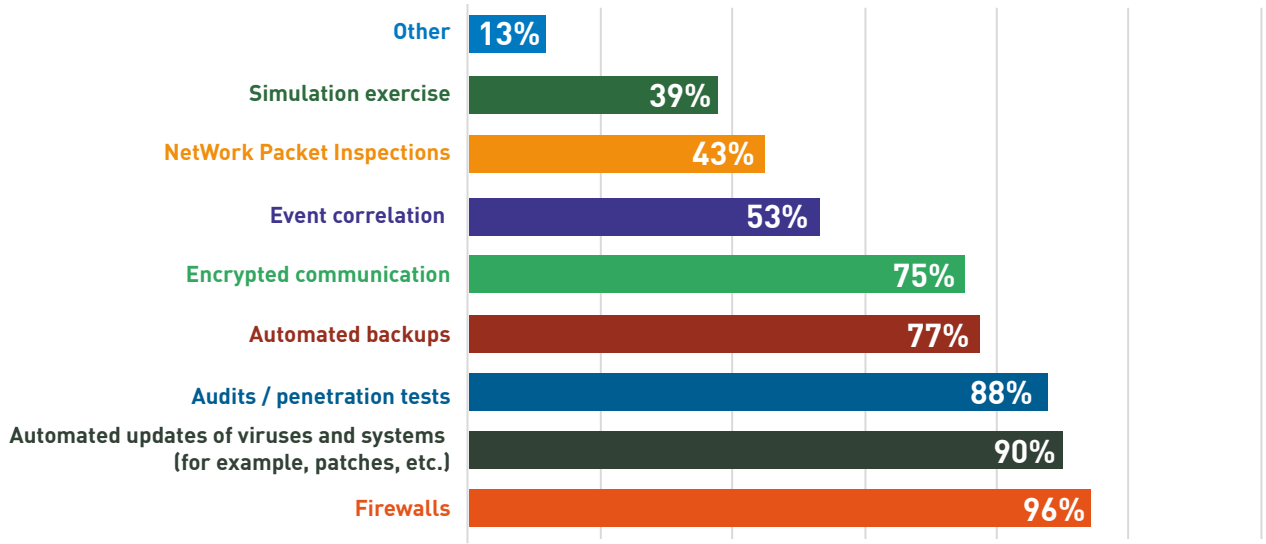
Note: 191 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

4.2.2 Detection and analysis of digital security events

According to PwC (2017), *"criminals target financial institutions because that's where the money is. Cybercrime has not changed this, but it has accelerated the speed and consequences. Entities must balance being open with being secure"*. The detection and analysis actions of digital security events are fundamental in the framework of systematic management of this type of risk. The main technical measures and actions of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) undertaken by banks in the Latin American and Caribbean region are i) firewalls (96% of the total), ii) automated updates of viruses and systems (e.g. patches, etc.) (90% of the total), iii) audits/penetration tests (88%), and iv) automated backups (77% of the total).

Graph 11. Actions and technical measures of digital security to protect critical information systems



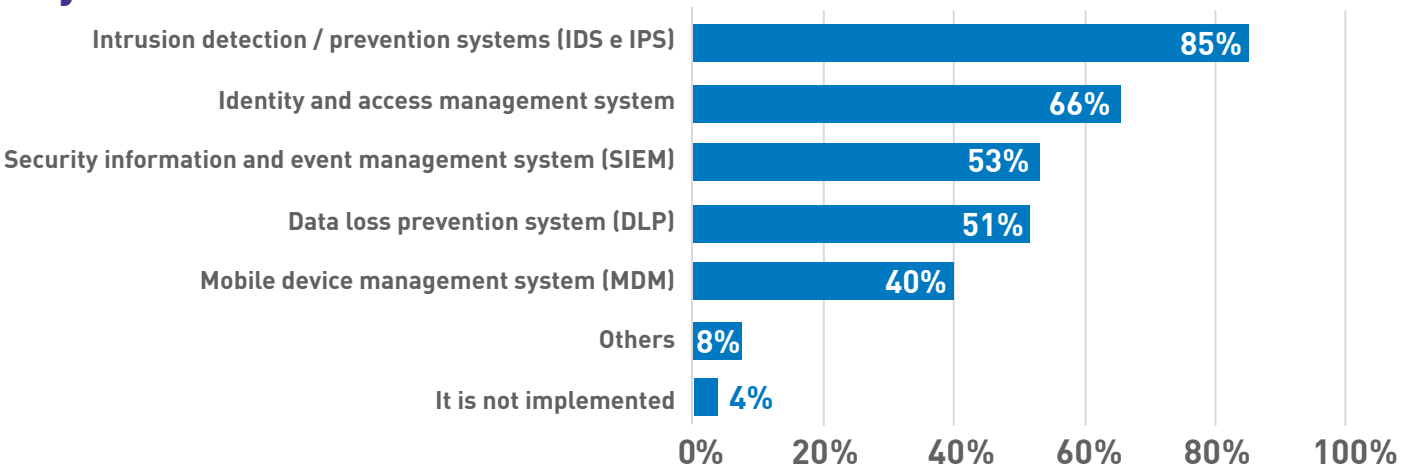
Note: 191 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

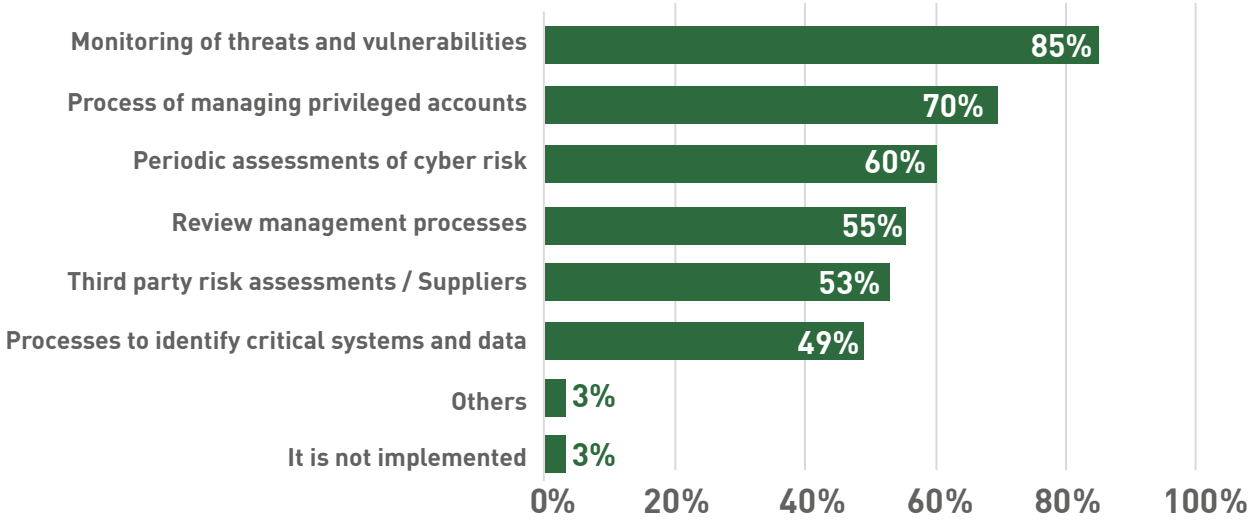
In addition, the systems implemented in the most common banking institutions in the region associated with digital security are intrusion detection/prevention systems (IDS and IPS) (85% of all banks) and identity and access management systems (66% of total banks). On the other hand, the most common processes implemented are the monitoring of threats and vulnerabilities (85% of the total of banks) and the process of managing privileged accounts (70% of the total of banks). It is necessary to emphasize the efficient implementation of this type of tools, controls and processes in the region. According to ACCENTURE (2017), globally, *"only 40% of banks have systems and processes that are properly designed in accordance with the requirements of cyber resilience"*.

Graph 12. Tools, controls and processes implemented in the banking entity

Systems



Processes

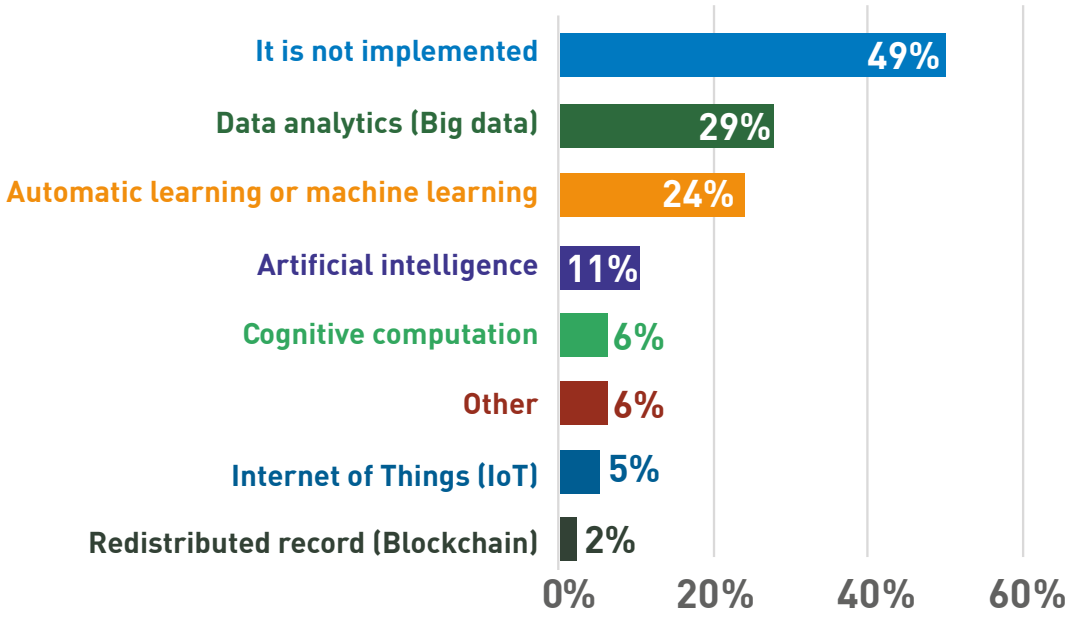


Note: 191 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

With respect to the use of emerging digital technologies applied to tools, controls or digital security processes in banking entities, EY (2018) concludes that at the global level *"banks that are investing or starting to invest in new technologies in the next three years are adopting multiple approaches to incorporate technology capabilities. (...) Artificial intelligence (AI) and advanced analytics will play a key role in preventing cyberattacks, reducing conduct risk and improving supervision to avoid financial crime"*. In Latin America and the Caribbean, 26% of large banks, 44% of medium banks and 67% of small banks mention that they are not currently implementing digital security tools, controls or processes using any of the following emerging digital technologies.

Graph 13. Emerging digital technologies applied to tools, controls or digital security processes in the bank



Note: 187 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Considering the group of banks that have implemented tools, controls or digital security processes using some emerging digital technology, the use of the following is highlighted: i) data analytics (big data) with 29% of the banks in the sample, ii) automatic learning or machine learning with 24% of the banks in the sample, and iii) artificial intelligence with 11% of the banks in the sample. It is worth noting that *"security professionals expect to spend more on tools that use artificial intelligence and machine learning in an attempt to improve defenses and help support the workload"*. (CISCO, 2018).

On the other hand, SYMANTEC (2017) concludes that *"financial institutions face attacks on multiple fronts. The two main types are attacks against their clients and attacks against their own infrastructure"* (SYMANTEC, 2017). The cyber risks that they consider deserve more attention from banking entities in the Latin America and the Caribbean region, regardless of the size of the organization, are i) the theft of a critical database, ii) the compromise of privileged user credentials, and iii) the loss of data.

Table 3. Cyber risks that deserve more attention from the bank

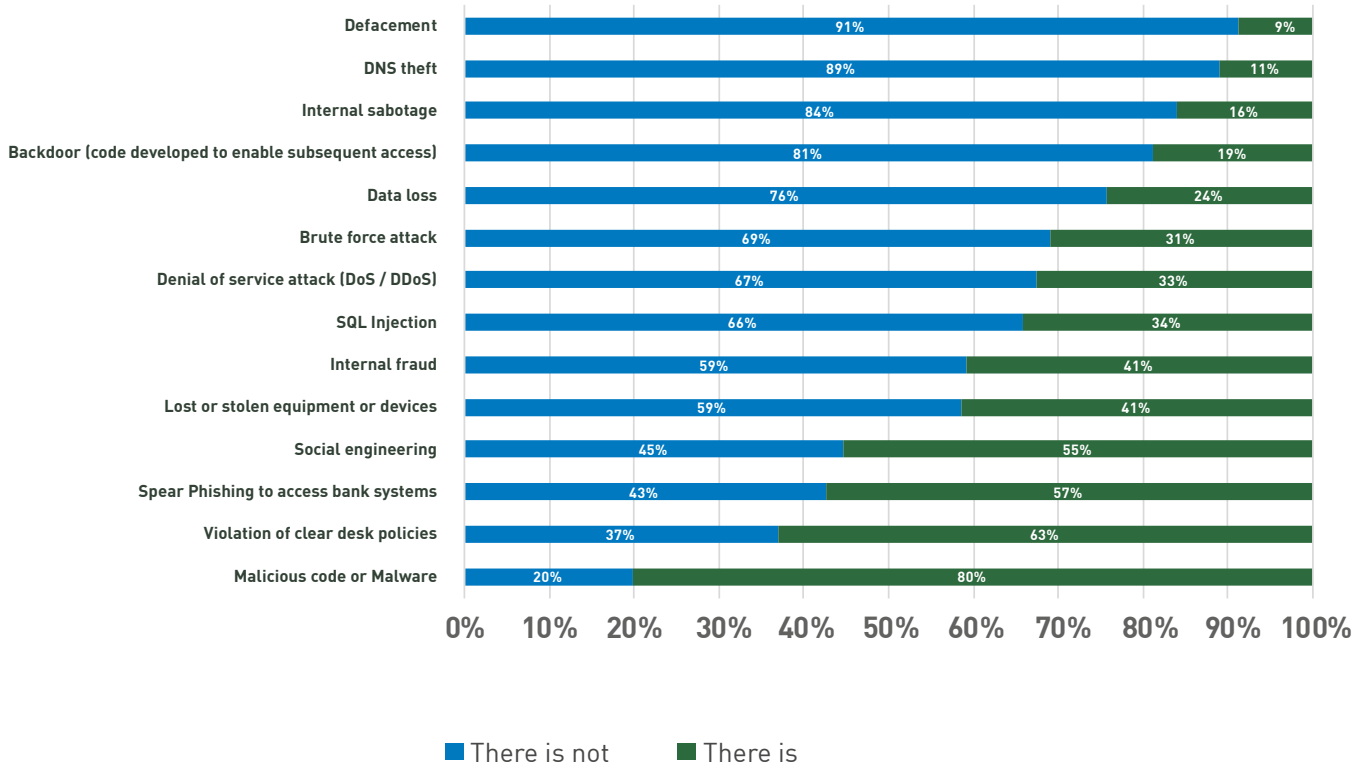
	Large	Medium	Small	Total
Theft of critical database	2,87	2,83	2,83	**2,83**
Compromise of privileged users' credentials	3,18	3,18	3,18	**3,18**
Data loss	3,57	3,61	3,57	**3,61**
Ransomware	3,77	3,70	3,73	**3,70**
Denial of service	4,25	4,29	4,33	**4,29**
Insider sabotage	4,80	4,82	4,78	**4,82**
Defacement - Website alteration	5,56	5,57	5,58	**5,57**

Note: 187 records and interviewees prioritized risks from 1 to 7, where 1 is the highest risk and 7 the lowest risk.
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

In the same study, SYMANTEC (2017) highlights for 2017 that *"another notable trend is the increase in attacks against companies and financial institutions themselves. On average, 38 percent of all detections of financial threats were in corporations. Once attackers identify an infection of this type, they log in remotely and, over time, they learn how transactions are performed. Depending on the opportunities they observe, they may try to inject fraudulent transactions into monthly bill payment orders or, in the case of a bank, try and send their own interbank transfers". Additionally, "the financial sector faces almost three times the cyber-attacks compared to other industries"* (BDO, 2017).

In this regard, it is highlighted that 176 of the 191 financial entities (92% of the total) stated that they identified some digital security event (successful attacks and unsuccessful attacks) in 2017 (including aspects of information security, cybersecurity and fraud prevention using digital media). Thus, the digital security events most commonly identified by banking entities in the region in 2017 were: i) malicious code or malware (80% of the total number of banks), ii) the violation of clear desk policies (63% of the total number of banks), and iii) directed phishing to access the bank's systems (57% of total banks). In contrast, banks in the region mentioned that the least common security events are: i) defacement (only 9% of total banks), ii) DNS theft (only 11% of all banks), and iii) internal sabotage (only 16% of the total number of banks).

Graph 14. Digital security events against banking entities that have been identified in the last twelve months

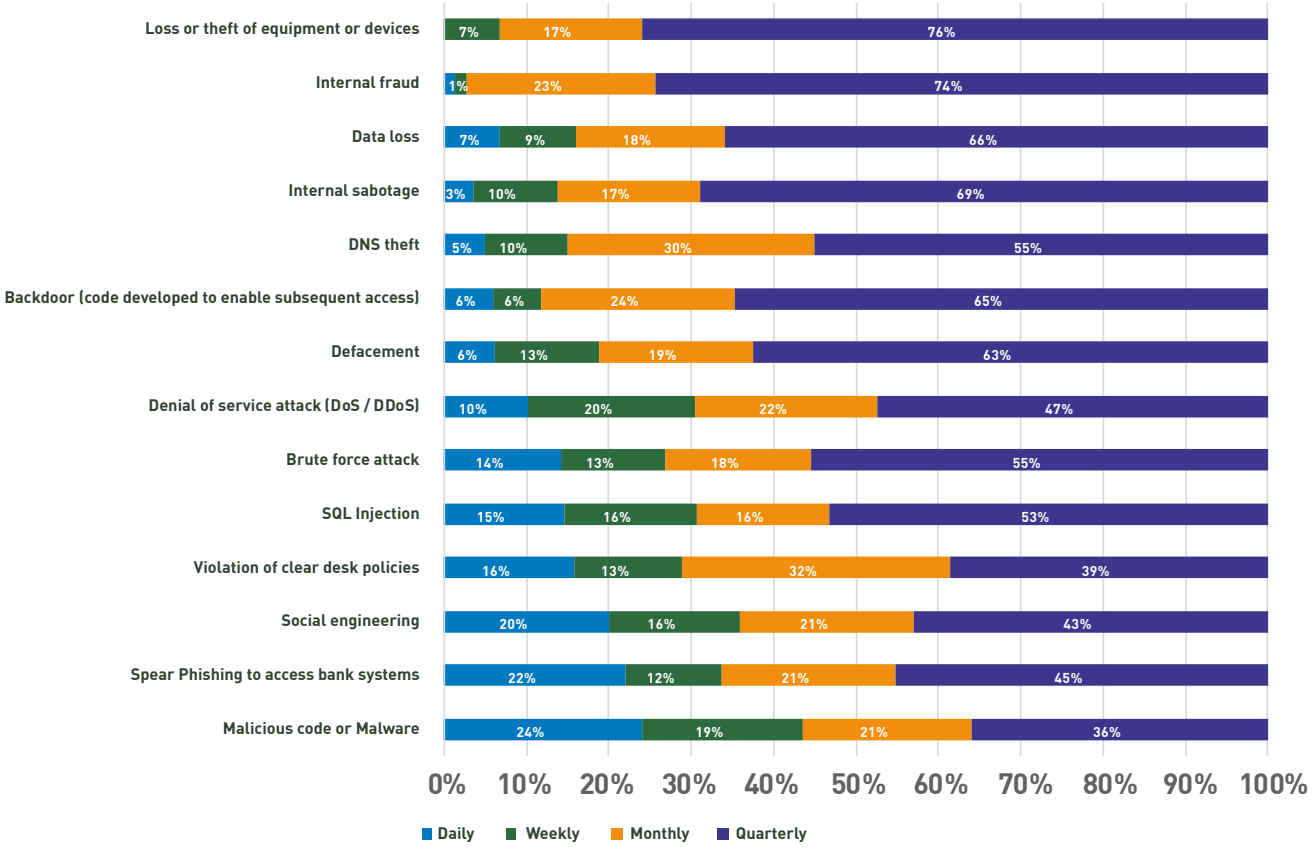


Note: 181 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

The above results are comparable with studies that are related to the identification of incidents in the financial sector, such as OFR (2017), which states that *"cyber-attacks are deliberate efforts to interrupt, steal, alter or destroy the data stored in the IT systems. Tactics include finding weaknesses in the software to enter IT systems, attack passwords (spear-phishing), attack websites to infect users with malicious software (malware) and install software that blocks users from using their own systems (ransomware)"*.

When analyzing the results regarding the approximate frequency of occurrence of events identified by banking entities in the Latin America and the Caribbean region in 2017, a particular dynamic can be seen by type of event that also depends on organization size. For example, when reviewing the frequency with which events related to malicious code or malware occur for the total number of banks in the region, the following was observed: i) 24% of the banks identified the occurrence of malware events on a daily basis, ii) 19% of the total identified this occurrence weekly, iii) 21% of the total identified this monthly, and iv) 36% of the total identified this quarterly. With respect to *Phishing targeting access to the bank's systems*, the following was observed: i) 22% of the banks identified the occurrence of this type of events on a daily basis, ii) 12% of the total identified this weekly, iii) 21% of the total identified this monthly, and iv) 45% of the total identified this quarterly.

Graph 15. Frequency of the occurrence of digital security events against banking entities



Note: 181 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

The analysis under a banking sector approach at the regional level regarding the frequency dynamics of occurrence of digital security events (successful attacks and unsuccessful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media) presents a panorama of an average occurrence. However, when reviewing the results by bank size, particular dynamics emerge. **Annex 2** presents the analysis of each of the events by bank entity size.

For example, it is highlighted that large banks were the target of attacks of all kinds of digital security events, where almost all of these entities were identified in the region. The digital security events (successful attacks and unsuccessful attacks) most commonly identified by large banks in the region in 2017 were: i) malicious code or malware (89% of the total of large banks), ii) the violation of clear desk policies (86% of the total of large banks), and iii) social engineering (86% of the total of large banks).

When reviewing the frequency with which events related to malicious code or malware occur for the total of large banks in the region, the following was observed: i) 40% of large banks detected malware events daily, ii) 24% of the they identified it weekly, iii) 24% of the total identified it monthly, and iv) 12% of the total identified it quarterly. Lastly, there is a dynamic of identification of occurrence of a variety of digital security events daily, weekly, monthly and quarterly by large banks in the region.

Table 4. Digital security events against large banking entities that have been identified during the last twelve months

	Large		
	There is not	Yes there are	Total
Social engineering	14%	86%	100%
Malicious code or Malware	11%	89%	100%
Spear Phishing to access bank systems	32%	68%	100%
Data loss	61%	39%	100%
Loss or theft of equipment or devices	39%	61%	100%
Denial of service attack (DoS / DDoS)	43%	57%	100%
DNS theft	75%	25%	100%
Violation of clear desk policies	14%	86%	100%
Internal sabotage	71%	29%	100%
Internal fraud	21%	79%	100%
Defacement	75%	25%	100%
Backdoor (code developed to enable subsequent access)	50%	50%	100%
SQL Injection	36%	64%	100%
Brute force attack	46%	54%	100%

Table 4.

	Large				
	Daily	Weekly	Monthly	Quarterly	Total
Social engineering	21%	21%	25%	33%	100%
Malicious code or Malware	40%	24%	24%	12%	100%
Spear Phishing to access bank systems	37%	11%	5%	47%	100%
Data loss	9%	18%	27%	45%	100%
Loss or theft of equipment or devices	0%	24%	24%	53%	100%
Denial of service attack (DoS / DDoS)	6%	31%	0%	63%	100%
DNS theft	0%	0%	29%	71%	100%
Violation of clear desk policies	17%	25%	33%	25%	100%
Internal sabotage	0%	25%	25%	50%	100%
Internal fraud	0%	5%	45%	50%	100%
Defacement	14%	14%	0%	71%	100%
Backdoor (code developed to enable subsequent access	7%	7%	21%	64%	100%
SQL Injection	22%	22%	6%	50%	100%
Brute force attack	27%	27%	7%	40%	100%

Note: 33 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

In relation to medium banks, it is highlighted that they were also the object of attacks of all kinds of digital security events, highlighting the identification of some by most of these entities in the region. The digital security events (successful attacks and unsuccessful attacks) most commonly identified by the medium banks in the region in 2017 were: i) malicious code or malware (86% of the total of medium banks), ii) the violation of clear desk policies (69% of the total of medium banks); and iii) Spear Phishing to access the bank's systems (66% of the total of medium banks).

When reviewing the frequency of occurrence of events related to malicious code or malware for the total of medium banks in the region, the following was observed: i) 28% of medium banks identified the occurrence of malware events daily, ii) 16% of the total identified this weekly, iii) 25% of the total identified this monthly, and iv) 32% of the total identified this quarterly. Finally, there is a dynamic of identification of the occurrence of some digital security events on a daily basis, and the rest of the events occurred monthly and quarterly on the part of the medium banks in the region.

Table 5. Digital security events against medium banks that have been identified during the last twelve months

	Medium		
	There is not	Yes there are	Total
Social engineering	40%	60%	100%
Malicious code or Malware	14%	86%	100%
Spear Phishing to access bank systems	34%	66%	100%
Data loss	68%	32%	100%
Loss or theft of equipment or devices	49%	51%	100%
Denial of service attack (DoS / DDoS)	66%	34%	100%
DNS theft	89%	11%	100%
Violation of clear desk policies	31%	69%	100%
Internal sabotage	83%	17%	100%
Internal fraud	52%	48%	100%
Defacement	92%	8%	100%
Backdoor (code developed to enable subsequent access	82%	18%	100%
SQL Injection	63%	38%	100%
Brute force attack	67%	33%	100%

Table 5.

	Medium				
	Daily	Weekly	Monthly	Quarterly	Total
Social engineering	23%	11%	21%	45%	100%
Malicious code or Malware	28%	16%	25%	32%	100%
Spear Phishing to access bank systems	21%	10%	26%	43%	100%
Data loss	4%	7%	14%	75%	100%
Loss or theft of equipment or devices	0%	2%	18%	80%	100%
Denial of service attack (DoS / DDoS)	10%	10%	33%	47%	100%
DNS theft	10%	10%	30%	50%	100%
Violation of clear desk policies	18%	11%	38%	33%	100%
Internal sabotage	7%	7%	20%	67%	100%
Internal fraud	2%	0%	17%	81%	100%
Defacement	0%	14%	43%	43%	100%
Backdoor (code developed to enable subsequent access	0%	0%	31%	69%	100%
SQL Injection	9%	9%	27%	55%	100%
Brute force attack	3%	7%	28%	62%	100%

Note: 91 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Finally, in relation to small banks, it is highlighted that they were subject to attacks of some types of digital security events, highlighting the identification of a few by most of these entities in the region. The digital security events (successful attacks and unsuccessful attacks) most commonly identified by small banks in the region in 2017 were: i) malicious code or malware (68% of the total of medium banks), ii) the violation of clear desk policies (45% of the total of medium banks) and iii) spear phishing to access the bank's systems (42% of the total of medium banks).

When reviewing the frequency of occurrence of events related to malicious code or malware for the total of small banks in the region, the following was observed: i) 9% of small banks identified the occurrence of malware events daily, ii) 23% of the total identified this weekly, iii) 11% of the total identified this monthly, and iv) 57% of the total identified this quarterly. Finally, there is a dynamic of identification of the occurrence of some digital security events on a daily basis, and of the rest of the events occurred weekly, monthly and quarterly on the part of the small banks of the region.

Table 6. Digital security events against small banking entities that have been identified during the last twelve months

	Small		
	There is not	Yes there are	Total
Social engineering	65%	35%	100%
Malicious code or Malware	32%	68%	100%
Spear Phishing to access bank systems	58%	42%	100%
Data loss	92%	8%	100%
Loss or theft of equipment or devices	80%	20%	100%
Denial of service attack (DoS / DDoS)	80%	20%	100%
DNS theft	95%	5%	100%
Violation of clear desk policies	55%	45%	100%
Internal sabotage	91%	9%	100%
Internal fraud	85%	15%	100%
Defacement	97%	3%	100%
Backdoor (code developed to enable subsequent access	94%	6%	100%
SQL Injection	83%	17%	100%
Brute force attack	82%	18%	100%

Table 6.

	Small				
	Daily	Weekly	Monthly	Quarterly	Total
Social engineering	13%	22%	17%	48%	100%
Malicious code or Malware	9%	23%	11%	57%	100%
Spear Phishing to access bank systems	15%	15%	22%	48%	100%
Data loss	20%	0%	20%	60%	100%
Loss or theft of equipment or devices	0%	0%	8%	92%	100%
Denial of service attack (DoS / DDoS)	15%	31%	23%	31%	100%
DNS theft	0%	33%	33%	33%	100%
Violation of clear desk policies	10%	7%	21%	62%	100%
Internal sabotage	0%	0%	0%	100%	100%
Internal fraud	0%	0%	0%	100%	100%
Defacement	0%	0%	0%	100%	100%
Backdoor (code developed to enable subsequent access	25%	25%	0%	50%	100%
SQL Injection	18%	27%	0%	55%	100%
Brute force attack	25%	8%	8%	58%	100%

Note: 67 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

When analyzing the type of digital security events (successful attacks and unsuccessful attacks) used by cybercriminals against users of financial services, banking entities mentioned that the events of i) phishing, ii) social engineering and iii) spyware (malware or Trojans) were the most frequent in the region. On the other hand, the less common digital security events against users were: i) self-fraud (fraud carried out by the same person who claims), ii) the key logger, and iii) internal fraud (carried out by corporate clients' officers).

In relation to digital security events against the bank identified by the banks, it is important to draw some conclusions from other studies with a global scope on the subject:

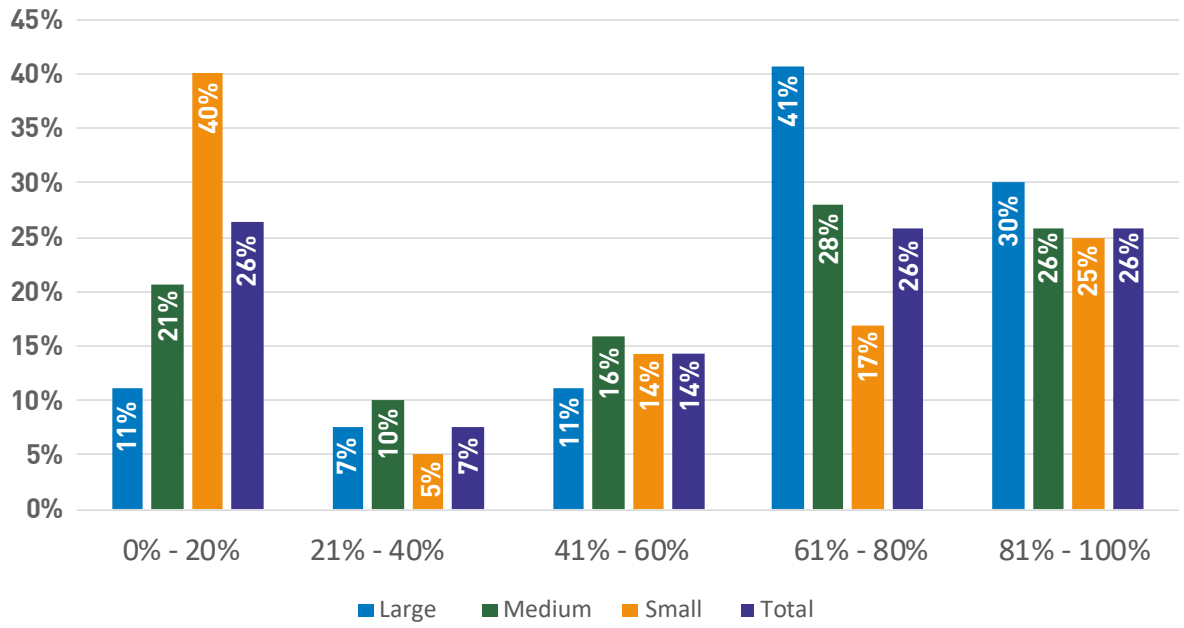
- *"No matter how much the threat landscape changes, malicious email and spam are still vital tools for adversaries to distribute malware because they carry threats directly to the endpoint. By applying the right combination of social engineering techniques, such as phishing and malicious links and attachments, adversaries just have to sit back and wait for unsuspecting users to activate their exploits". (CISCO, 2018)*

- *"Social engineering continues to play an important role in many attacks. As transaction authentication through mobile applications or text messages grows in popularity, there is also an increase in mobile malware trying to steal these credentials". (SYMANTEC, 2017)*

- *"Attacks do not just target bank customers. We have seen several attacks against the financial institutions themselves, with attackers attempting to transfer large sums in fraudulent inter-bank transactions". (SYMANTEC, 2017)*

Finally, in matters of detection and analysis of digital security events, it is highlighted that on average, 26% of banks in the region detect, by means of their own systems (and not third parties) between 0% and 20% of digital security events (successful attacks and unsuccessful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media), 7% of banks detect between 21% and 40% of events with their own systems, 14% of banks detect between 41% and 60% of events with their own systems, 26% of banks detect between 61% and 80% of events with their own systems and 26% of banks detect between 81% and 100% of events with their own systems.

Graph 16. Percentage of digital security events that are detected by the bank's own (and not third-party) detection systems



Note: 174 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

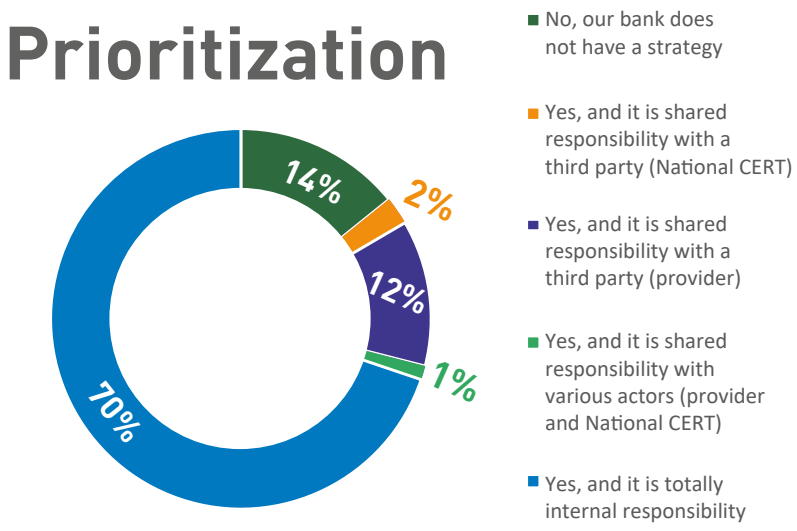
When analyzing by bank size, the majority of large banks (41%) detect between 61% and 80% of events with their own systems, the majority of medium banks (28%) detect between 61% and 80% of events with own systems and most small banks (40%) detect between 0% and 20% of events with their own systems.

4.2.3 Management, digital security incident response and recovery

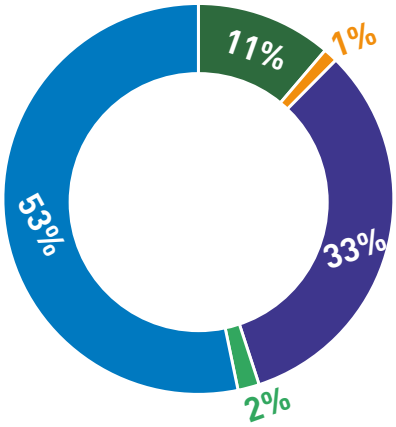
Taking into account the difference in the information collection instrument sent to banking entities between digital security event (which is the sum of successful attacks and unsuccessful attacks that the institution suffered during a period of time) and digital security incident (a total of successful attacks suffered by the institution during the same period of time), the results are analyzed below, emphasizing the latter: digital security incident management, response and recovery.

When analyzing the strategies for digital security incidents (successful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media) it is highlighted that: i) 70% of the banks in the region had and implemented a strategy to prioritize incidents under the organization's internal responsibility, ii) 53% of the banks in the region had and implemented an incident containment strategy under the organization's internal responsibility, iii) 52% of the banks of the region had and implemented an incident response strategy under the organization's internal responsibility, and iv) 53% of the banks in the region had and implemented an incident recovery strategy under the organization's internal responsibility. That is, at least half of the banks in the region had digital security incident strategies for management, response and recovery.

Graph 17. Strategies for digital security incidents (successful attacks)

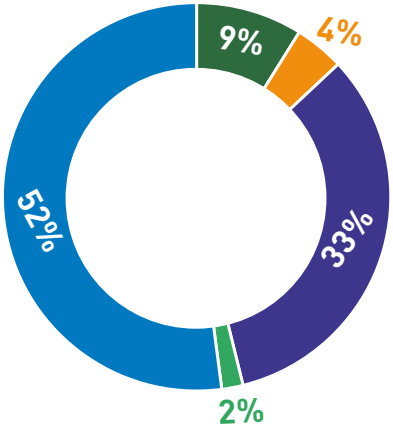


Containment



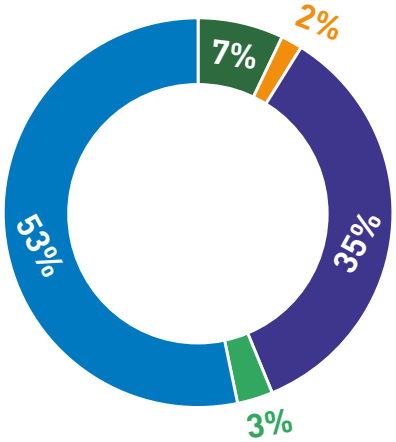
- No, our bank does not have a strategy
- Yes, and it is shared responsibility with a third party (National CERT)
- Yes, and it is shared responsibility with a third party (provider)
- Yes, and it is shared responsibility with various actors (provider and National CERT)
- Yes, and it is totally internal responsibility

Response



- No, our bank does not have a strategy
- Yes, and it is shared responsibility with a third party (National CERT)
- Yes, and it is shared responsibility with a third party (provider)
- Yes, and it is shared responsibility with various actors (provider and National CERT)
- Yes, and it is totally internal responsibility

Recovery



- No, our bank does not have a strategy
- Yes, and it is shared responsibility with a third party (National CERT)
- Yes, and it is shared responsibility with a third party (provider)
- Yes, and it is shared responsibility with various actors (provider and National CERT)
- Yes, and it is totally internal responsibility

Note: 169 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Table 7. Strategies against digital security incidents (successful attacks) by bank size

Prioritization

	Large	Medium	Small	**Total**
No, our bank does not have a strategy	3	7	14	**24**
Yes, and it is shared responsibility with a third party (National CERT)		1	3	**4**
Yes, and it is shared responsibility with a third party (provider)	6	8	7	**21**
Yes, and it is shared responsibility with various actors (provider and National CERT)		2		**2**
Yes, and it is totally internal responsibility	17	62	39	**118**
	26	**80**	**63**	**169**

	Large	Medium	Small	**Total**
No, our bank does not have a strategy	12%	9%	22%	**14%**
Yes, and it is shared responsibility with a third party (National CERT)	0%	1%	5%	**2%**
Yes, and it is shared responsibility with a third party (provider)	23%	10%	11%	**12%**
Yes, and it is shared responsibility with various actors (provider and National CERT)	0%	3%	0%	**1%**
Yes, and it is totally internal responsibility	65%	78%	62%	**70%**
	100%	**100%**	**100%**	**100%**

Table 7.

Containment

	Large	Medium	Small	**Total**
No, our bank does not have a strategy	1	6	12	**19**
Yes, and it is shared responsibility with a third party (National CERT)			2	**2**
Yes, and it is shared responsibility with a third party (provider)	16	25	14	**55**
Yes, and it is shared responsibility with various actors (provider and National CERT)		2	1	**3**
Yes, and it is totally internal responsibility	9	47	34	**90**
	26	**80**	**63**	**169**

	Large	Medium	Small	**Total**
No, our bank does not have a strategy	4%	8%	19%	**11%**
Yes, and it is shared responsibility with a third party (National CERT)	0%	0%	3%	**1%**
Yes, and it is shared responsibility with a third party (provider)	62%	31%	22%	**33%**
Yes, and it is shared responsibility with various actors (provider and National CERT)	0%	3%	2%	**2%**
Yes, and it is totally internal responsibility	35%	59%	54%	**53%**
	100%	**100%**	**100%**	**100%**

Table 7.

Response

	Large	Medium	Small	**Total**
No, our bank does not have a strategy		6	9	**15**
Yes, and it is shared responsibility with a third party (National CERT)		4	3	**7**
Yes, and it is shared responsibility with a third party (provider)	16	22	18	**56**
Yes, and it is shared responsibility with various actors (provider and National CERT)		2	1	**3**
Yes, and it is totally internal responsibility	10	46	32	**88**
	26	**80**	**63**	**169**

	Large	Medium	Small	**Total**
No, our bank does not have a strategy	0%	8%	14%	**9%**
Yes, and it is shared responsibility with a third party (National CERT)	0%	5%	5%	**4%**
Yes, and it is shared responsibility with a third party (provider)	62%	28%	29%	**33%**
Yes, and it is shared responsibility with various actors (provider and National CERT)	0%	3%	2%	**2%**
Yes, and it is totally internal responsibility	38%	58%	51%	**52%**
	100%	**100%**	**100%**	**100%**

Table 7.

Recovery

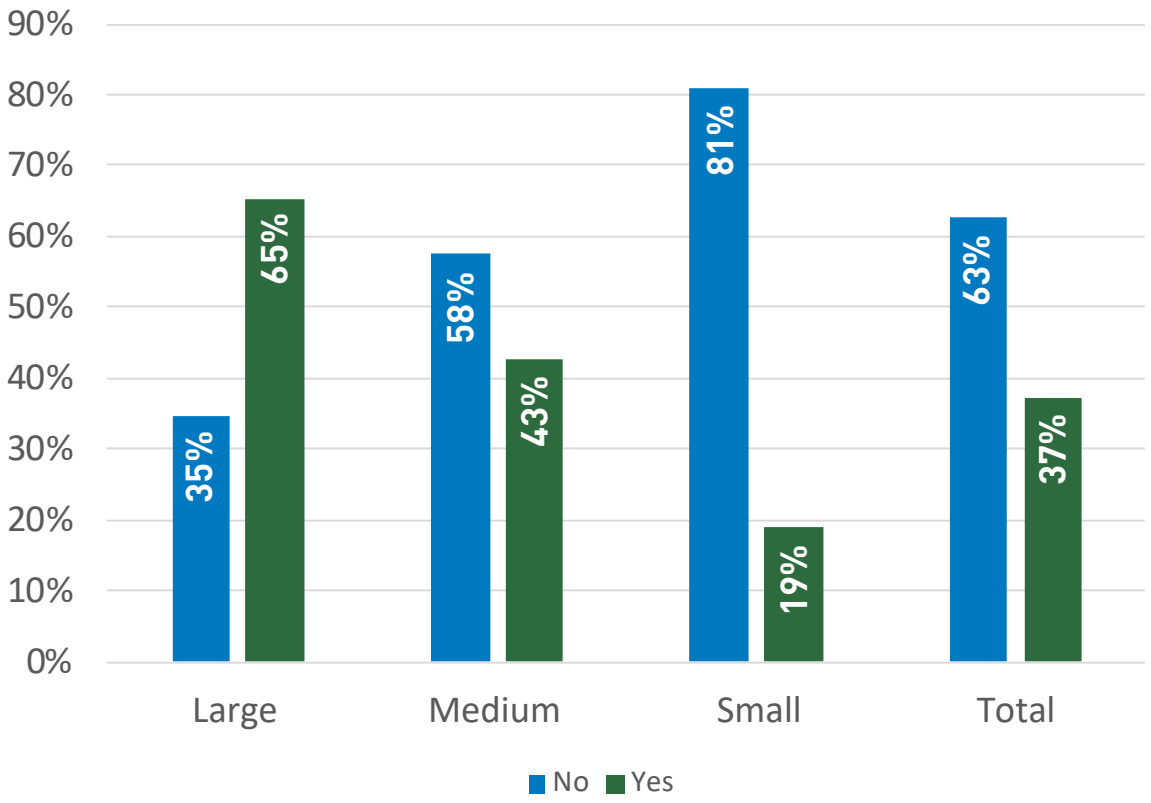
	Large	Medium	Small	**Total**
No, our bank does not have a strategy	1	3	8	**12**
Yes, and it is shared responsibility with a third party (National CERT)			3	**3**
Yes, and it is shared responsibility with a third party (provider)	16	25	18	**59**
Yes, and it is shared responsibility with various actors (provider and National CERT)		4	1	**5**
Yes, and it is totally internal responsibility	9	48	33	**90**
	26	**80**	**63**	**169**

	Large	Medium	Small	**Total**
No, our bank does not have a strategy	4%	4%	13%	**7%**
Yes, and it is shared responsibility with a third party (National CERT)	0%	0%	5%	**2%**
Yes, and it is shared responsibility with a third party (provider)	62%	31%	29%	**35%**
Yes, and it is shared responsibility with various actors (provider and National CERT)	0%	5%	2%	**3%**
Yes, and it is totally internal responsibility	35%	60%	52%	**53%**
	100%	**100%**	**100%**	**100%**

Notwithstanding the above, there is a particularity when analyzing the previous results by organizational size. The vast majority of large, medium and small banks carry out the implementation of prioritization strategies under full internal responsibility in the organization. However, the vast majority of large banks perform the execution of containment, response and recovery strategies under shared responsibility with a third party (provider) while the vast majority of medium and small banks do so under full internal responsibility in the organization.

In relation to the materialization of digital security incidents (successful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media) in banking entities in the region during 2017, it is highlighted that 65% of the large banks state that they were victims of successful attacks, while among the medium banks the percentage is 43% and among the small banks, 19%.

Graph 18. Was the banking entity, as an organization, the victim of digital security incidents (successful attacks) in the last twelve months?



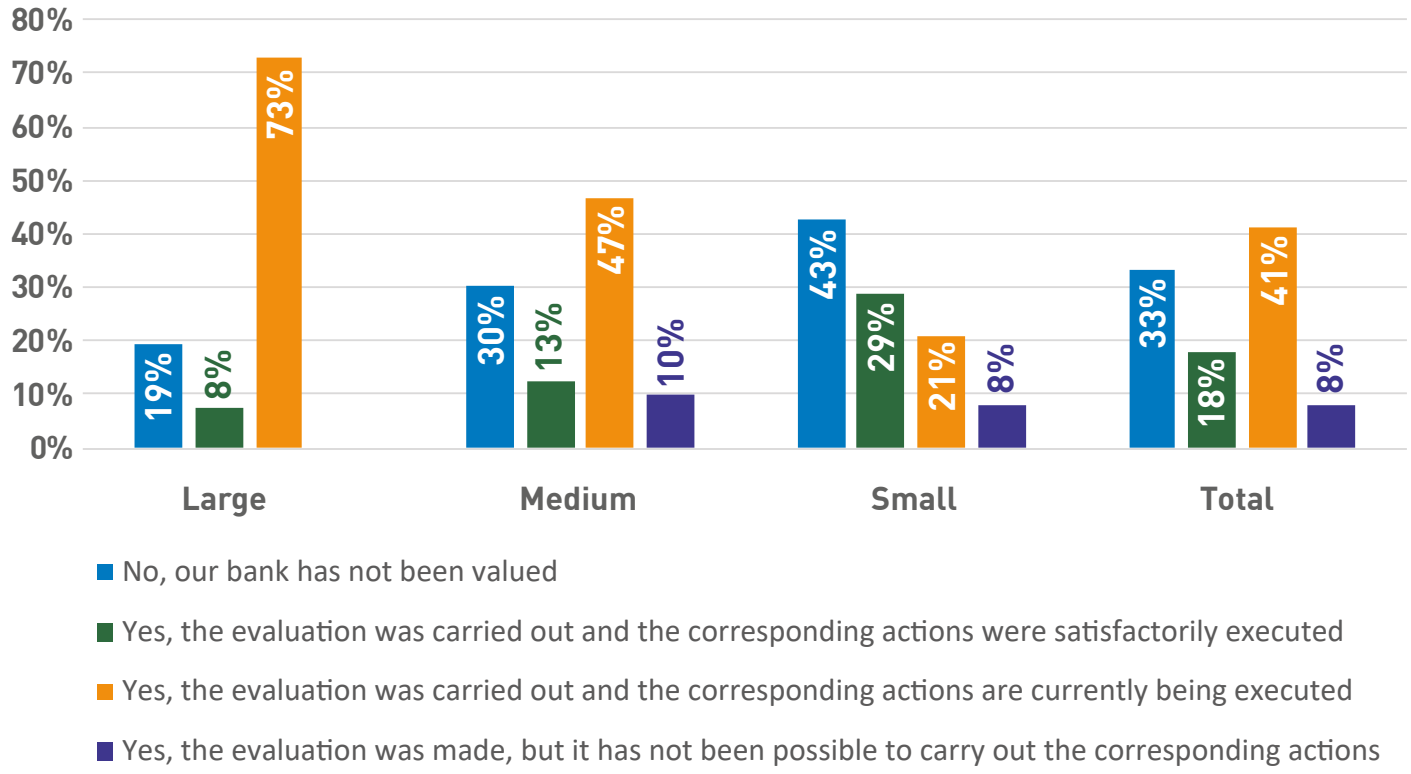
Note: 169 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Specifically, and based on the banks (63 entities) that said they were victims of digital security incidents (successful attacks), it is highlighted that almost all (90% on average) investigated the source that generated these incidents.

In addition, and as a result of the investigations, said banking entities in the region identified and prioritized the main motivations of these digital security incidents (successful attacks) suffered in 2017, which were: i) economic reasons (79% of victim banks), ii) theft of personal information (35% of victim banks), and iii) generation of reputational damage to the bank (23% of victim banks).

When asking whether the banking entities had been valued externally in the last two (2) years under some assessment methodology of the digital security maturity (including aspects of information security, cybersecurity and fraud prevention using digital media) and if they had completed said evaluation, differences were found according to the size of the organization. While 73% of the large banks in the region had conducted such an assessment and are currently carrying out the corresponding actions, only 47% of medium banks and 21% of small banks reflect this situation. In contrast, it is worrying that 30% of medium banks and 43% of small banks have never evaluated the maturity of digital security.

Graph 19. Has the bank been externally rated in the last two (2) years under any digital security maturity assessment methodology and has it completed that evaluation?



Note: 168 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Faced with this type of activity, for example, BANKDIRECTOR (2018) concludes in a banking entity study in the United States that "*all respondents say that their bank has an incident response plan established to address a cyber incident, but the 37% are not sure if that plan is effective. 69% say that the bank carried out a table-top exercise, essentially a simulated cyber-attack in 2017*". Based on the banking entities that stated that they have not fully completed an assessment of the digital security maturity or have not executed all their derived actions, these banking entities attribute it mainly to: i) insufficient specialized staff (46% of banks without evaluation), ii) lack of budget allocation (45% of banks without evaluation), and iii) lack of specific regulation that requires implementation (34% of banks without evaluation).

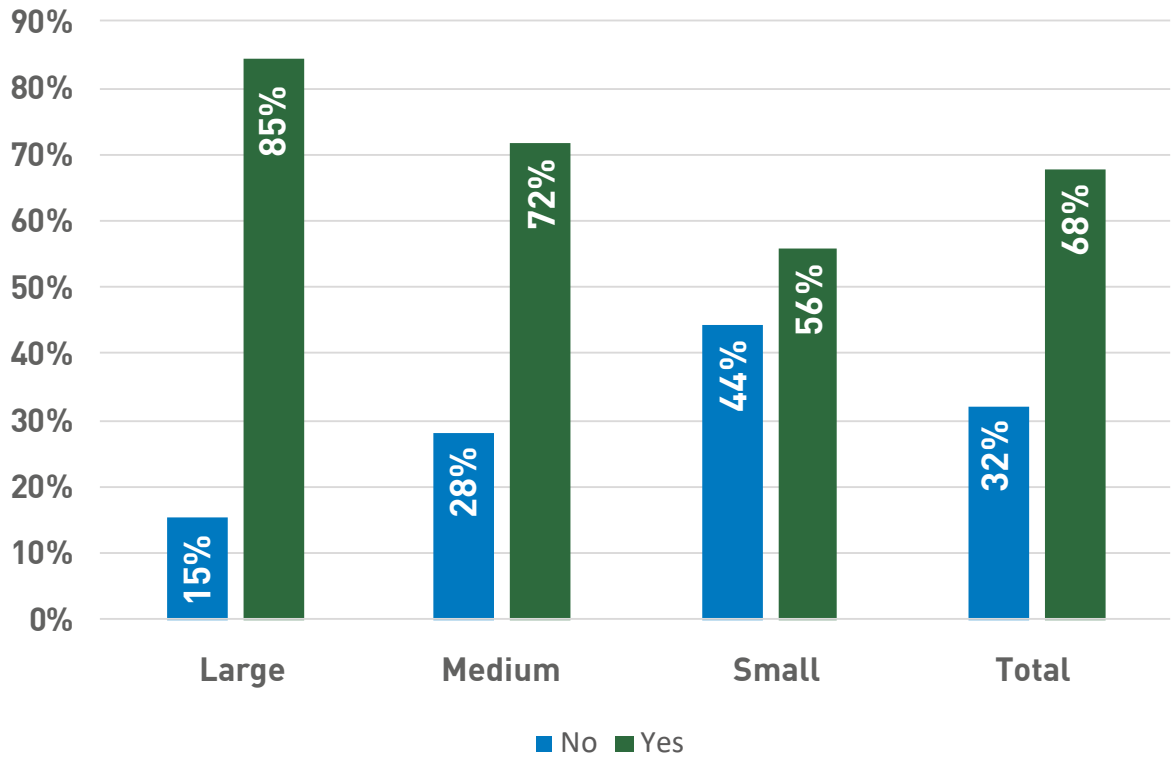
4.2.4 Reports of digital security incidents

From the analysis of results regarding the report of digital security incidents (total successful attacks to the institution during the same period of time) it is important to check whether the organizations have internal mechanisms or plans, as well as specific regulations and institutions in relation to the subject.

In general terms, it can be seen that the vast majority of banks in Latin America and the Caribbean–large (88%), medium (92%) and small (82%)–offer a mechanism for their internal users (employees and contractors) to report digital security incidents (successful attacks).

Contrary to the above, the existence of mechanisms for the financial services clients to report digital security incidents to the entity (successful attacks) varies according to bank size. It is noted that 85% of large banks and 72% of medium banks in the region offer a mechanism for their financial services clients to report digital security incidents (successful attacks) to the entity, in contrast to the 56 % of small banks.

Graph 20. Does the bank offer a mechanism for its financial services clients to report digital security incidents (successful attacks) to the entity?

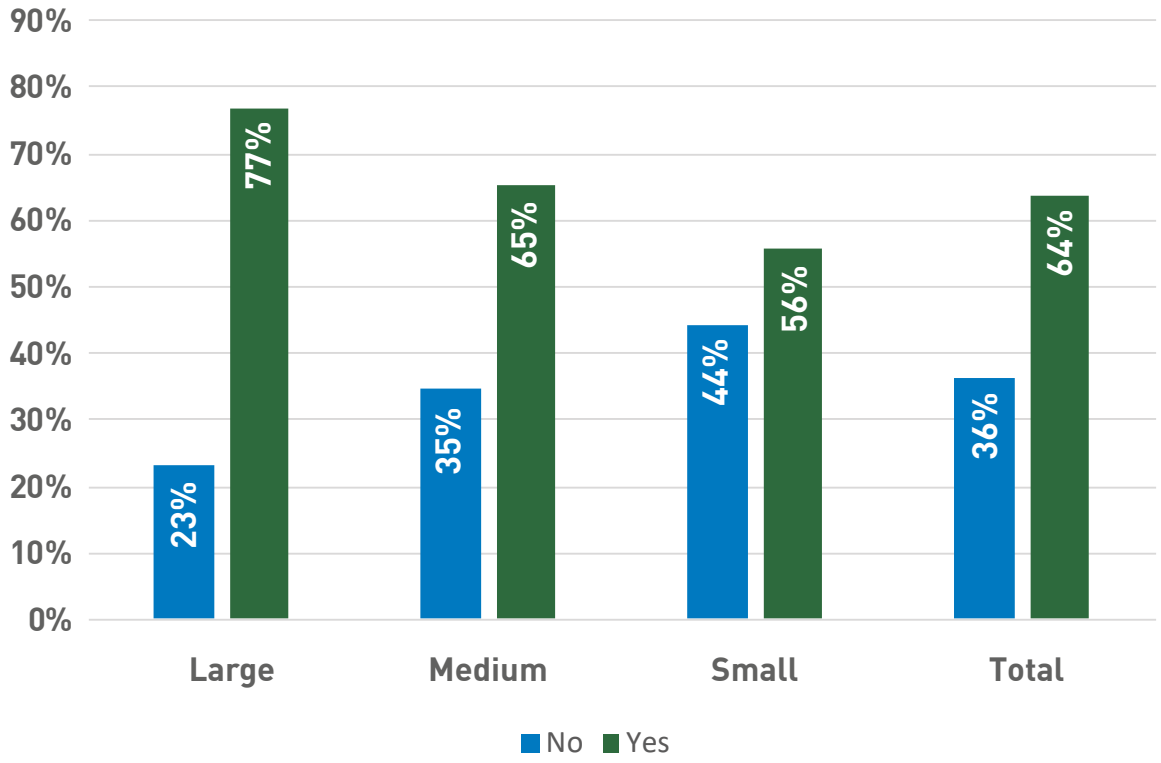


Note: 165 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Likewise, the existence of a communications plan that allows clients to report financial services when their personal information has been compromised varies according to the size of the bank. It can be seen that in most of the large banks (77%) and medium banks (65%) in the region there is a communications plan to inform their clients of financial services when their personal information has been compromised, in contrast with half the small banks (56%).

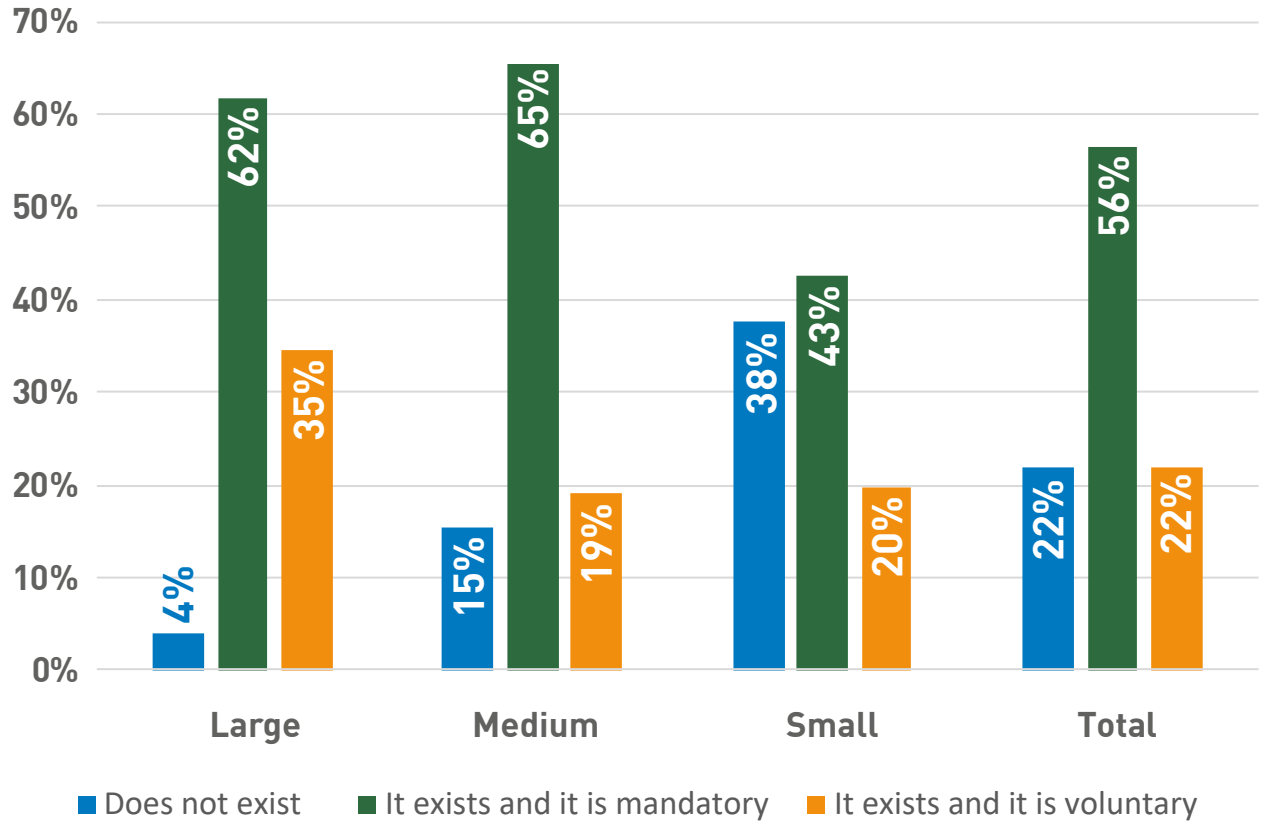
Graph 21. **Does the banking entity have a communications plan that allows its customers to be informed of financial services when their personal information has been compromised?**



Note: 165 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

In relation to the reporting of incidents (successful attacks) to a regulatory authority in the countries of the region by banking entities, differences between large and medium banks are also seen compared to small banks. 62% of large banks and 65% of medium banks versus 43% of small banks state that they know some incident report mechanism and it is mandatory because of the provisions established by a regulatory authority. On the other hand, 35% of large banks state that they know of some mechanism to report incidents and application is voluntary. It is also highlighted that only 4% of large banks in the region, in contrast to 38% of small banks, state that there is no mechanism to report incidents to a regulatory authority.

Graph 22. **Do you know any mechanism to report digital security incidents (successful attacks) by the banking entity to a regulatory authority in your country?**

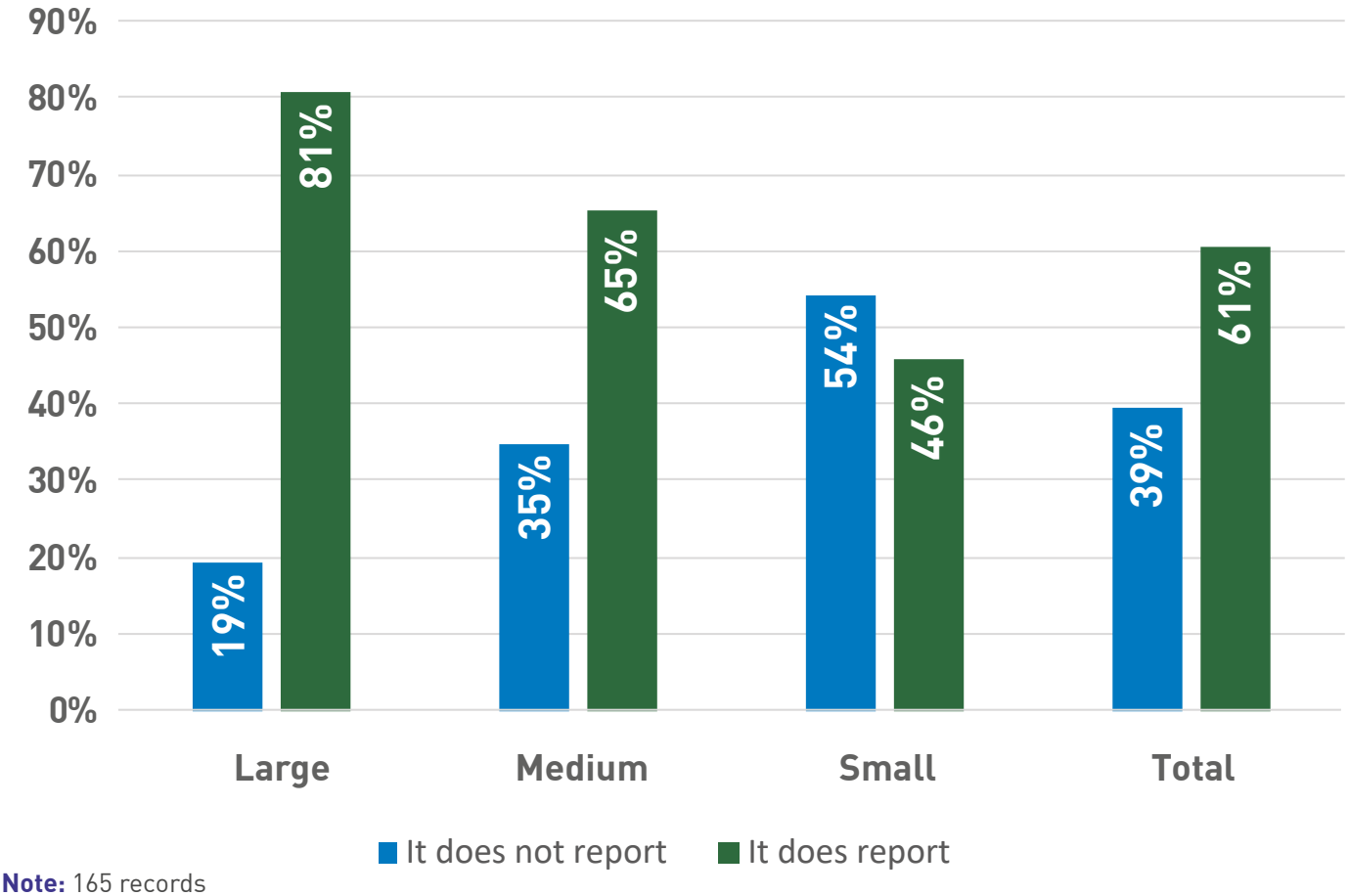


Note: 165 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Additionally, it is appreciated that while the size of the bank grows, the report of digital security incidents (successful attacks) to a law enforcement authority increases. 81% of large banks, 65% of medium banks and 46% of small banks report incidents suffered by this type of authority in the region.

Graph 23. **Does the bank report the digital security incidents (successful attacks) to a law enforcement authority?**

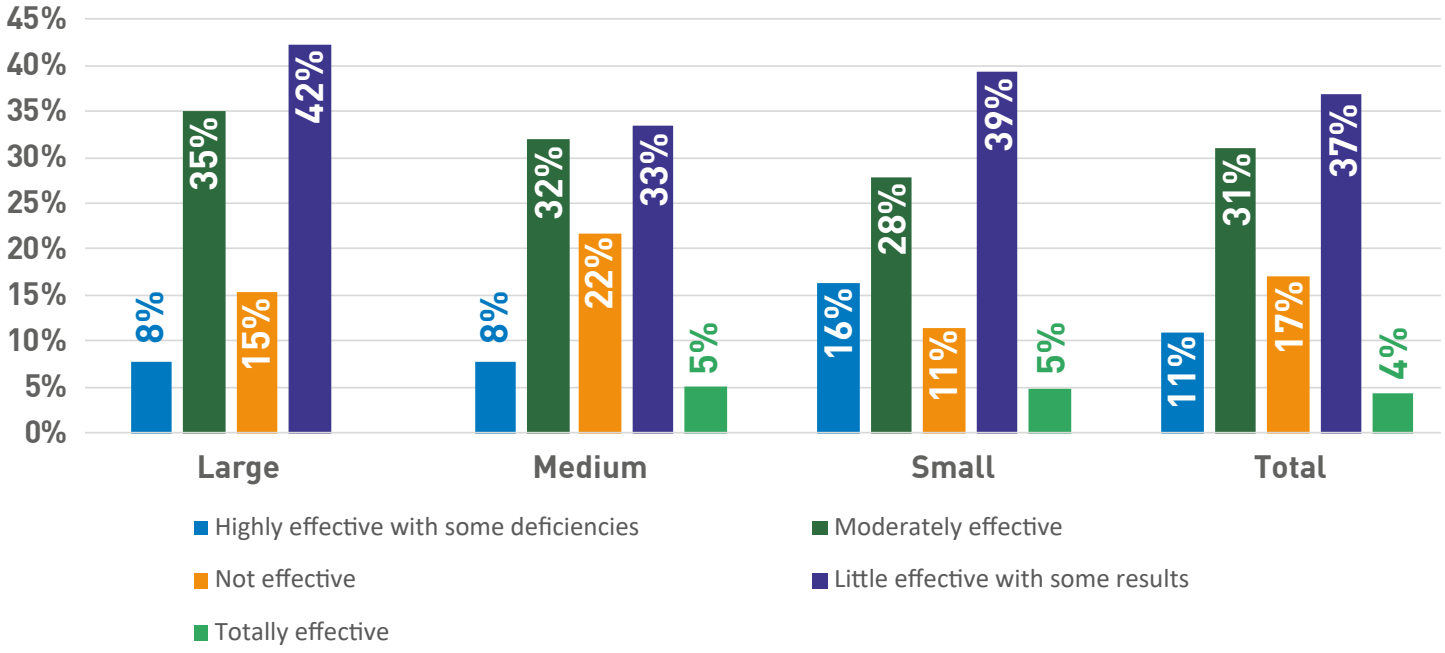


Note: 165 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Finally, it is highlighted that regardless of the size of the bank, 31% of banking entities in the Latin America and the Caribbean region consider the role of law enforcement authorities moderately effective, in relation to respond to, investigate and prosecute cybercriminals, while 37% consider the role of the aforementioned authorities as little effective in some results.

Graph 24. **How does the bank consider the effectiveness of the law enforcement authorities regarding the response to, investigation and prosecution of cybercriminals?**



Note: 165 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

4.2.5 Training and awareness

Lastly, the systematic management of digital security risks must have training and awareness actions within organizations. This topic highlights the conclusion of EY (2018): "*By instilling cybersecurity concepts and practices throughout the innovation process, banks will be able to better identify and mitigate digital risk. Cycle times can be reduced by designing security from the beginning, and a greater value is generated when the justification of cybersecurity goes from preventing infringements to allowing innovation and growth*". In particular and without distinguishing by bank size, the vast majority (82%) of banking entities in the Latin America and the Caribbean region had plans for preparation, response and training in digital security matters for their employees and bank insourcing. It is noted that only 70% of small banks have such plans in the region.

When considering the base of banking entities in the region that have preparedness, response and training plans in matters of digital security for their employees and bank insourcing, it is highlighted that 75% of them are realized annually, 16% are implemented every six months and 9% are executed annually.

On the other hand, 77% of the banking entities in the region prove the capacity of the bank's employees to adequately respond to digital security incidents and phishing and social engineering schemes on an annual basis, 11% every six months and 12% on a quarterly basis.

Finally, in relation to training and awareness-raising issues, the banking entities identified that the most effective mechanisms that have aided to create more awareness in the banking entity of digital security risks are: i) internal information training, ii) actions due to compliance with legal and/or regulatory requirements, and iii) presentations and debates at conference.

Table 8. Most effective mechanism aiding the bank to become more aware of the digital security risks

	Large	Medium	Small	**Total**
Internal information capabilities	2,00	2,02	2,03	**2,02**
Legal and/or regulatory requirements	3,37	3,39	3,42	**3,39**
Presentations and debates at conferences	4,52	4,41	4,47	**4,41**
Free publications in magazines, websites and mailing lists	4,45	4,52	4,47	**4,52**
Social networks	4,64	4,72	4,69	**4,72**
Documentation of specialized organisms in the matter	5,49	5,50	5,49	**5,50**
Specialized services by subscription	6,09	6,05	6,04	**6,05**
Professional associations	6,22	6,16	6,18	**6,16**
Other	8,22	8,22	8,22	**8,22**

Note: 165 records and all mechanisms are prioritized using a number from 1 to 9, with 1 being the most effective mechanism and 9 the least effective mechanism.
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

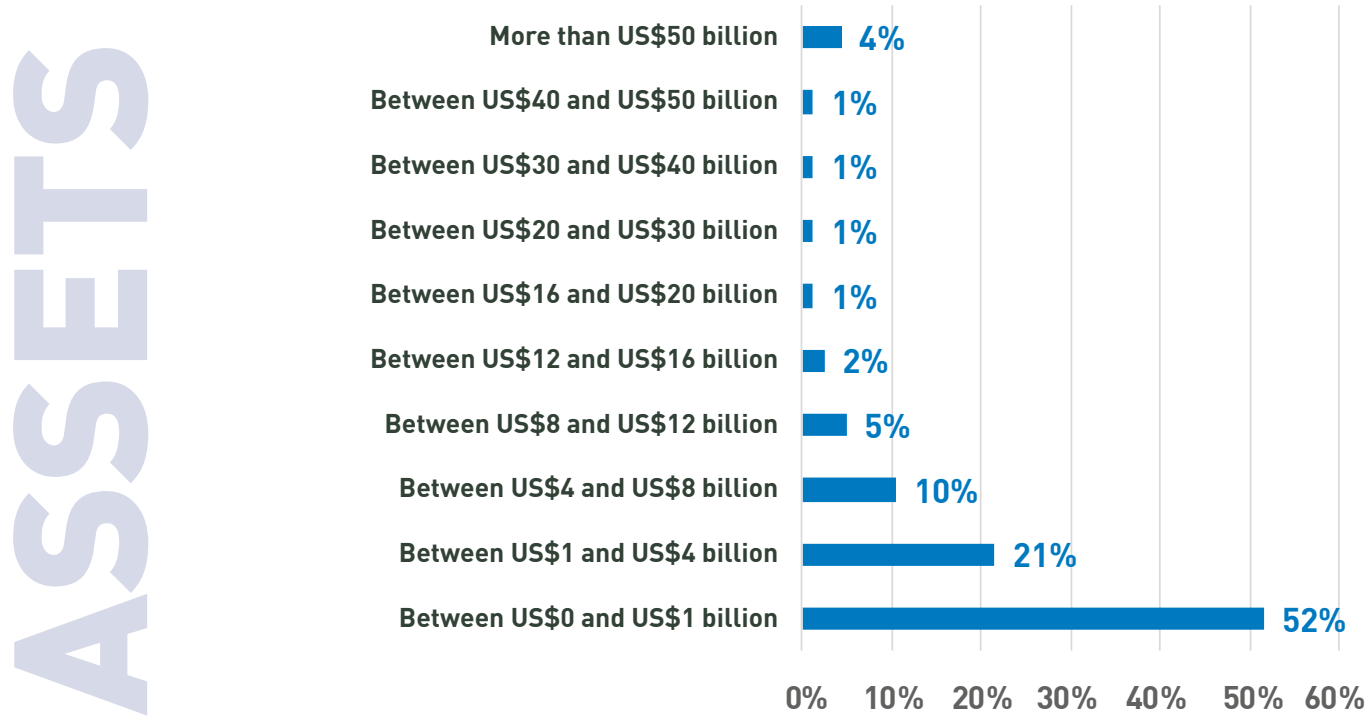
4.3 Impact of digital security incidents

Once the banking entities that participated in the development of this study were characterized and the results found on the management of digital security risks by the banking sector in the Latin America and the Caribbean region were presented, the following is an analysis of the impact of the digital security incidents in banking entities in 2017.

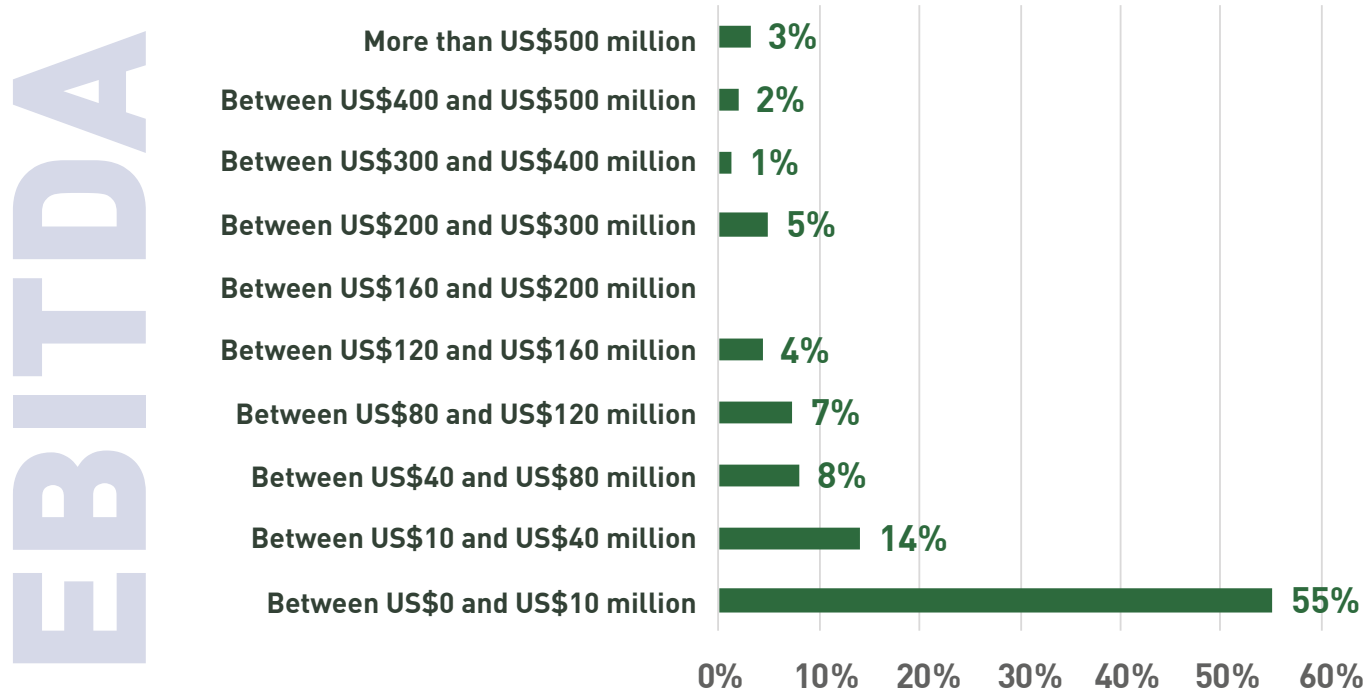
As mentioned, the sample of banking entities from which the following results are presented reached bank assets of US$1 trillion and net profits of US$10.5 billion as of December 31, 2017. This allows affirming that said sample contains a representativeness of the different levels of assets and equity of the Latin America and the Caribbean region.

It is highlighted that 52% of the banking entities stated that they reached total assets as of December 31, 2017 of US$0 - US$1 billion, 21% between US$1 billion and US$4 billions, 10% between US$4 billions and US$8 billions and 17% total assets above US$8 billions as of December 31, 2017. On the other hand, 55% of the banking entities stated that they obtained an EBITDA (Earnings Before Interests, Taxes, Depreciations and Amortizations) December 31, 2017 between US$0 and US$10 million, 14% between US$10 and US$40 million, 8% between US$40 and US$80 million and 23% an EBITDA higher than US$80 million.

Graph 25. Distribution of banking entities by values of the immediately preceding year



Graph 25.

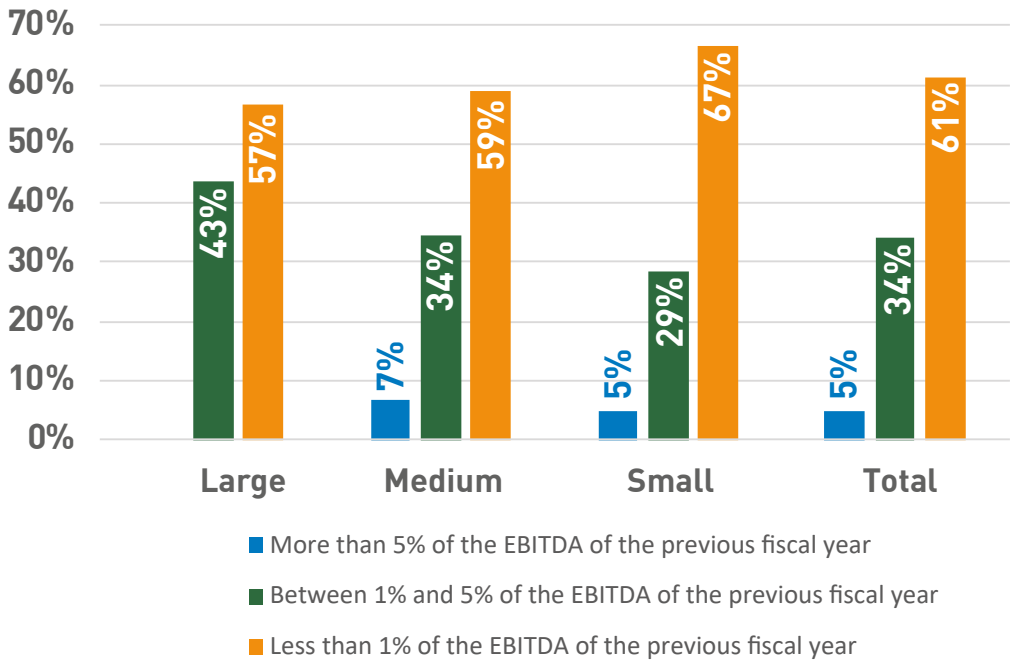


Note: 163 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Based on the banking entities that presented information, it is highlighted that 61% of the banking entities in the region stated that the digital security budget (including aspects of information security, cybersecurity and fraud prevention using digital media) is equivalent, on average, to less than 1% of the EBITDA of the previous fiscal year, 34% of the banking entities stated that the amount of said budget was between 1% and 5% of the EBITDA of the previous fiscal year and 5% said that the amount of said budget is equivalent to an amount greater than 5% of the EBITDA of the previous fiscal year.

From the analysis, it can also be inferred that as the size of the bank increases, the digital security budget increases as a percentage of the EBITDA of the immediately preceding year. For example, 43% of large banks said that the amount of said budget was between 1% and 5% of the EBITDA of the previous fiscal year, while 34% of medium banks and 29% of small banks They stated that the dedicated budget was in that range.

Graph 26. Budget of digital security as a percentage of EBITDA of the immediately preceding year



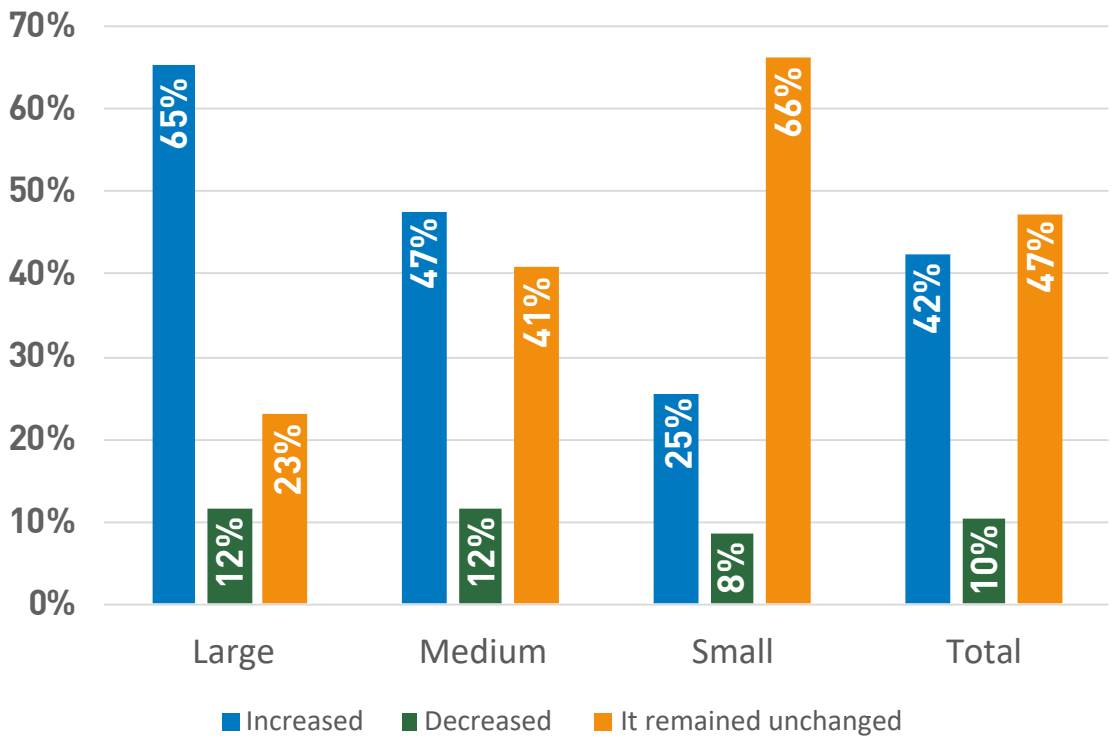
Note: 126 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

It is worth noting that other studies targeting the banking sector present estimates that could correspond to the magnitudes obtained in this study. For example, according to BANKDIRECTOR (2018), 52% of the banks in their study devoted between 1% and 5% of the revenues as digital security budget for 2017, 46% dedicated less than 1% of the revenues and only 2% dedicated more than 5% of the income. Additionally, ACCENTURE (2017) found that "*four out of ten banking entities spend between 7% and 10% of their IT budget on cybersecurity*".

In addition, compared to the immediately previous fiscal year, 46% of the banking entities in the region stated that the digital security budget remained unchanged (including aspects of information security, cybersecurity and fraud prevention using digital media), 42% said it had increased and only 10% said it had decreased.

When analyzing in detail, differences in the results were observed for each bank entity size. It is noted that for 65% of large banks, 47% of medium banks and 25% of small banks the digital security budget had increased compared to the immediately previous fiscal year. On the other hand, for 23% of large banks, 41% of medium banks and 66% of small banks, the digital security budget remained the same as that of the immediately preceding fiscal year. Finally, there is a similar percentage of large (12%), medium (12%) and small (8%) banks where the budget had decreased.

Graph 27. Dynamics of the digital security budget in the last year



Note: 163 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

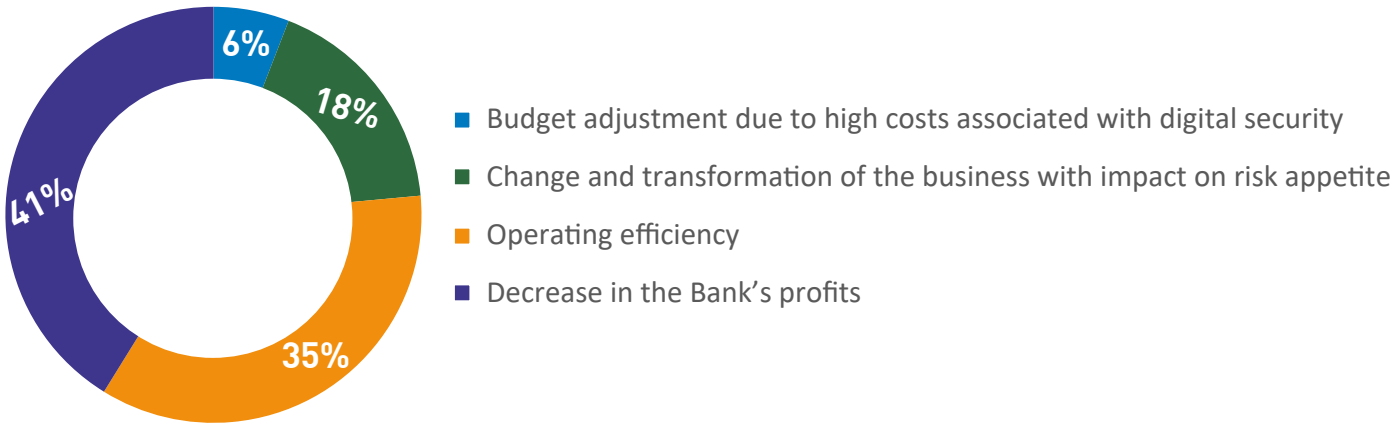
These estimates obtained from the analysis of the sample of banking entities in the Latin America and the Caribbean region also correspond to some estimates presented by ISACA (2017)–"*50% of the organizations increased the security budgets from 2016 to 2017*"–or by ISACA (2018), where it is concluded that only 8% of the organizations surveyed said that the digital security budget will decrease, while 28% said that it will remain unchanged, and 64% that the budget will increase.

Additionally, according to BANKDIRECTOR (2018), 55% of the banks in their study increased the digital security budget in 2018 up to 10% compared to that allocated in 2017, 23% of banks increased it by 10% and 25% compared to the previous year, 6% increased it between 25% and 50%, and only 1% grew more than 50%. It is highlighted that 15% of the banks in the sample remained unchanged between 2017 and 2018.

Of the total of banking entities that stated that the digital security budget had increased compared to the immediately previous fiscal year, 62% said that their increase was due to Regulatory Compliance, 55% of that sample was due to Changes and Transformation of the Business, and 54% to New threats of cybersecurity due to the use of NICT. It is worth noting that CISCO (2018) concludes that "*the most important factors that drive future investments and, therefore, improvements in technology and processes, seem to be violations. In 2017, 41 percent of security professionals said that security breaches are driving greater investment in security technologies and solutions, an increase of 37 percent in 2016*".

On the other hand, of the total of banking entities that stated that the digital security budget had decreased compared to the immediately previous fiscal year, 41% said that it was due to a *Reduction in the Bank's Profit, 35% due to Efficiency Operational, 18% to Change and transformation of the business with impact on risk appetite and 6% to Budget adjustment for high costs associated with digital security.*

Graph 28. Reasons for the decrease in the digital security budget



Note: 17 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

In relation to the decrease of budgets devoted to digital security, it is interesting to bring up some conclusions of other studies on the subject, for example:

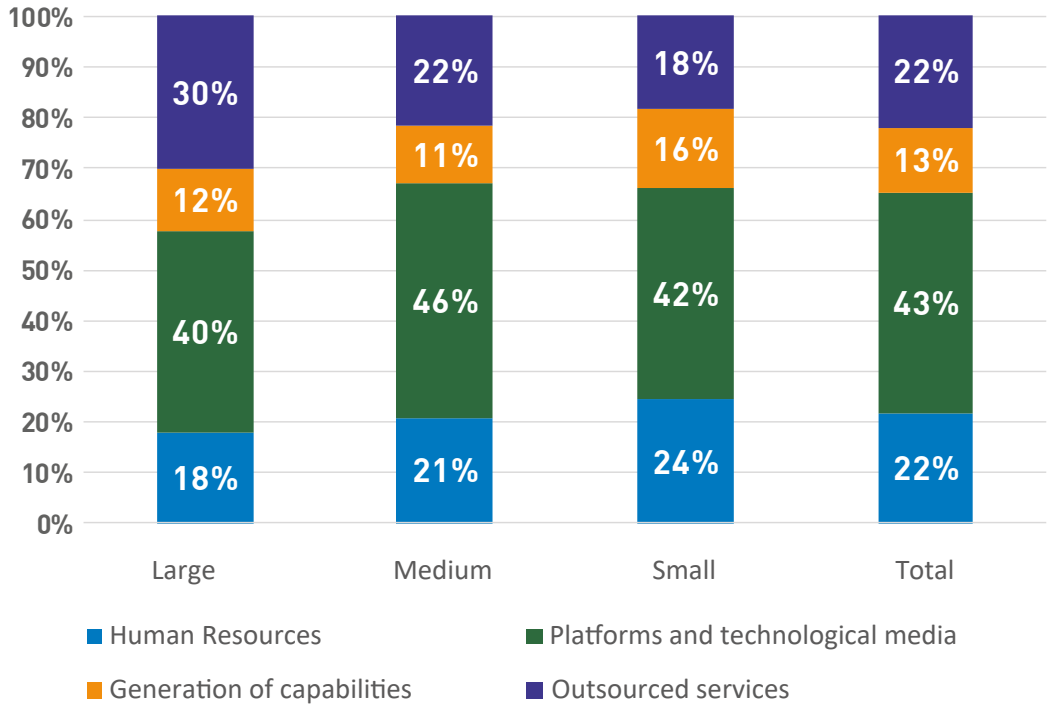
- *"Banks should treat cybersecurity as a business problem, not as an IT problem, since poor security will not only generate non-compliance and litigation costs, but will also erode the client's confidence in the organization". (CAPGEMINI, 2017)*

- *"Security professionals cite budget, interoperability and staff as their main limitations when administering security (figure 42). The lack of trained personnel is also mentioned as a challenge for the adoption of advanced technology and security processes". (CISCO, 2018)*

- *According to CISCO (2018), the main obstacles to adopting advanced technology and security processes in organizations in Latin America (Argentina, Chile and Colombia) are: budget constraints, lack of organizational culture and problems of compatibility with legacy systems.*

Now, the digital security budget (including aspects of information security, cybersecurity and fraud prevention using digital media) destined by the banking entities in the current fiscal year, shows the following distribution of the same, which was very similar, when analyzing by size of organization: 43% in *Platforms and technological media (e.g.: hardware, software)*, 22% in *Human Resources (e.g.: employees in the payroll)*, 22% in *outsourced services (e.g.: security management, outsourcing, support)* and *13% in capacity building* (*e.g. training, awareness, research*). Regarding this last category, the findings of ACCENTURE (2017) are noted: *"Only 13% would invest in cybersecurity training".*

Graph 29. Distribution of the digital security budget of the banking entity



Note: 162 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

In relation to the budget for outsourced services, the conclusions presented in WBG (2018) are: *"Financial institutions depend more and more on various IT service providers. Cloud services, in particular, are evolving, going from providing only "infrastructure as a service" (IaaS) to "platform as a service" (PaaS) and even to "software as a service" (SaaS)". And "Institutions of all sizes and risk profiles must rely, at least partially, on proprietary software applications (hence closed source) developed by third parties, which in turn are usually built on many different libraries developed by additional third parties completely unknown for the bank".*

From the estimate of the digital security budget as a percentage of the EBITDA of the immediately preceding year that the banking entities in the region spend on the size of the organization and the estimation of the percentage of budget allocated to human resources, it follows that: i) the budget assigned to an average member of the digital security team by a large bank in the region in 2017 was US$22,713 per year, ii) the budget assigned to an average member of the digital security team by a medium bank in the region in 2017 it was US$21,766 a year, and iii) the budget assigned to an average member of the digital security team by a small bank in the region in 2017 was US$13,927 a year.

Table 9. Average annual budget assigned to Human Resources, estimating one member of the bank's digital security team

Size	Up to 300 employees	Between 301 and 999 Employees	Between 1,000 and 4,999 Employees	More than 5,000 employees	Total average
Large	-	-	$20.523	$23.809	**$22.713**
Medium	-	$15.119	$27.556	-	**$21.766**
Small	$13.927	-	-	-	**$13.927**
Total average	**$13.927**	**$15.119**	**$26.260**	**$23.809**	**$19.437**

Note: 116 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

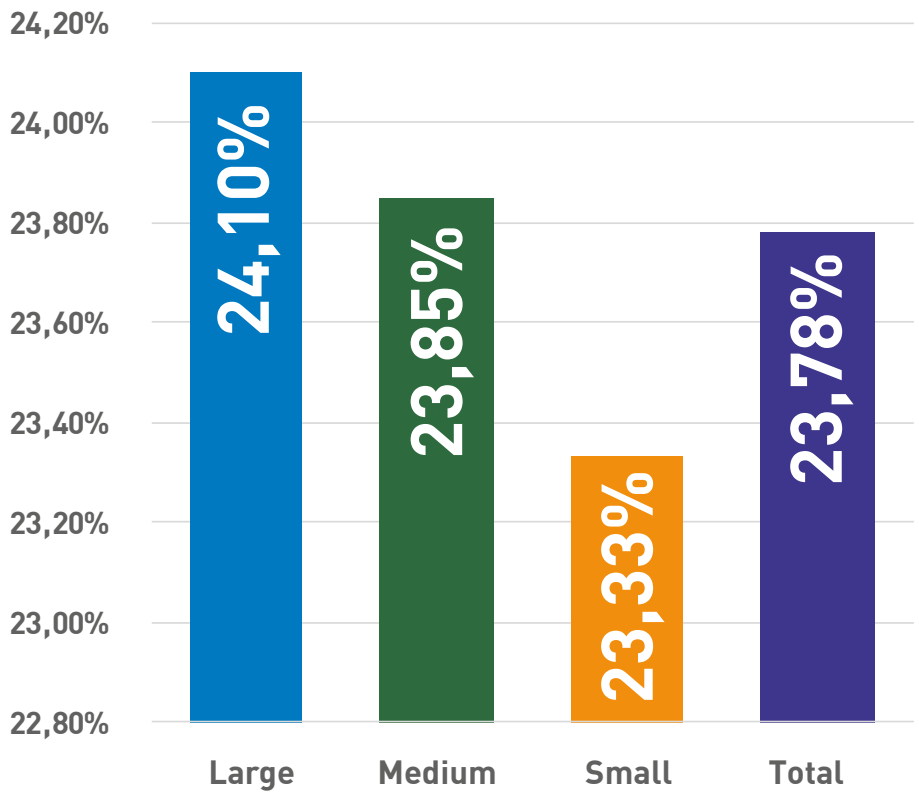
These average figures keep an adequate relationship with those that are reflected in the GLOBAL KNOWLEDGE study (2017), which indicates that the average annual salary for experts in Cybersecurity functions is US$36,025, if we consider that the cybersecurity areas also involve assistants and administrative staff, which could explain the difference with the average amounts obtained compared to amount assigned to Human Resources of the bank's digital security team.

Regarding the importance of allocating and maintaining the adequate Human Resource devoted to

carrying out activities related to security risk management, the conclusions by EY (2018) stand out: *"Cyber risk is the main risk in evolution. Our survey of global banking perspectives reveals that improving cybersecurity has become the top priority for banks in the coming year. However, since banking leadership teams focus on investing in people and technology to improve cybersecurity, they are likely to face a number of new problems, such as finding the right talent when there is a shortage of cybersecurity skills and how to integrate cyber experts in their organizations. Hiring people with the right cyber skills is one thing; helping them develop the right business and risk skills for a banking environment is another".*

On the other hand, from the information collected from the sample of banking entities, it is estimated that the return on investment in digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) amounts approximately to: i) a 24.1% for a large bank in the region, ii) 23.85% for a medium bank in the region, and iii) 23.33% for a small bank in the region.

Graph 30. Return on investment in digital security



Note: 32 records

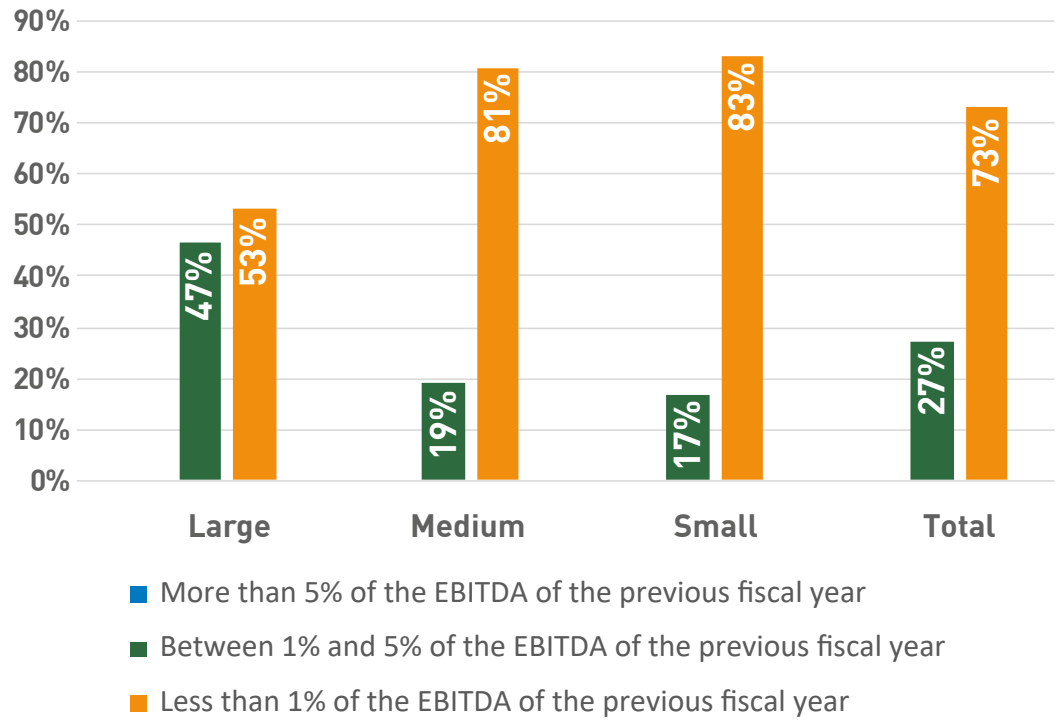
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Regarding the estimates of the return on investment in digital security: i) 20% of large banks, 8% of medium banks and 22% of small banks consider them to be low profitability returns, ii) 70%. % of large banks, 54% of medium banks and 56% of small banks consider returns to be medium profitability, iii) 10% of large banks, 31% of medium banks and 2% of small banks consider that they are high profitability returns, and iv) only 8% of medium banks consider it as very high profitability.

Now, from the banking entities that presented information, it is highlighted that 73% of the banking entities in the region said that the total cost of digital security incident response and recovery is equivalent to less than 1% of the EBITDA of the previous fiscal year; and 27% of the banking entities stated that the value of said cost was between 1% and 5% of the EBITDA of the previous fiscal year.

From the analysis it can also be inferred that as the size of the bank increases, the total cost of digital security incident response and recovery increases as a percentage of the EBITDA of the immediately preceding year. For example, 47% of large banks stated that the value of said cost was between 1% and 5% of the EBITDA of the previous fiscal year, while 19% of medium banks and 17% of small banks stated that said cost was in that range.

Graph 31. Total cost of digital security incident response and recovery as a percentage of EBITDA of the immediately preceding year



Note: 48 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Based on the information collected from the banking entities of the Latin America and the Caribbean region that participated in this study, it was possible to analyze some average indicators for the region and by organization size that allow estimating the impact of the digital security incidents in 2017. For example: i) the budget and cost related to digital security as a percentage of EBITDA of the immediately previous year, ii) the total annual cost of digital security incident response and recovery by bank, and iii) the total annual cost of digital security incident response and recovery of banking entities in Latin America and the Caribbean.

Table 10. Estimate of budget and cost related to digital security as a percentage of EBITDA of the immediately preceding year

Banks that estimated digital security budget and costs

				DigSec Budget		DigSec Cost			
Size	No. of banks	Assets (US$M)	EBITDA (US$M)	Budget as % EBITDA	Total (US$M)	Cost as % EBITDA	Total (US$M)	Budget per bank per year (US$M)	Cost per bank per year (US$M)
Large	14	269.000	3.960	1,86%	73,5	1,86%	73,5	USD 5,253	USD 5,253
Medium	21	59.500	920	2,14%	19,7	1,38%	12,7	USD 0,939	USD 0,605
Small	11	62.500	130	2,27%	3,0	1,36%	1,8	USD 0,269	USD 0,161
Total	**46**	**391.000**	**5.010**	**2,09%**	**96**	**1,52%**	**88**	**USD 2,091**	**USD 1,913**
Participation in 191 banks		40%	47%				**Profits/Assets**	**1,28%**	

Table 10.

Banks that estimated digital security budget and costs

	No. of banks	Assets (US$M)	EBITDA (US$M)	Budget as % EBITDA	Total (US$M)
Total	126	724.500	9.265	1,87%	171
Participation in 191 banks		74%	87%		

Profits/Assets 1,28%

Banks with complete answers

	No. of banks	Assets (US$M)	EBITDA (US$M)
Total	191	977.500	10.675

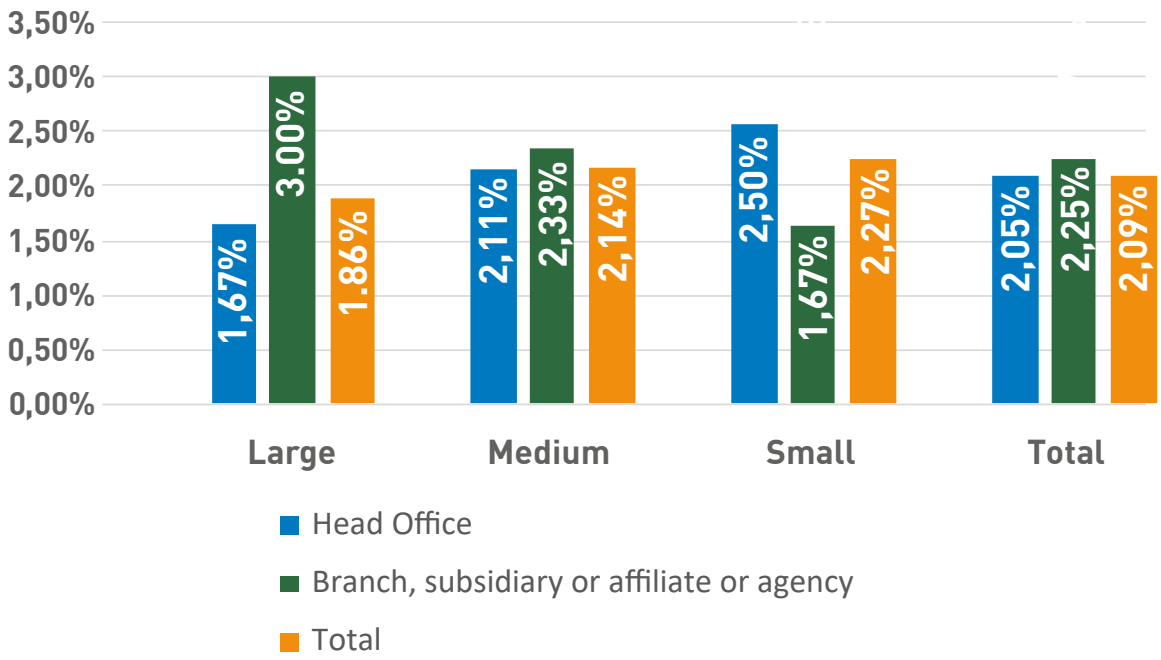
Profits/Assets 1,28%

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

For example, from the sample of banking entities that reported information on average, it is concluded that: i) the budget allocated to digital security by an average bank in the region is approximately 2.09% of the EBITDA of the immediately preceding year and ii) the total cost of responding to and recovering from digital security incidents for an average bank in the region is equivalent to approximately 1.52% of the EBITDA of the immediately preceding year.

When analyzing by size of the organization, it is highlighted that the budget allocated to digital security by a large average bank in the region is equivalent to approximately 1.86% of the EBITDA of the immediately previous year, to 2.14% of said EBITDA for an average bank and 2.27% of said EBITDA for an average small bank. From the analysis, it is highlighted that the budget as a percentage of EBITDA of the previous year for entities that are Head Offices in the country decreases as the size of the bank increases, while the budget as a percentage of EBITDA for entities that are a bank Branch, Subsidiary or Agency in the country increases as the size of the bank increases.

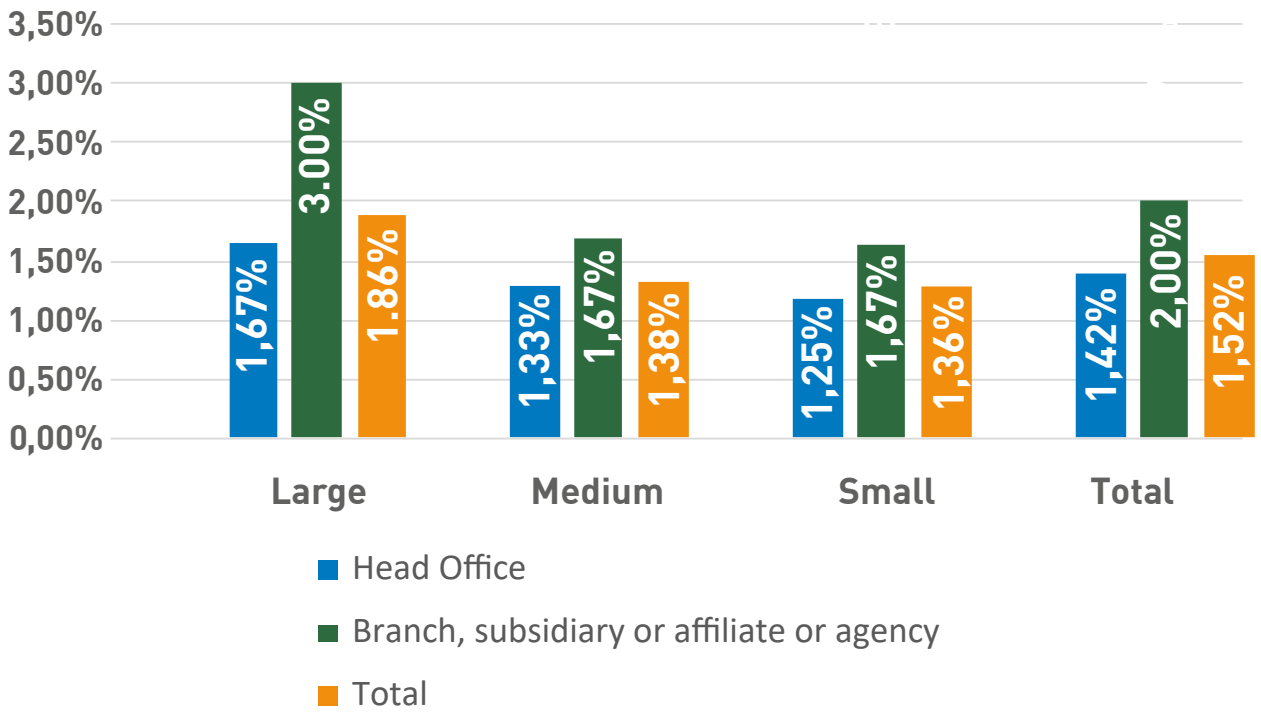
Graph 32. Budget allocated to digital security as a percentage of EBITDA of the immediately previous year, considering whether it is i) Head Office or ii) Branch, Subsidiary or Agency of the banking entity



Note: 46 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

On the other hand, the total cost of digital security incident response and recovery for a large average bank in the region is equivalent to approximately 1.86% of the EBITDA of the immediately preceding year, to 1.38% of said EBITDA for a bank average and 1.36% of said EBITDA for an average small bank. Contrary to what was found in relation to the budget for digital security, it is highlighted that the total cost as a percentage of EBITDA of the previous year increases as the size of the bank increases, regardless of whether the bank is Head Office or Branch, Subsidiary or Agency.

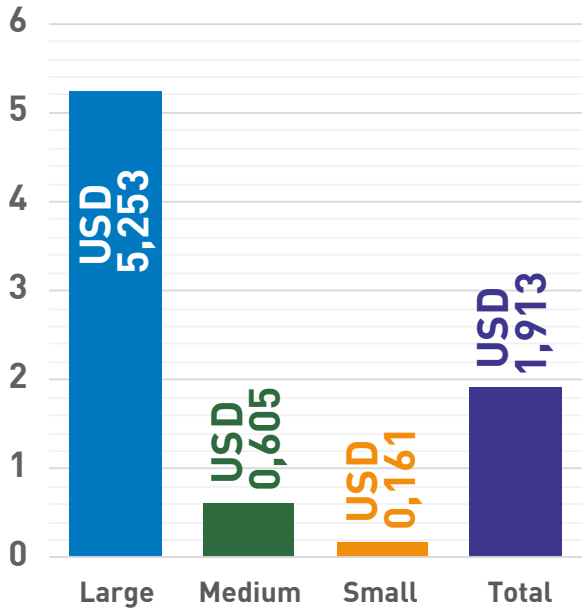
Graph 33. Total cost of digital security incident response and recovery as a percentage of EBITDA of the immediately previous year, considering whether it is i) Head Office or ii) Branch, Subsidiary or Agency of the bank



Note: 46 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

When analyzing the results in absolute terms, it is estimated that the total cost of responding to and recovering from digital security incidents for an average large bank is approximately US$5,253,000 per year, for an average medium bank approximately equivalent to US$605,000 per year and for an average small bank equivalent to approximately US$161,000 per year.

Graph 34. **Total annual cost of digital security incident response and recovery by banking entity (millions of US dollars)**



Note: 46 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

These estimates correspond to the results of other regional and global studies on the subject:

- According to BANKDIRECTOR (2018), banks in the United States with assets greater than US$10 billion budgeted on average US$5 million for digital security expenses (including personnel and technology), banks that have assets between US$1 billion and US$10 billion budgeted on average between US$200,000 and US$450,000 and banks that have assets under US$1 billion budgeted between US$50,000 and US$105,00.

- *"Violations cause a real economic damage to the organizations, damages that can take months or years to be solved. According to survey respondents, more than half (53 percent) of all attacks resulted in financial damages of over US$500,000, including, among others, loss of income, customers, opportunities and out-of-pocket costs"*. (CISCO, 2018)

• *"Respondents report that banks budgeted a median of US$200,000 for cybersecurity expenses, including staff and technology". (BANKDIRECTOR, 2018)*

From the sample of banking entities that reported information, on average it is estimated that the total cost of digital security incident response and recovery of banking entities in Latin America and the Caribbean reached US$809 million for the year 2017.

Estimation of the total annual cost of digital security incident response and recovery of banking entities in Latin America and the Caribbean (millions of US dollars)

Accumulated Net Income Bank Entities LAC Dic2017 (FELABAN) = US$53.17 billion approx.

Total cost of digital security incident response and recovery as a percentage of EBITDA = 1,52%

Total annual cost of digital security incident response and recovery of banking entities in LAC in 2017 = US$53,17 billion x 1,52% = US$809 million approx.

4.4 Econometric analysis of the results

Next, econometric estimations are conducted where the objective is to find the factors that determine whether a bank was a victim of attacks on digital security. The starting point is cross-sectional information where the analysis unit corresponds to Latin American banks that responded to the respective survey. The following are included as dependent variables: a set of indicators that seek to capture the characteristics of the financial institution, digital security risk management, preparedness and governance, detection and analysis of digital security events, tools, controls and processes implemented in the banking entity, management, digital security incident response and recovery, reporting of digital security incidents, training and awareness, and impact of digital security incidents.

The model used in the estimation presents discrete dependent variable {0,1}, LOGIT or PROBIT type, chosen according to the best fit. This type of models is widely used in the literature and employs a normal cumulative distribution function (FDA). In this case the dependent variable (y) takes the value of 1 if the bank was a victim of digital security events and 0 otherwise. As mentioned in the previous paragraph, independent variables related to the aforementioned topics were included in order to estimate the probability of existence of events to digital security or other interpretation and find the factors that determine that a bank has the characteristic "events to digital security".

Regarding the estimation of this type of models, it is carried out through the maximum likelihood method using successive iterations. The estimation aims to establish the overall significance of the estimated model. Likewise, it focuses on the individual significance of independent variables to establish their relevance as an explanatory factor of the probability of events to digital security in banking entities. The above is in order to determine whether the associated factor increases or decreases the probability of event occurrence. Finally, the marginal effects of the explanatory variables on the probability of existence of events to digital security will be calculated to determine their contribution.

The description of the variables used and that can potentially be part of the model is shown in the following table:

Table 11. Variables used in the model used of the LOGIT type - Banks

TYPE	VARIABLE	DESCRIPTION
Inherent characteristics of the financial institution	Property	Considering the type of property, the bank to which you belong (in the country where you are located), is a
Inherent characteristics of the financial institution	Social capital	Indicate where the majority of the share capital of the bank to which you belong (in the country where you are located) comes from
Inherent characteristics of the financial institution	Employees	How many employees does the bank to which you belong (in the country where you are) have?
Inherent characteristics of the financial institution	Branch offices	How many branches does the bank to which you belong (in the country where you are) have?
Inherent characteristics of the financial institution	Non-contact operations	Of the total operations of the bank to which you belong (in the country where you are), what percentage was made through non-contact transactional channels (Internet, electronic transactions, ATMs, automatic payments, mobile telephony and audio response) during the last twelve months.
Preparedness and governance	Digital Security Area	In the bank to which you belong (in the country where you are located) is there a single area responsible for digital security (including aspects of information security, cybersecurity and fraud prevention using digital media)?
Preparedness and governance	Digital security responsibility	How many areas have the maximum responsibility for digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) in the bank to which you belong (in the country where you are located)?
Preparedness and governance	Hierarchical levels	Understanding that the CEO of the bank to which you belong (in the country where you are located) is the head of the institution (Level 0), how many hierarchical levels are there between the CEO and the head of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media)? (for example, if the head reports directly to the CEO, it would be one level)
Preparedness and governance	Responsible position of digital security	What is the name of the position held by the head of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) in the bank to which you belong (in the country where you are located)?)?
Preparedness and governance	Outsourcing related to digital security	What outsourcing has the bank to which you belong (in the country where you are) hired to carry out the following activities related to digital security (including aspects of information security, cybersecurity and fraud prevention using digital media)? Multiple answers may be possible

TYPE	VARIABLE	DESCRIPTION
Preparedness and governance	Teams associated with digital security	How many people make up all the teams that manage processes associated with digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) in the bank to which you belong (in the country where you are located), not including personnel from companies that provide outsourcing? Do you consider it appropri-ate for this team to grow in the short term?
Detection and analysis of digital security events	Digital security reports	As part of the governance model of the institution, does the board of directors of the bank to which you belong (in the country where you are) receive periodic reports on indicators and digital security risk management (including aspects of information security, cybersecuri-ty and fraud prevention using digital media)?
Detection and analysis of digital security events	Senior management in digital security management	How does the top management of the bank to which you belong (in the country where you are) manage the digital security (including aspects of information security, cybersecurity and fraud prevention using digital media)?
Detection and analysis of digital security events	Senior management support for digital security risk	How does the top management of the bank to which you belong (in the country where you are) demonstrate the support for digital security risk management (including aspects of information security, cybersecurity and fraud prevention using digital media)? Multiple answers may be possible.
Detection and analysis of digital security events	Investment in digital security solutions	How complex is it, in your opinion, to convince the top management of the bank to which you belong (in the country where you are) to invest in digital security solutions (including aspects of information security, cybersecurity and prevention of fraud using digital media)?
Tools, controls and processes implemented in the bank	Security frames	Has the bank to which you belong (in the country where you are located) adopted the following security frameworks and/or international standards? Multiple answers may be possible.
Tools, controls and processes implemented in the bank	Actions/technical measures of digital security	What kind of digital security actions and technical measures (including aspects of infor-mation security, cybersecurity and fraud prevention using digital media) does the bank to which you belong (in the country where you are) have to protect the critical information systems? Multiple answers may be possible.
Tools, controls and processes implemented in the bank	Current digital security tools	Is the bank to which you belong (in the country where you are) currently implementing tools, controls or digital security processes using any of the following emerging digital technologies? Multiple answers may be possible.
Tools, controls and processes implemented in the bank	Digital security tools/processes	Is the bank to which you belong (in the country where you are) currently implementing tools, controls or digital security processes using any of the following emerging digital technologies? Multiple answers may be possible.
Tools, controls and processes implemented in the bank	Solutions with emerging digital technologies.	If possible, comment or contribute to the OAS with additional information on digital security solutions implemented using emerging digital technologies such as those indicated in the previous point.

TYPE	VARIABLE	DESCRIPTION
Digital security risk management	Cyber risks	What are the cyber risks that you think deserve more attention from the bank to which you belong (in the country where you are)? Prioritize all risks by giving them a number from 1 to 7, with 1 being the highest risk and 7 the lowest risk.
Detection and analysis of digital security events	Events against digital security	What types of events (successful attacks and unsuccessful attacks) of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) against the bank to which you belong (in the country where you are located) have been identified during the last twelve months? For each type, please indicate the approxi-mate frequency of occurrence.
Detection and analysis of digital security events	Digital security events used by cybercriminals	What types of events (successful attacks and unsuccessful attacks) of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) do cybercriminals use against the users of financial services of the bank to which you belong (in the country where you are)? Prioritize all events by giving them a number from 1 to 12, with 1 being the most frequent event and 12 the least frequent event.
Detection and analysis of digital security events	Percentage of events detected by proprietary systems	What percentage of events (successful attacks and unsuccessful attacks) of digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) are detected by the bank's own (and not third-party) detection systems of the bank to which you belong (in the country where you are)?
Management, response and recovery from digital security incidents	Strategies against digital security incidents	Does the bank to which you belong (in the country where you are located) have and executes the following strategies against digital security incidents (successful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media)?
Management, response and recovery to digital security incidents	Current digital security incidents	The bank to which you belong (in the country where you are located), as an organization, was the victim of digital security incidents (successful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media) during the last twelve months?
Report of digital security incidents, training and awareness	Sources of digital security incidents	Did the bank to which you belong (in the country where you are) investigate the source that generated such digital security incidents (successful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media)?
Report of digital security incidents, training and awareness	Motivations of current digital security incidents	What do you consider to be the main motivations for such digital security incidents (successful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media) suffered by the bank to which you belong (in the country where you are) during the last twelve months? Multiple answers may be possible.

TYPE	VARIABLE	DESCRIPTION
Management, response and recovery to digital security incidents	External assessment of digital security	The bank to which you belong (in the country where you are located) has been externally rated in the last two (2) years under some digital security maturity assessment methodology (including aspects of information security, cybersecurity and fraud prevention using digital media) and has it completed that evaluation?
Management, response and recovery to digital security incidents	Digital security assessment	In the event that the bank to which you belong (in the country where you are located) has not fully completed a digital security maturity assessment (including aspects of information security, cybersecurity and fraud prevention using media digital) or executed all derivative actions, to what do you attribute this? Multiple answers may be possible.
Tools, controls and processes implemented in the bank	Internal mechanisms of digital security	Does the bank to which you belong (in the country where you are located) offer a mechanism for its internal users (employees and contractors) to report digital security incidents (successful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media)?
Tools, controls and processes implemented in the bank	Mechanisms for digital security financial customers	Does the bank to which you belong (in the country where you are located) offer a mechanism for the financial services clients to report incidents (successful attacks) digital security (including aspects of information security, cybersecurity and prevention) of fraud using digital media) to the bank?
Tools, controls and processes implemented in the bank	Communications plan	Does the bank to which you belong (in the country where you are located) have a communications plan that allows it to inform its financial services customers when their personal information has been compromised?
Tools, controls and processes implemented in the bank	Digital security reporting mechanisms	Do you know of any mechanism to report digital security incidents (successful attacks) (including aspects of information security, cybersecurity and fraud prevention using digital media) suffered by the bank to which you belong (in the country where you are located) before a regulatory authority in your country?
Tools, controls and processes implemented in the bank	Reports before the law of digital security inci-dents	Does the bank to which you belong (in the country where you are) report the digital security incidents (successful attacks) before a law enforcement authority?
Tools, controls and processes implemented in the bank	Effectiveness of authorities against cyber criminals	In general, how do you consider the effectiveness of law enforcement authorities regarding the response, investigation and prosecution of cybercriminals?
Tools, controls and processes implemented in the bank	Digital security preparedness, response and training plans	Does the bank to which you belong (in the country where you are) have preparedness, response and training plans in digital security matters (including aspects of information security, cybersecurity and fraud prevention using digital media) for its employees and bank insourcing?

TYPE	VARIABLE	DESCRIPTION
Tools, controls and processes implemented in the bank	Plan implementation times	How often are preparedness, response and training plans executed?
Tools, controls and processes implemented in the bank	Testing response capability against digital security incidents	How often is the capability of employees of the bank to which you belong (in the country where you are) tested to adequately respond to digital security incidents (successful attacks) (including aspects of information security, cybersecurity and prevention of fraud using digital media) and phishing and social engineering schemes?
Tools, controls and processes implemented in the bank	Effective mechanics in the face of digital security risks	What has been the most effective mechanism to generate greater awareness in the bank to which you belong (in the country where you are located) with respect to digital security risks (including aspects of information security, cybersecurity and fraud prevention using digital media)? Prioritize all the mechanisms by giving them a number from 1 to 9, with 1 being the most effective mechanism and 9 the least effective mechanism.
Impact of digital security incidents	Total assets	What was the value of the total assets of the bank to which you belong (in the country where you are located) in the immediately preceding fiscal year?
Impact of digital security incidents	EBITDA	What was the EBITDA value (Earnings Before Interests, Taxes, Depreciations and Amortizations) of the bank to which you belong (in the country where you are) in the immediately preceding fiscal year?
Impact of digital security incidents	Digital security budget	What was the digital security budget (including aspects of information security, cybersecurity and fraud prevention using digital media) of the bank to which you belong (in the country where you are) for the current fiscal year?
Impact of digital security incidents	Digital security budget increase	Compared to the immediately preceding fiscal year, how much has the digital security budget (including aspects of information security, cybersecurity and fraud prevention using digital media) increased in the bank to which you belong (in the country where you are) for the current fiscal year? If there was an increase in the digital security budget (including aspects of information security, cybersecurity and fraud prevention using digital media), identify the three (3) main reasons that led to the increase:
Impact of digital security incidents	% Budget	Of the digital security budget (including aspects of information security, cybersecurity and fraud prevention using digital media) of the bank to which you belong (in the country where you are located) in the current fiscal year, please estimate the assigned percentage to each of the following four (4) categories (The options must add up to 100%).
Impact of digital security incidents	Digital security ROI	Has the bank to which you belong (in the country where you are located) carried out return on investment calculations in digital security (including aspects of information security, cybersecurity and fraud prevention using digital media)?

TYPE	VARIABLE	DESCRIPTION
Impact of digital security incidents	% Digital security ROI	What was the return on investment in digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) for your bank in the immediately preceding fiscal year? Please express your answer as a whole number equivalent to a percentage (for example, 30 indicates 30%).
Impact of digital security incidents	Cost of response and recovery of digital security incidents	Did the bank to which you belong (in the country where you are) estimate the total cost of response and recovery to incidents (successful attacks) in digital security (including aspects of information security, cybersecurity and fraud prevention using media digital) for the last fiscal year?
Impact of digital security incidents	Current cost of digital security incidents.	What was the cost of responding to and recovering from incidents (successful attacks) in digital security (including aspects of information security, cybersecurity and fraud prevention using digital media) for the bank to which you belong (in the country where is there) for the last fiscal year?

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Regarding the results of the estimations, models of the Logit type were run, using banking entities as the unit of analysis. Different models were estimated including the independent variables described above. Additionally, the information from 191 observations (banking entities) was included.

After testing different functional forms and independent variables, the model with the best fit was chosen: LOGIT. In general, the model presents a good global adjustment, with as probability approaching zero levels. The foregoing indicates that the estimated model as a whole is a good representation of the dependent variable: in this particular case, the probability that a bank was a victim of digital security events. Next are the results of the aforementioned model.

Table 12. Results of the LOGIT model estimates where the dependent variable (y) takes the value of 1 if the bank was the victim of events to digital security and 0 otherwise

Logistic regression	**Number of obs**	**=**	**191**
	LR chi2(9)	**=**	**33.19**
	Prob > chi2	**=**	**0.0001**
Log likelihood = -104.51284	**Pseudo R2**	**=**	**0.1370**

VictimaInc	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
costo	.2439135	.122274	1.99	0.046	.0042606	.4835665
miembros	-.0037382	.004924	-0.76	0.448	-.0133891	.0059126
activo	.2439135	.0000175	1.18	0.046	.0042606	.4835665
TLarge	1.014411	.5992369	1.69	0.090	-.1600722	2.188893
TMedium	1.001714	.4063689	2.47	0.014	.2052454	1.798182
casaMatriz	.768328	.4457521	1.72	0.085	-.10533	1.641986
Bprivado	1.055184	.0000175	1.73	0.084	-.1425247	2.252892
Bmixto	1.556309	.8095643	1.92	0.055	-.0304074	3.143026
areaUnicaSD	.7641452	.4195664	1.82	0.069	-.05819	1.58648
_cons	-3.816138	.8742597	-4.36	0.000	-5.529656	-2.102621

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Control variables such as the *Asset*, entity size dummies (according to the number of branches and employees) and dummies of the Bank's *property* were included. Additionally, inherent variables associated with the digital security management of the banking entity were included, among them, the *Cost* dedicated to digital security actions, the Members of the work team dedicated to digital security and if it has a *Unique* Area devoted to digital security.

Regarding the control variables related to the characteristics of the banking entities, it is found that the amount of the *Assets* is not significant. On the other hand, according to the results of the model, large and medium banks have a higher probability of digital security incidents compared to small banks. It is also reported that those private and mixed banks have a higher probability of having digital security incidents, compared to public banks.

The inclusion of the variable *Cost* is important to mention. The model shows that it is significant, presenting a positive sign, which indicates that those banks that have assumed a higher total Cost of digital security incident response and recovery in 2017 presented a higher probability of having incidents in the period. For its part, the number of staff *Members* dedicated exclusively to the digital security team was included as a dependent variable. It is observed that the variable presents a negative sign and significant, in the estimation. This suggests that those entities that dedicate more personnel to these tasks reduce their probability of presenting digital security incidents.

Additionally, several well-adjusted models were analyzed in order to explain the following dependent variables: i) the size of the team that manages processes associated with digital security, ii) the budget dedicated to digital security, and iii) the total cost of digital security incident response and recovery.

In relation to the results of the estimations with dependent variable to the members of the team that manages processes associated with digital security (or the natural logarithm of the members) it is seen that a larger number of members is expected in large and medium banks and gradually as the *Assets* of the entity grow. In contrast, there is a relationship between the size of the team and the nature of the bank, that is, smaller teams are expected in private and mixed banks compared to public banks.

Table 13. **Results of the estimations with dependent variable:** personnel (members)

Source	SS	df	MS		
Model	82037.9532	9	9115.32814	Number of obs	= 191
				F(9, 181)	= 4.59
				Prob > F	= 0.0000
Residual	359403.775	181	1985.65621	R-squared	= 0.1858
				Adj R-squared	= 0.1454
Total	441441.728	190	2323.37751	Root MSE	= 44.561

miembros	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TLarge	52.1681	10.37778	5.03	0.000	31.69113	72.64511
TMedium	8.884608	7.470472	1.19	0.236	-5.855807	23.62502
casaMatriz	-11.38604	8.020053	-1.42	0.157	-27.21086	4.438788
Bprivado	-22.52051	10.10413	-2.23	0.027	-42.45754	-2.583481
Bmixto	-28.52225	15.07817	-1.89	0.060	-58.27385	1.229357
areaUnicaSD	1.765107	7.536372	0.23	0.815	-13.10534	16.63555
VictimaInc	-3.320306	7.428902	-0.45	0.655	-17.9787	11.33808
costoEBT	-674.5167	675.1612	-1.00	0.319	-2006.716	657.6823
activo	.000514	.0003167	1.62	0.106	-.0001108	.0011388
_cons	42.3053	15.86651	2.67	0.008	10.99819	73.61242

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Table 14. Results of the estimations with natural logarithm of a dependent variable of the personnel (member)

Source	SS	df	MS		
Model	122.287039	9	13.5874488	Number of obs	= 191
Residual	176.020474	181	.972488806	F(9, 181)	= 13.97
				Prob > F	= 0.0000
				R-squared	= 0.4099
				Adj R-squared	= 0.3806
Total	298.307513	190	1.57003954	Root MSE	= .98615

lnmiembros	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TLarge	1.972616	.2392491	8.25	0.000	1.50054	2.444692
TMedium	.7126999	.1706015	4.18	0.000	.3760763	1.049323
casaMatriz	-.2720873	.1775568	-1.53	0.127	-.6224348	.0782601
Bprivado	-.3132121	.2247507	-1.39	0.165	-.7566805	.1302563
Bmixto	-.1979587	.3332581	-0.59	0.553	-.8555292	.4596118
areaUnicaSD	-.1332119	.1691046	-0.79	0.432	-.4668819	.200458
VictimaInc	-.0352649	.1709216	-0.21	0.837	-.3725202	.3019903
lncosto1	.0535321	.0671529	0.80	0.426	-.0789711	.1860353
lnactivo	.0993163	.0726377	1.37	0.173	-.0440094	.242642
_cons	.5704745	.6768391	0.84	0.400	-.7650353	1.905984

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

In relation to the results of the estimations with dependent variable, the budget (or the natural logarithm of the budget) devoted to digital security shows that in larger banks a larger dedicated budget is expected, as well as a positive relation with cost, that is, the dedicated budget can be explained with the total cost of response assumed (a higher budget is expected in digital security matters). As a result of this model, a dummy control variable was also included, which represents whether the entity was a victim or not of incidents in the period, noting that the entities that were not victims of incidents dedicated more budget dedicated to digital security.

Table 15. **Results of the estimations with dependent variable:** Budget (ppto)

Source	SS	df	MS		
Model	526.735089	9	58.526121	Number of obs	= 191
				F(9, 181)	= 30.99
				Prob > F	= 0.0000
Residual	341.810824	181	1.88845759	R-squared	= 0.6065
				Adj R-squared	= 0.5869
Total	868.545913	190	4.57129428	Root MSE	= 1.3742

ppto	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TLarge	.8317346	.3433371	2.42	0.016	.1542766	1.509193
TMedium	.2317614	.2310129	1.00	0.317	-.2240632	.6875861
activo	6.05e-06	.0000101	0.60	0.548	-.0000138	.0000259
casaMatriz	.1210165	.2472759	0.49	0.625	-.3668977	.6089306
Bprivado	.2559118	.3116485	0.82	0.413	-.3590196	.8708432
Bmixto	.6535669	.4659528	1.40	0.162	-.2658311	1.572965
areaUnicaSD	-.207409	.2323549	-0.89	0.373	-.6658817	.2510637
VictimaInc	-.0210439	.2311328	-0.09	0.928	-.4771052	.4350173
costo1	7.79e-07	6.52e-08	11.95	0.000	6.50e-07	9.07e-07
_cons	-.1681109	.432029	-0.39	0.698	-1.020572	.6843502

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Table 16. Results of the estimations with dependent variable: natural logarithm of Budget (lnppto1)

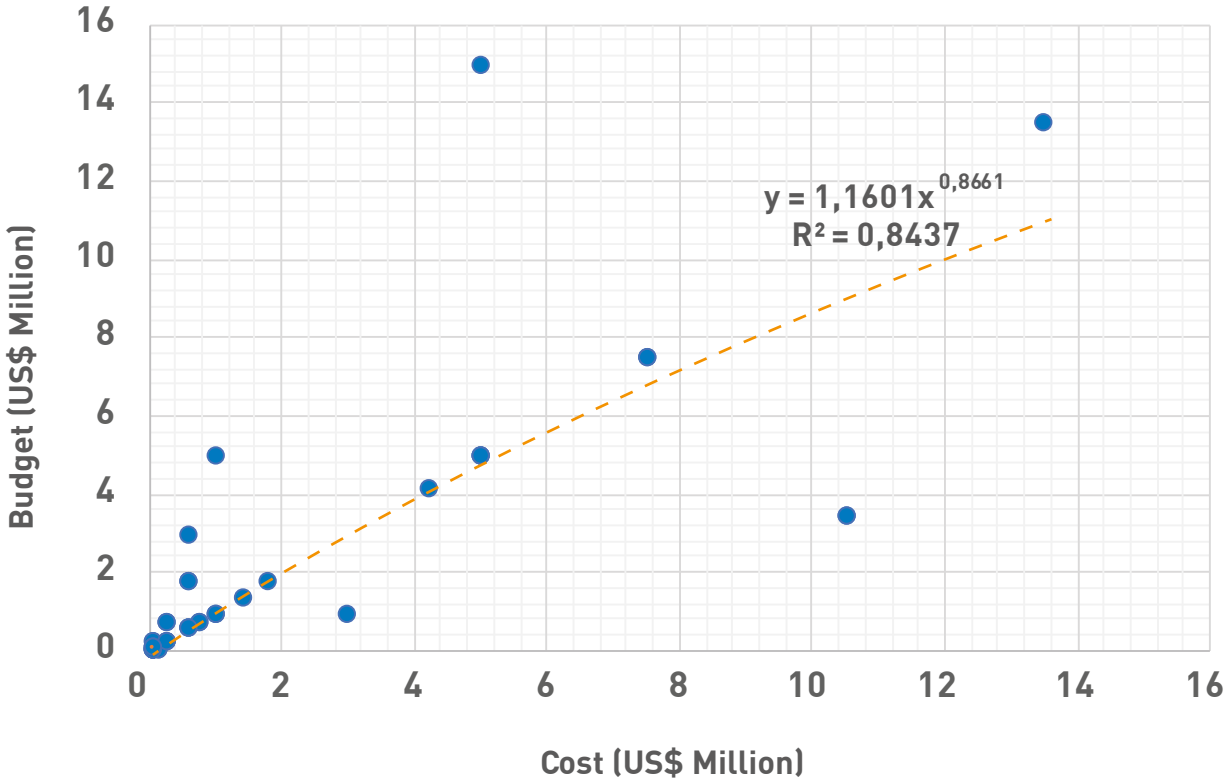
Source	SS	df	MS		
Model	967.455085	9	107.495009	Number of obs	= 191
Residual	4031.36323	181	22.272725	F(9, 181)	= 4.83
				Prob > F	= 0.0000
				R-squared	= 0.1935
				Adj R-squared	= 0.1534
Total	4998.81831	190	26.3095701	Root MSE	= 4.7194

lnppto1	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TLarge	2.226543	1.147933	1.94	0.054	-.0385091	4.491595
TMedium	.7836754	.8167697	0.96	0.339	-.8279395	2.39529
activo	-.000067	.0000362	-1.85	0.066	-.0001383	4.37e-06
casaMatriz	1.210602	.8487889	1.43	0.156	-.4641922	.2.885395
Bprivado	1.633892	1.074449	1.52	0.130	-.4861643	3.753949
Bmixto	-.297355	1.598058	-0.19	0.853	-3.450575	2.855865
areaUnicaSD	.1493896	.7983161	0.19	0.852	-1.425813	1.724593
VictimaInc	-1.332826	.8078245	-1.65	0.101	-2.92679	.2611389
lncosto1	1.353621	.273823	4.94	0.000	.8133252	1.893917
_cons	-8.55294	3.388622	-2.52	0.012	-15.23922	-1.866657

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

The positive relationship between the budget variables dedicated to digital security and the total cost of digital security incident response and recovery can be seen when doing a correlation analysis between them. The following graph presents the same result obtained through the econometric model, with a higher cost of response and recovery, there is a greater budget dedicated to digital security. **Annex 3** of this document presents the list of variables mentioned by bank size (Large, Medium and Small Banks) in Latin America and the Caribbean.

Graph 35. Relationship between the budget allocated to Digital Security and the total cost of security incident response and recovery for banking entities in Latin America and the Caribbean



Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Finally, in relation to the results of the estimates with dependent variable the total cost (or the natural logarithm of the cost) of digital security incident response and recovery, it is seen that large and medium banks assumed higher costs during the period, a situation that is related to the value of the assets of the entity (the higher the value of the assets, the greater the cost assumed). Likewise, this model included a dummy control variable that represents whether the entity was a victim or not of incidents in the period, noting that the entities that were victims of incidents incurred a higher total cost of response and recovery in the event of digital security incidents.

Table 17. **Results of the estimations with dependent variable:** Cost

Source	SS	df	MS		
Model	220.131823	8	27.5164778	Number of obs	= 191
				F(9, 181)	= 11.26
				Prob > F	= 0.0000
Residual	444.657573	182	2.44317348	R-squared	= 0.3311
				Adj R-squared	= 0.3017
Total	664.789396	190	3.49889156	Root MSE	= 1.5631

costo	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TLarge	2.084347	.3586582	5.81	0.000	1.376684	2.792009
TMedium	.262295	.26204	1.00	0.318	-.2547319	.7793218
casaMatriz	-.1238546	.2811084	-0.44	0.660	-.6785051	.4307959
Bprivado	-.1315021	.3543434	-0.37	0.711	-.8306513	.5676472
Bmixto	-.4602598	.528888	-0.87	0.385	-1.5038	.5832807
areaUnicaSD	-.0165476	.2642839	-0.06	0.950	-.5380019	.5049067
VictimaInc	.6026437	.2590737	2.33	0.021	.0914695	1.113818
activo	.0000416	.000011	3.77	0.000	.0000198	.0000633
_cons	.1217271	.4913186	0.25	0.805	-.8476858	1.09114

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Table 18. **Results of the estimations with dependent variable:**
natural logarithm of cost

Source	SS	df	MS		
Model	272.003375	9	30.2225973	Number of obs	= 191
				F(9, 181)	= 25.46
				Prob > F	= 0.0000
Residual	214.898432	181	1.18728415	R-squared	= 0.5586
				Adj R-squared	= 0.5367
Total	486.901807	190	26.3095701	Root MSE	= 1.0896

lnppto1	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TLarge	.9784556	.3013972	3.25	0.001	.3837515	1.57316
TMedium	.535855	.1933211	2.77	0.006	.1544021	.9173079
casaMatriz	.1176836	.1972627	0.60	0.552	-.2715466	.5069138
Bprivado	-.3327028	.2484349	-1.34	0.182	-.8229038	.1574983
Bmixto	-.1866016	.3683247	-0.51	0.613	-.9133642	.5401609
areaUnicaSD	.2947919	.1858819	1.59	0.115	-.0719822	.6615661
VictimaInc	.3103659	.1874647	1.66	0.100	-.0595313	.6802631
lnactivo	.6622524	.0639145	10.36	0.000	.536139	.7883657
lnmiembros	.0653558	.0819851	0.80	0.426	-.0964136	.2271252
_cons	6.464284	.5749981	11.24	0.000	5.329723	7.598846

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

05

CYBERSECURITY FROM THE PERSPECTIVE OF USERS OF BANKING SECTOR ENTITIES IN LATIN AMERICA AND THE CARIBBEAN

In order to prepare this Study on Cybersecurity in the banking sector in Latin America and the Caribbean, the General Secretariat of the Organization of American States (GS/OAS), in addition to the aforementioned instrument for banking entities, developed a particular one in order to obtain information on aspects related to digital security incidents (including aspects of types of banking operations performed, means used, security measures, reporting and impact mechanisms) for the users of the entities banking in the region.

In particular, the user instrument presented a catalog of questions classified into three (3) sections:

- Users characterization
- Digital security culture
- Impact of digital security incidents

Along the same line regarding confidentiality of the information, the GS/OAS did not request any information that could be identified to any of the users at a personal level, and in this case no information was requested referring to the country, nor was any information stored about its location. All the answers were compiled, analyzed and distributed at the aggregate level, that is, by thematic blocks, without the same being made available to any person or institution in detail.

During the application of the instrument, the questions came with concepts that advanced some of them, especially to facilitate the verification of aspects associated with digital safety culture.

A total of 722 people started filling out the questionnaire during the publication period of the information collection instrument (the first quarter of 2018) and, based on the detailed review, a database was established with records of 562 users of banking entities from the Latin American and Caribbean region that filled out the survey until its last part. At this point it is necessary to specify that to the extent that the respondent was advancing, he/she encountered questions that instructed answering subsequent questions or not. An example of this is related to the impact of cyber incidents, which were only answered by those who, in the respective question, had said that they had suffered an incident.

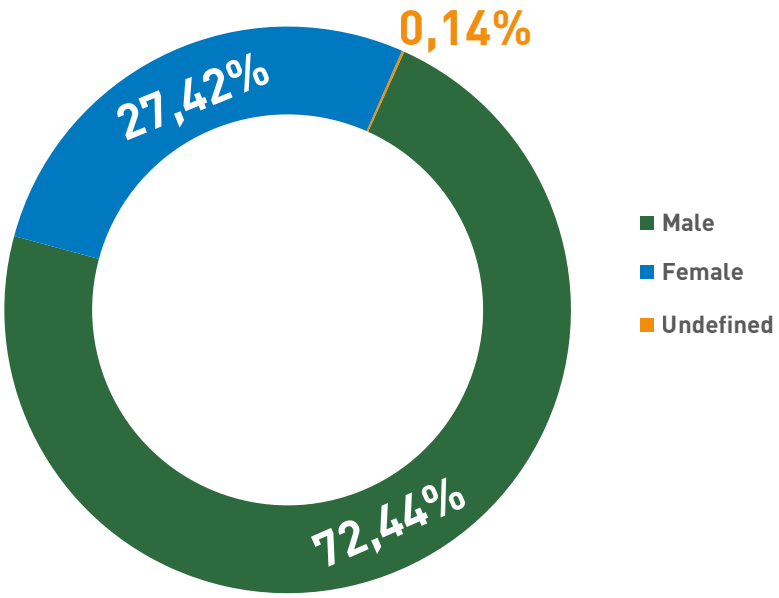
Therefore, each graph has associated the number of answers obtained for the respective question.

5.1 User profile

In this component of the study, questions were asked to establish the characteristics of the bank users that completed the survey, in aspects associated with the individual (gender and age range), as well as in the form and particular characteristics of the way in which they carry out the different types of transactions with their bank, for example, means used (to check transactions and balances, make deposits, withdrawals, purchases and transfers) and the preference of different digital media, and in the case of not using them , the motivations for not using them in conducting banking transactions.

Regarding gender, among the interviewed users, 72.44% reported being male, while 27.42% reported being female and 0.14% were "not defined".

Graph 36. Gender of the users

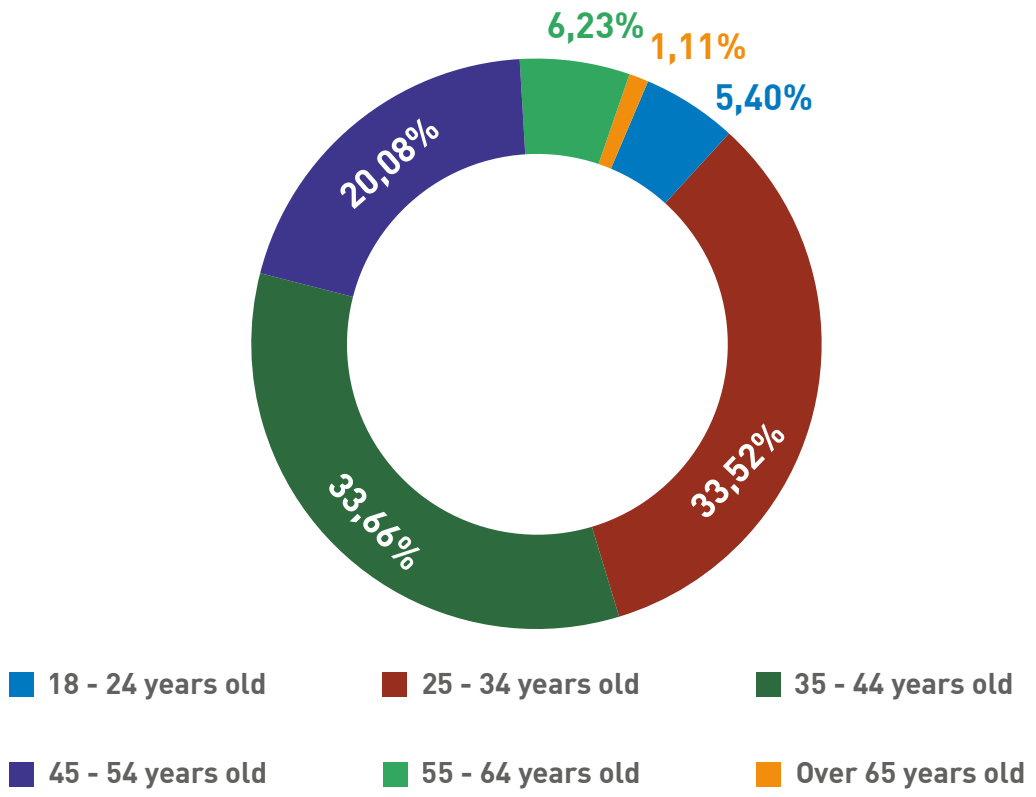


Note: 722 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Regarding the age range of the users interviewed, 33.66% are between 35 and 44 years old, 33.52% between 25 and 34 years old, 20.08% between 45 and 54 years old, 6.23% between 55 and 64 years old, 5.40% between 18 and 24 years old and only 1.1% are over 65 years old.

This indicates that almost 90% of the users who responded the survey are between 25 and 54 years old, which contrasts with just 1.1% of respondents over 65 years of age.

Graph 37. Age range of the users



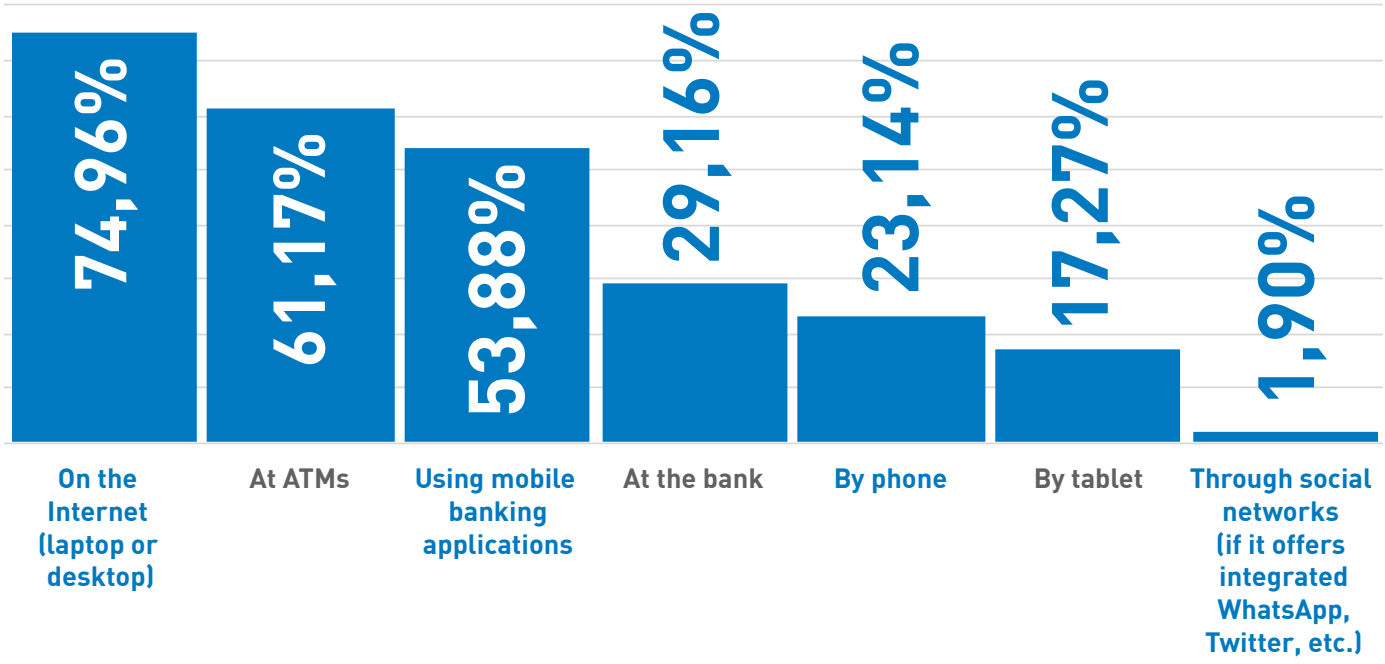
Note: 722 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

To determine the level of assimilation of electronic media in banking operations, the study included questions to determine the preference for the different types of options available. The questions included both face-to-face and remote channels.

Regarding the means used by users to review recent transactions and available balances, the results show a significant use of laptops or desktops connected to the Internet, as well as ATMs and mobile applications (74.96% said that they used computers connected to the Internet, 61.17% said they used ATMs, 53.88% said they used applications); compared to a lower percentage that said they preferred the use of direct channels in the bank, through the telephone, as well as tablets and social networks in the event that the bank offered this (29.16% revealed that they did this at the bank, 23.14% said they used the telephone, 17.27% said that they used the tablet and 1.90%, services integrated into social networks).

Based on the results, it is clear that users privilege virtual media over face-to-face media, which is consistent with the high degree of digitalization of services and the impulse to their appropriation by users. The following graphic shows the summary of the results:

Graph 38. **Means to review recent transactions and available balances**



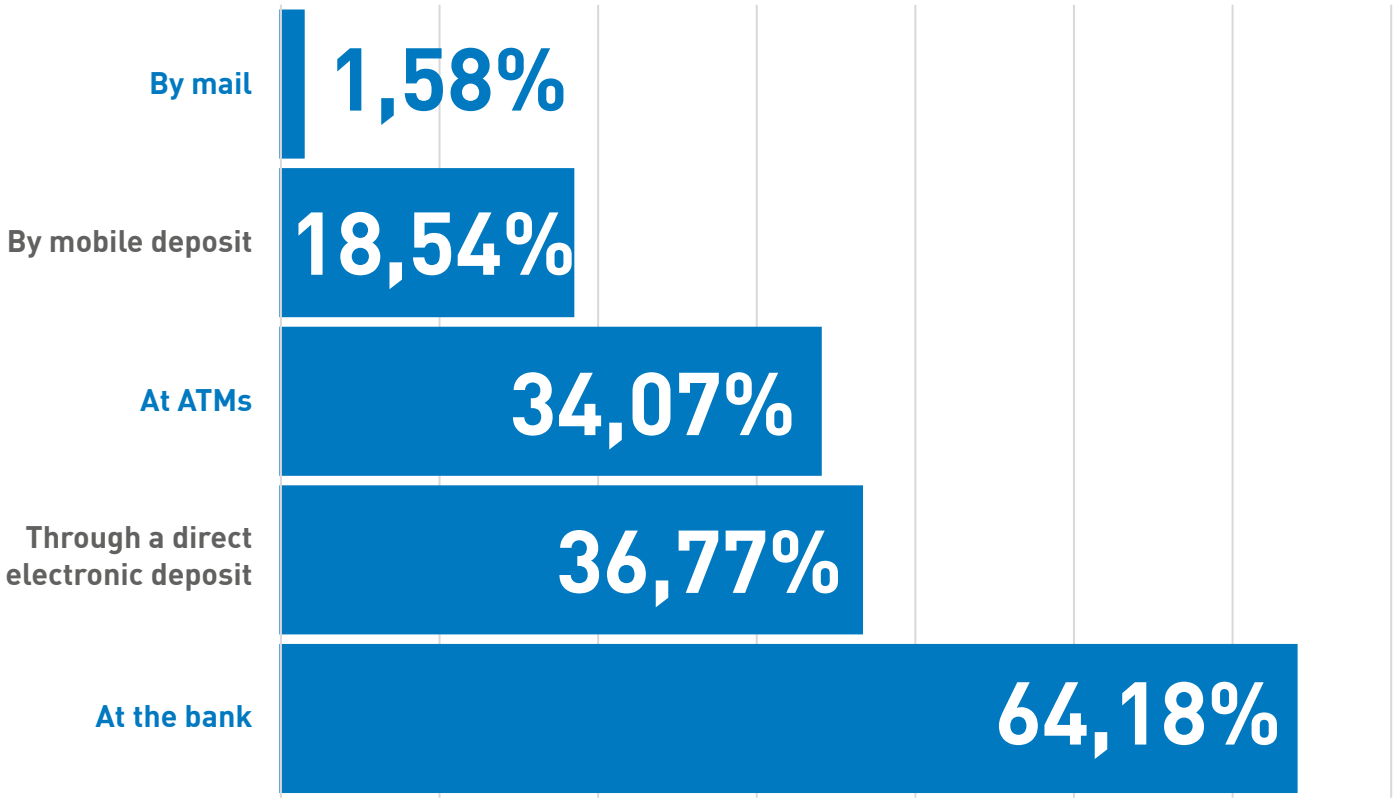
Note: 631 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

The low use of media such as tablets can be explained because they do not offer the same usability conditions (or even perception of security) as computers. In the case of the integration of financial services in social networks, such as the possibility of making transfers through a chat message or checking the balance of an account with a direct message to the Bank's Twitter account, it is still a very limited offer because there are not many banks that offer this option to their customers.

Regarding the means used by users to deposit checks and cash, a high percentage said that they used the bank's face-to-face channel (64.18%), privileging it over other means such as direct electronic deposit (36.77%), ATMs automatic (34.07%) and, much less, mobile deposits (18.54%) and mail. It can be inferred that it is natural that, in the face of this type of operation, users lean more to the face-to-face channel. However, it is worth noting that other means with technological support such as ATMs that accept cash or mobile deposits (when, for example, the amount of a check can be deposited by capturing the image and endorsing using the smartphone camera) begin to be regarded within the options, albeit in a lower percentage. This shows that users are assimilating more Mobile Banking services, taking advantage of their ease of use, convenience, reliability and security.

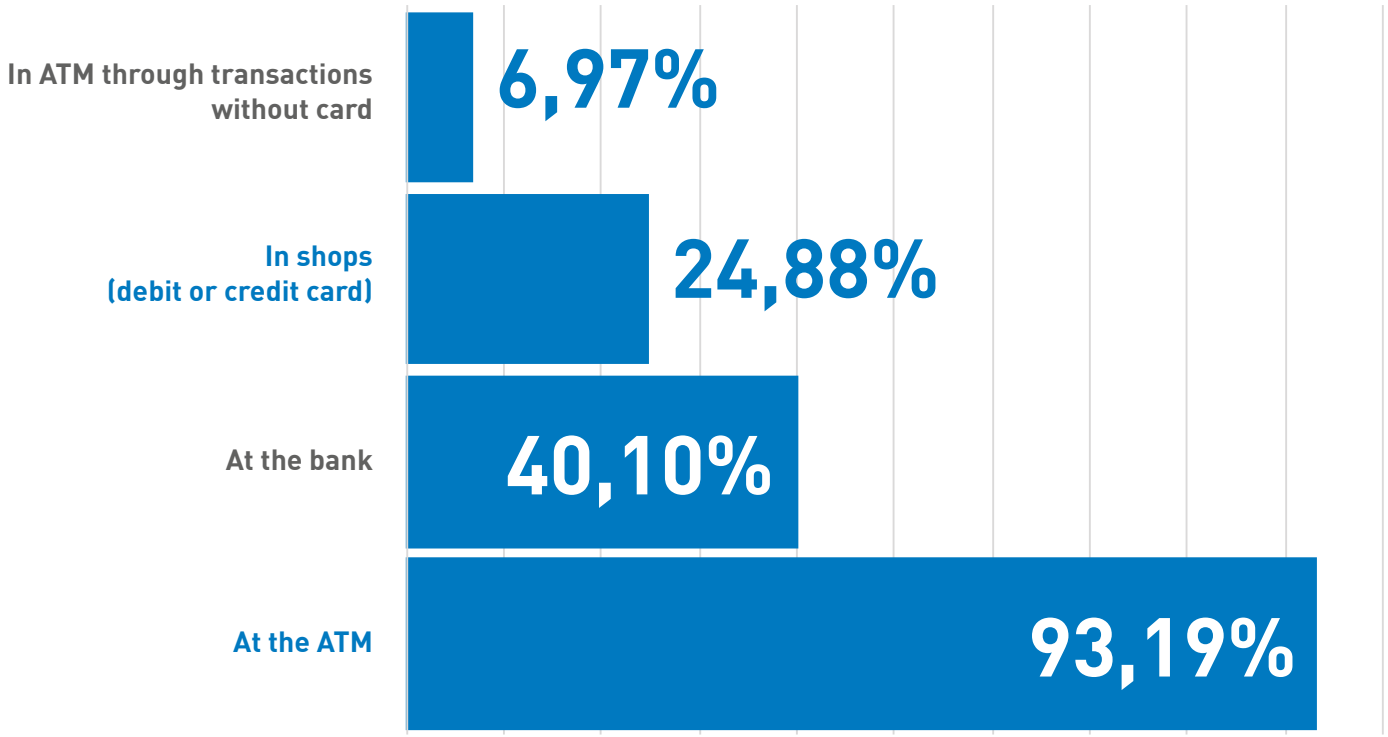
Graph 39. Means of depositing checks/cash



Note: 631 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Regarding the preferred means to obtain cash, the users , in a majority percentage (93.19%), expressed the use of the ATM as their preferred. On the other hand, a segment which amounted to less than half of them (40.10%) said that they preferred to go to the bank in person, compared to 24.88% who said that they used the debit or credit card in commercial establishments. The percentage of transactions that are made by cashier without the card being available (6.97%) is also growing, given that it is an alternative offered more and more by banks to their customers and which is beginnig to be accepted by them.

Graph 40. Means to obtain cash

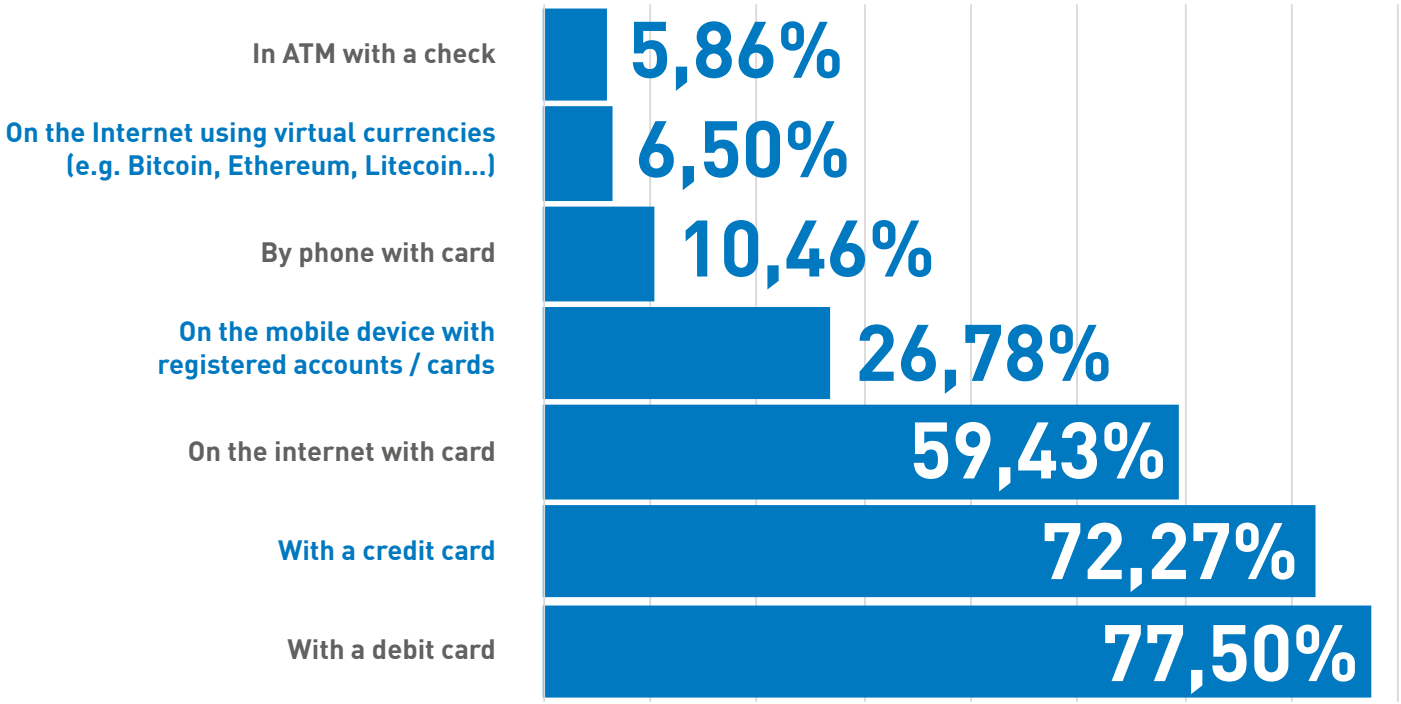


Note: 631 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Regarding the means utilized by users to make purchases, the significant use of debit and credit cards is evident (77.50% and 72.27, respectively) both in face-to-face and virtual channels, as well as the use of cards for online purchases (59.43%). In this type of operations, it is significant that the use of means such as a mobile device associated with bank accounts and cards (26.78%) surpasses their use for other traditional channels such as telephone purchases with a card (10.46%) and checks (5.86%).

Another striking aspect in this study is the significant percentage of the use of virtual currencies (6.50%) as a means of making purchases on the Internet, the percentage of which exceeds the use of the check as a purchasing means (5.86%).

Graph 41. Means to make purchases

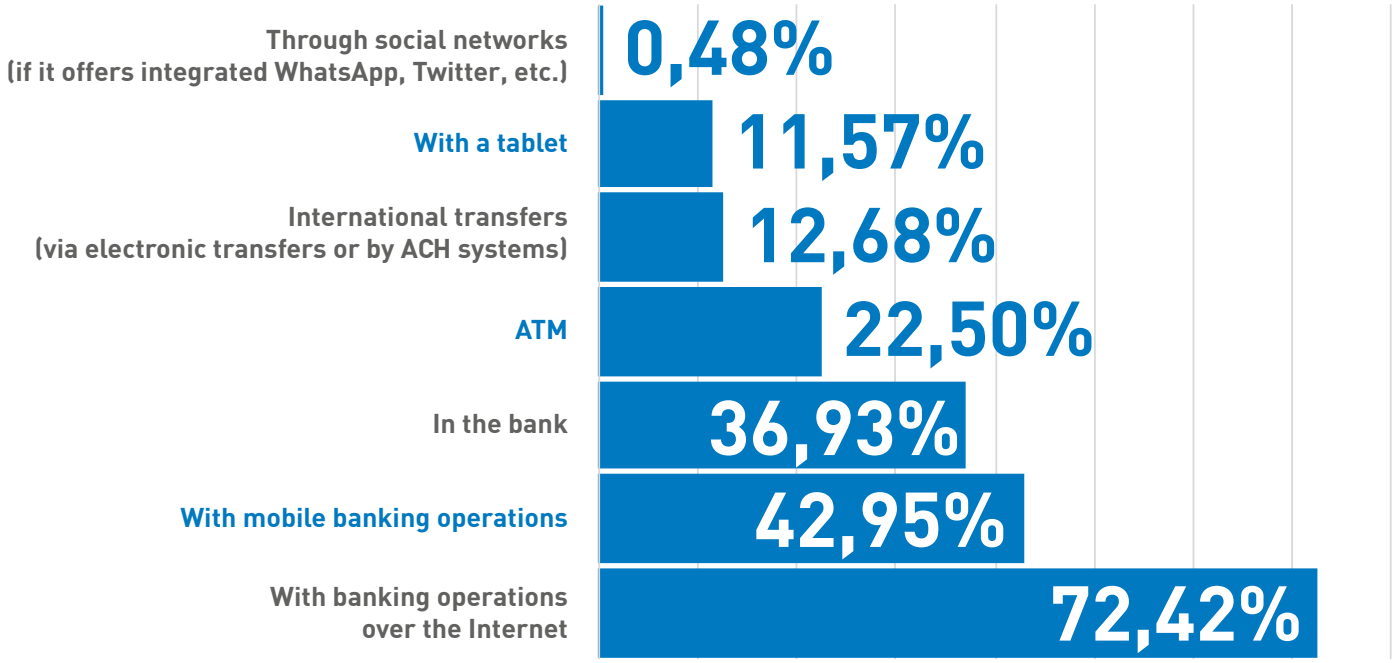


Note: 631 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Regarding the means used to make transfers, users mostly prefer to perform these banking operations online (72.42%), compared to 42.95% that perform them through mobile banking operations, 36.93% that make them directly at the bank, 12.68% through international transfers, 11.57% with a tablet and only 0.48% in services integrated in social networks. This type of operations also shows the preference for those associated with digital media, reflecting an increasing assimilation among users of this type of channels.

In particular, it is very important to note that the percentage represented by the use of mobile banking already exceeds that which prefers to make the transfers directly at the bank's offices. This result corroborates the information obtained from other sources, such as PwC's 2018 Digital Banking Consumer Survey: Mobile users set the agenda. This report recalls that the 2017 survey showed the rise of "omnidigital" consumers, that is, those who prefer to interact digitally with their bank with no preference over a laptop, a tablet or a smartphone, but in the 2018 edition, the results highlight the start of a preference for the smartphone.

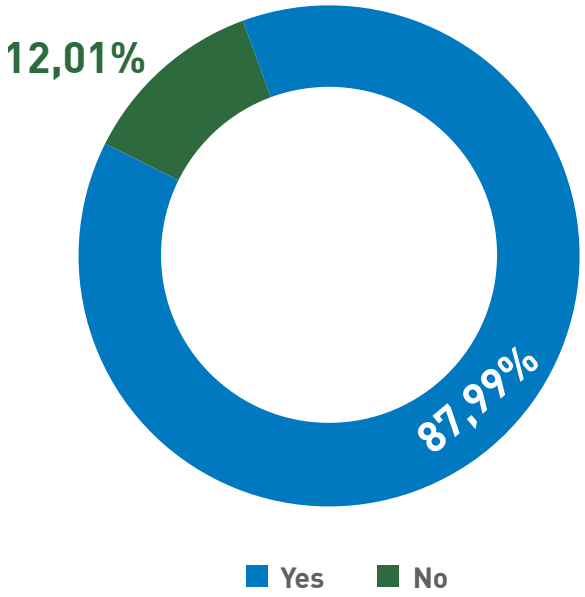
Graph 42. Means to transfer funds



Note: 631 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Now, as a general question to assess the appropriation of digital media, we consulted whether users used digital media to carry out their transactions, the response obtained was that a high percentage (87.99%) effectively used them for their banking operations, compared to 12.01% who said they did not use them. With this result, it is clear that the users of Latin American and Caribbean banking continues to evolve towards becoming a consumer of virtual channels for their transactions.

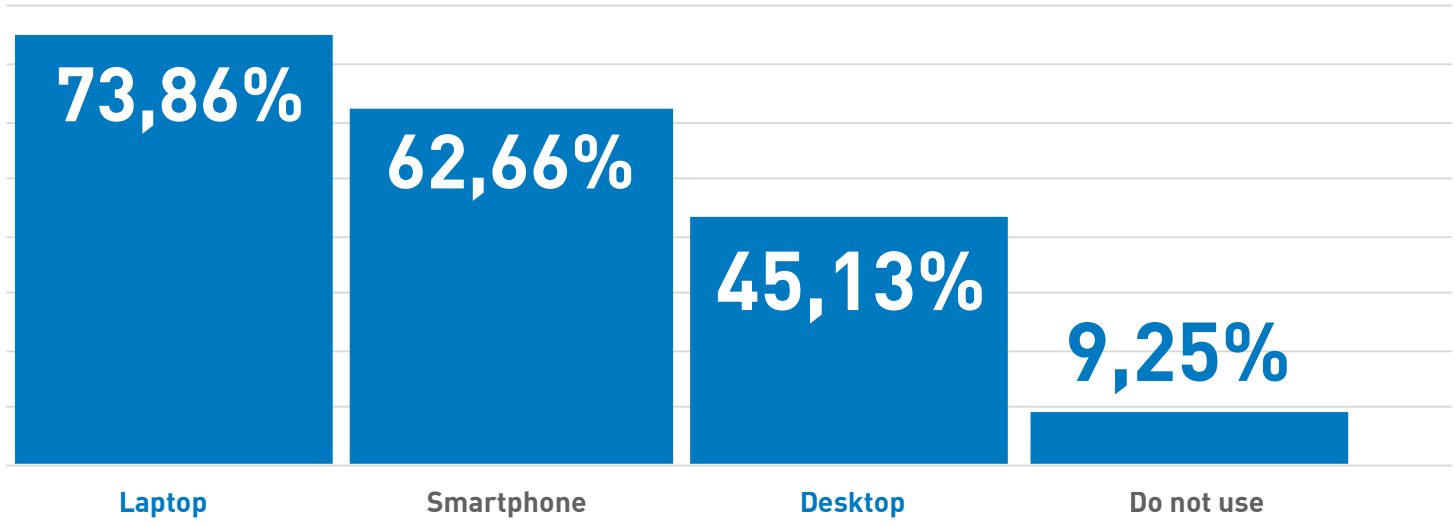
Graph 43. Percentage of users that use digital media for their banking transactions



Note: 616 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Finally, regarding the use of digital media for banking transactions, the laptop is the one with the highest preference of use (73.86%), followed by the smartphone (62.66%) and the desktop computer (45, 13%); in contrast to 9.25% who said they did not use any digital media. Although the laptop is still the most widelyused medium, it is important to highlight the relevance that smartphones have gained in this result, being already very close to the first place of preference, since the smart mobile seems to observe a tendency to position itself as the main device for users to enter the Internet and access multiple services. This result demonstrates a dynamic of inclusion and effects of the digital revolution that is being experienced in the region, where access to connectivity becomes a condition and its massification is mainstreaming in their countries. These aspects are driven by both information society agendas in Latin America and the Caribbean (eLAC) as well as by national digital agendas.

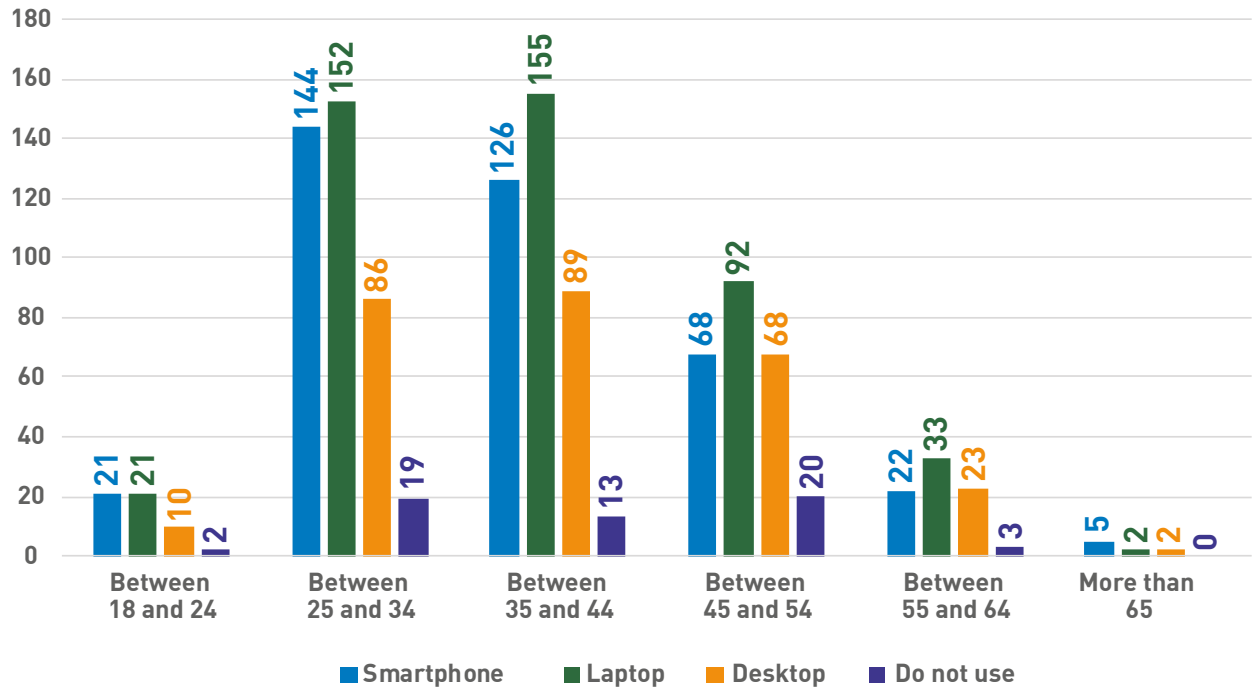
Graph 44. **Most-used digital media to carry out banking transactions**



Note: 616 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

With the obtained data, it was possible to analyze the most used digital means for banking transactions and their preferences by age range. In this analysis it is highlighted that in the case of the youngest (between 18 and 24 years old) the use of mobile devices equals that of laptops (39% in both cases), and in the following range (between 25 and 34 years old)) it is very close (36% mobile and 38% portable), which confirms the conclusion of PricewaterhouseCoopers (PwC, 2018) in the 2018 Digital Banking Consumer Survey: Mobile users set the agenda, in the sense of reflecting the increasing inclination of the users for this type of devices, something driven by the younger population groups. Another aspect observed is that the greater resistance or non-use of digital media to carry out transactions occurs in the range between 45 and 54 years, reaching 8.06% (people over 65 years old are not considered in this conclusion, since the sample is very limited for this age range).

Graph 45. Most-used digital media to perform banking transactions



Note: 616 records

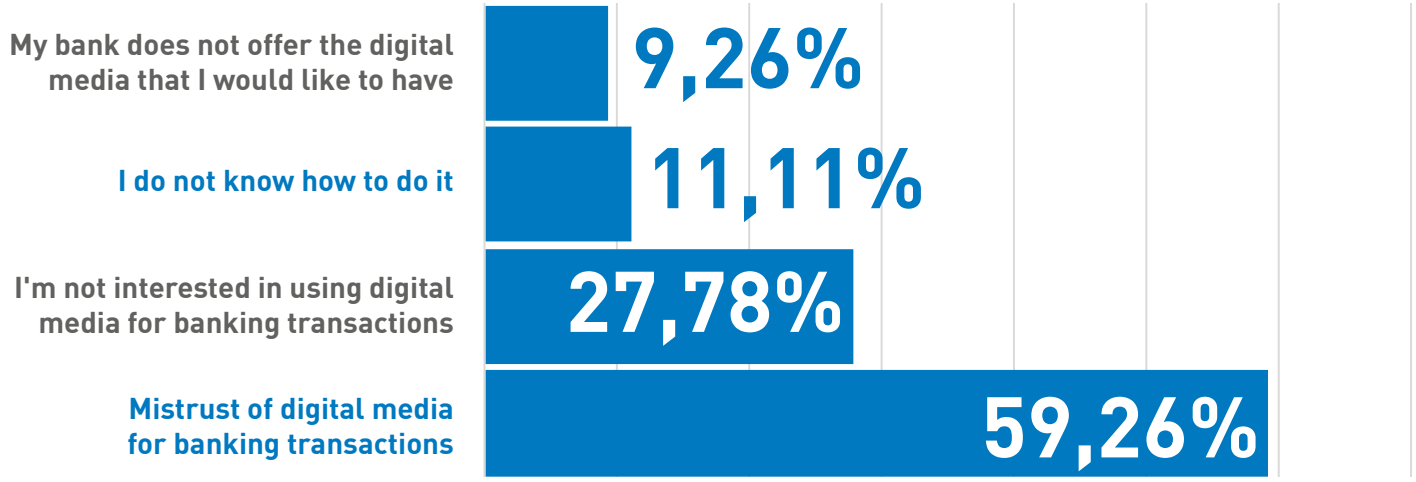
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

However, the survey deepened the study on the segment of users interviewed who said they did not use digital media to carry out banking transactions, in order to know the reasons for not using them, mainly observing distrust in them (59.26%), followed by lack of interest in the use of digital media (27.78%), unawareness of these (11.11%) and, finally, lack of supply in those services (9.26%). This result makes clear that the first step to encourage users in the use of digital media is, in addition to showing the benefits of these channels, to generate trust and security in them.

The perception of distrust of those users who do not use digital media to carry out banking transactions increases due to the fact that there is more disclosure of the incidents that have affected multiple organizations and users of the digital environment, especially in aspects related to the loss of personal data, identity theft and violations experienced by financial entities. This can be ratified in external references, as is the case of the recent study by The Financial Brand (The Financial Brand, 2018), the results of which establish that 81% of the users of online banking and mobile banking services surveyed are worried about theft of personal data and identity theft, and 65% expressed concern about data breaches involving financial entities.

On the other hand, the lack of interest in the use of digital media obtained a result that cannot be ignored and that denotes that there are still users who do not appreciate (or possibly ignore) the benefits they can obtain from the services offered by these means. Typical benefits such as savings in time and travel can be added to the characteristics of contributions that offer disruptive solutions such as those associated with FinTech, such as personalized services, credit options in minutes, crowdfunding, etc.

Graph 46. Reasons explained by people who do not use digital media to carry out banking transactions



Note: 54 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

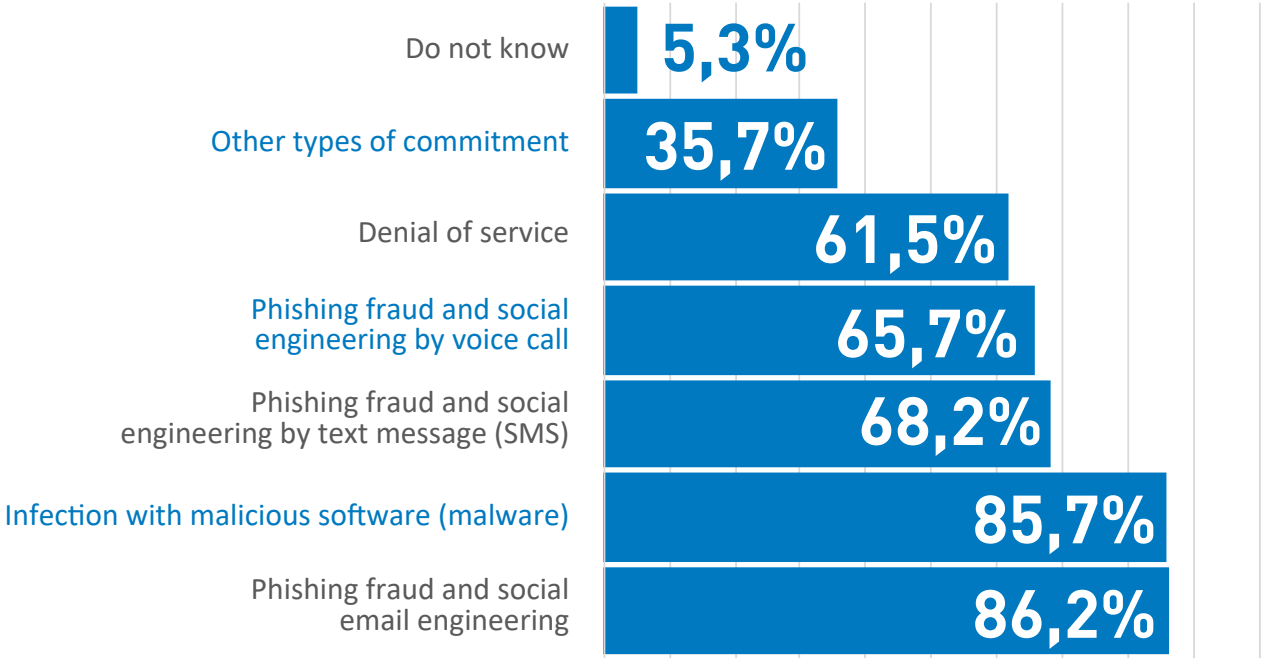
5.2 Digital Security Culture

In this component of the study, questions were asked to establish aspects related to culture in digital security topics by banks users that completed the survey, in matters associated with their prior knowledge of definitions related to types of cyber incidents, the most-used security measures to prevent such incidents, as well as the means through which they are kept informed of new forms of attacks and security threats.

In response to the question about the type of digital incidents about which users believed to have knowledge, it is evident that phishing fraud and social e-mail engineering, together with software infection, are the most answered by the users (86.2% and 85.7% respectively). On the other hand, phishing and social engineering fraud by text message occupies a third place–no less important–(with 68.2%), followed by phishing fraud and social engineering by a phone call (65.7%). %), denial of service (61.5%) and other types of compromise (35.66%).

It is important to note that in the questionnaire completed by the respondents, no type of definition was offered for this question, but rather it appealed to what the users themselves understood about this type of concepts.

Graph 47. Digital incidents about which users believe they have knowledge

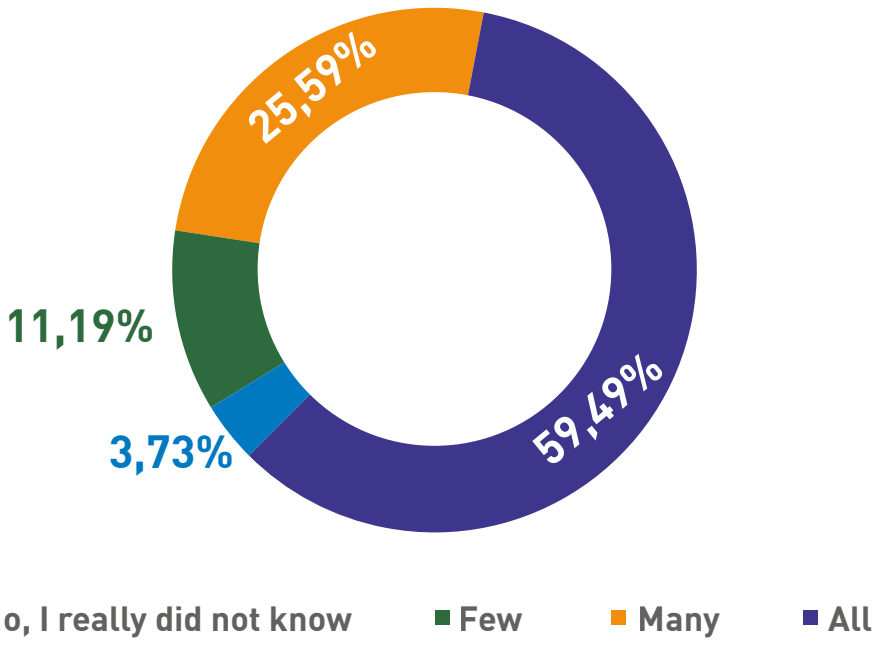


Note: 603 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

After respondents expressed their answer about the cyber incidents they thought they knew and after being offered their real definitions in order to validate their level of knowledge, it was found that 59.49% said they had knowledge about all the types of incidents, while 25.59% answered that they knew many of the types of incidents, compared to other users who expressed that they knew few of these (11.19%), compaed to those who claimed to be unaware of the issue (3.73%). Thus, according to the answers obtained, 85.08% of the users answered that they knew many or all of the definitions referring to the different types of cyber incidents.

Graph 48. **Level of knowledge regarding the actual definitions of the different types of cyber incidents**

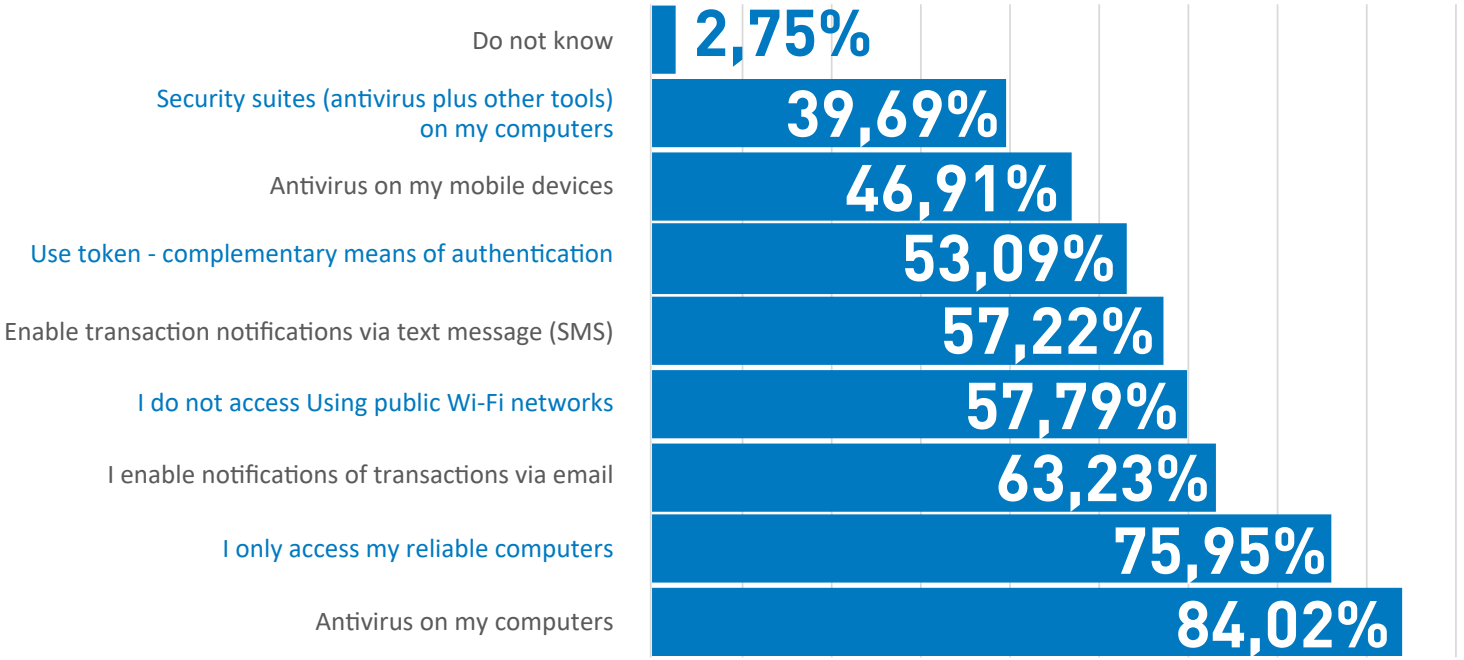


Note: 590 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Once the knowledge about the type of cyber incidents was validated, respondents were asked about the security measures they had implemented to prevent digital incidents. A high percentage (84.2%) said they used antivirus on their computers , followed by other security practices related to exclusive access to reliable computers (75.95%), enabling notifications of transactions via email (62.23%), avoiding accessing through public Wi-Fi networks (59.79%), the use of tokens or complementary means of authentication (53.09%) and, finally, the use of antivirus in mobile devices (46.91%) and security suites (39.69%). Although the percentages for measures such as the use of antivirus and reliable computers are high, it is also true that the results expose the use of devices–to some extent–without security measures, which leads to high levels of exposure to cyber-attacks.

Graph 49. Security measures most used by users to prevent digital incidents

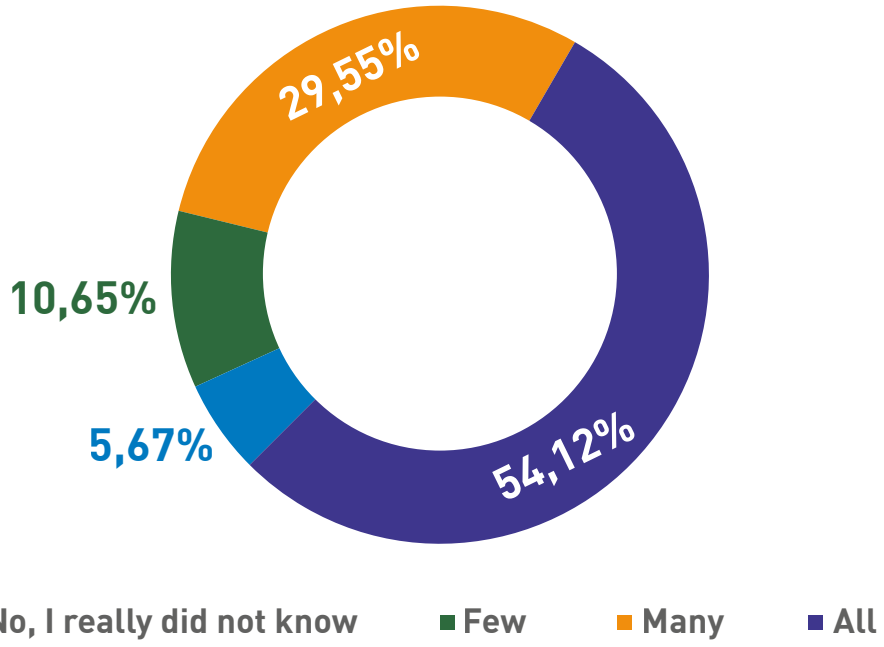


Note: 582 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Similar to the validation of knowledge about cyber incidents, when the interviewed users were consulted about knowing about the measures mentioned in the previous point, most of them said that they knew all the measures (54.12%) and a segment, 29.55%, said they knew many of them, in contrast to lower percentages that claimed to know few or none of them (10.65% and 5.67% respectively). In a manner consistent with the conclusions expressed above, the existence of knowledge related to security practices by the users interviewed is valued, given that 83.67% said that they knew many or all of the measures.

However, regarding the effectiveness of these measures or their level of application, although a specific question in this regard was not included, it is clear that the fact that such measures are known does not necessarily mean that they are used by the user, since most of the time there are difficulties for their implementation (e.g. investment that the user must make to acquire protection solutions) as well as excuses justified in circumstantial situations (e.g. accessing the online banking service or mobile banking through an unsecure free network due to being on vacation), which is why efforts are still required to raise the conscious use of this type of measures much more.

Graph 50. Level of knowledge in relation to exposed security measures

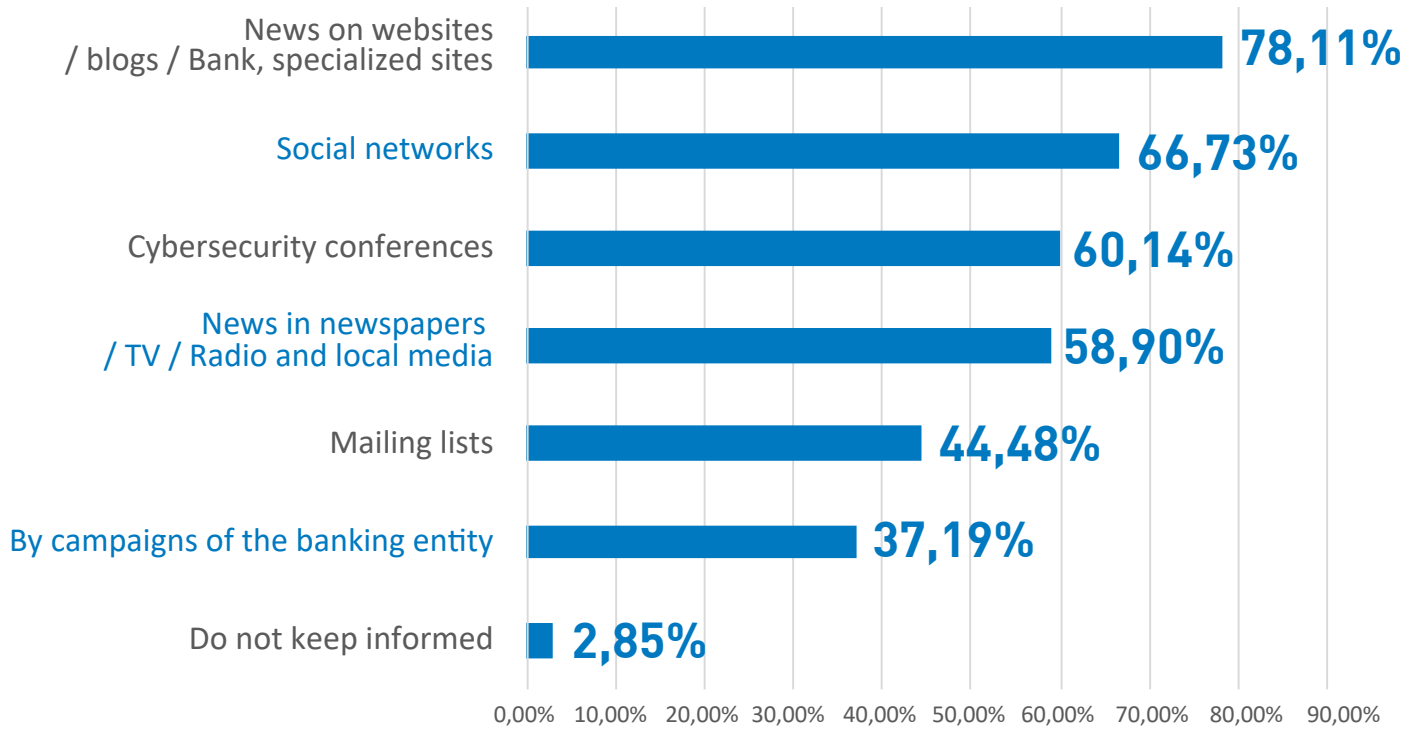


Note: 582 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

One of the aspects that should gain more relevance for users, since they depend more and more on the digital environment, has to do with keeping informed about new forms of attacks and security threats. In this regard, when consulting users about the sources they use the most to learn about these aspects, interviewees indicated that the most-used channels are news on websites, blogs and specialized sites (78.11%), as well as through social networks (66.73%). They also highlight other sources such as cybersecurity conferences (60.14%), news from the traditional written press, news and radio (58.90), mailing lists (44.48%) and campaigns by banking entities (37.19%).

As can be seen from the results, few of the users are informed of the new threats of cybersecurity due to security campaigns carried out by their banking entities, which can show that they are not enough to facilitate the development of awareness about threats targeting the weakest link in the chain, which is precisely the user. However, it is also true that more and more information is available about new forms of attacks and security threats, although they do not yet seem to be widespread in traditional media such as newspapers, TV and local radio stations, since this type of media was in a 4th place among those used by users as a source.

Graph 51. Most common sources used by users to stay informed of new forms of attacks and security threats



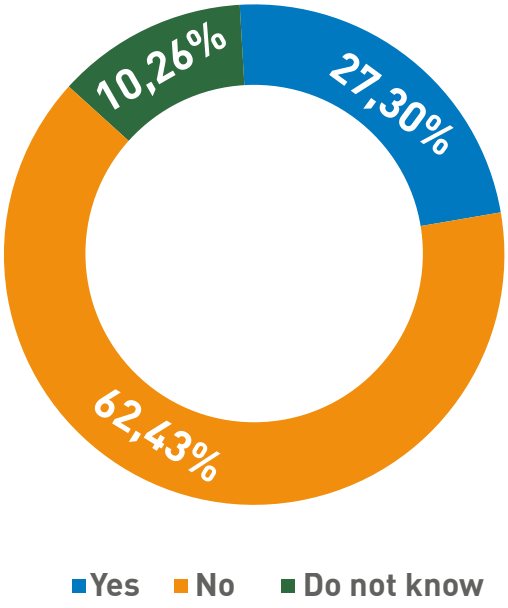
Note: 562 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

5.3 Impact of digital security incidents

In this component of the study, questions were asked to establish the impact suffered by users of banks that completed the survey, in aspects such as the type of digital incidents experienced, frequency, mechanisms and reporting actions, as well as the impact and their compensation or repair and other perception aspects that were considered relevant.

When inquiring of the users surveyed whether they had been compromised with respect to the confidentiality, integrity or availability of their information or their financial resources in their bank, most of them answered NOT having the confidentiality, integrity or availability of their information compromised or its financial resources in its bank (62.45%), compared to a smaller segment that affirmed the opposite (27.30%) and another fraction that declared not knowing and/or did not experience the matter (10.26%). The result shows that approximately 1 out of every 4 users of the banking sector have had some degree of compromise regarding their information or resources due to cyber incidents, which is worth noting.

Graph 52. **Percentage of users who have had the confidentiality, integrity or availability of their information or their financial resources compromised in their bank**



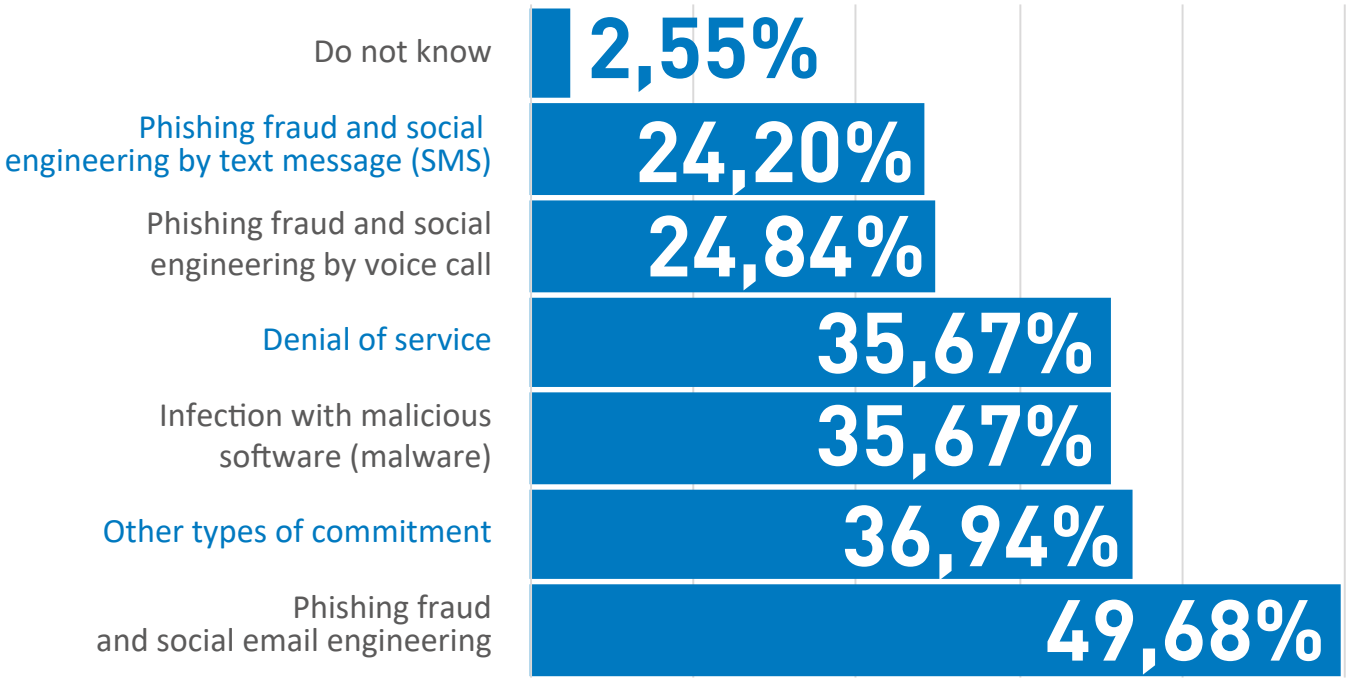
Note: 575 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

In response to the question related to the types of digital incidents experienced, most of them revealed phishing fraud and social e-mail engineering (49.68%) as the most usual, including a lower percentage of other types of compromise (36.94%), infection with malware (35.67%), denial of service (35.67%), phishing fraud and social engineering by phone call (24.84%) and phishing fraud and social engineering by text message (24.02%).

It is clear that attacks that use an email as a vector with the objective of obtaining access information (credentials) from users are still the attacks that most commonly affect them. This coincides with what is said in an analysis of the panorama of financial threats published by experts in Kaspersky Lab (Kaspersky Lab, 2017), which also concludes that a high percentage of phishing attacks (47.48%) are aimed at theft of money from the attacked users.

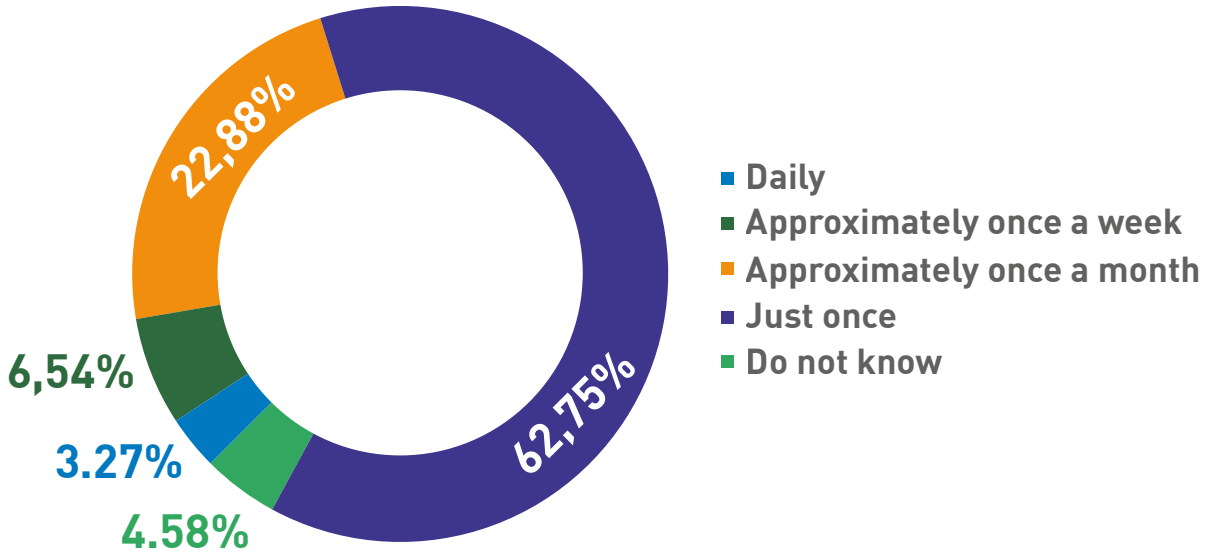
Graph 53. Type of digital incidents experienced by bank users



Note: 157 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Regarding the question about the frequency with which they had been affected by cyber incidents, the majority of users (62.75%) said that they had experienced incidents of this nature only once. This figure contrasts with those who said they had experienced it once a month (22.88%), once a week (6.54%) and daily (3.27%). At this point, it is important to highlight that users are not necessarily aware of being affected by cyber incidents, because not all of them have adopted security mechanisms or measures that, among other aspects, allow them to be warned of this type of situation, such as the alerts provided by the security suites for real-time protection, notifications of access to virtual platforms or notifications of transactions or operations that can be programmed with the bank.

Graph 54. **Frequency of occurrence of cyber incidents suffered by bank users**



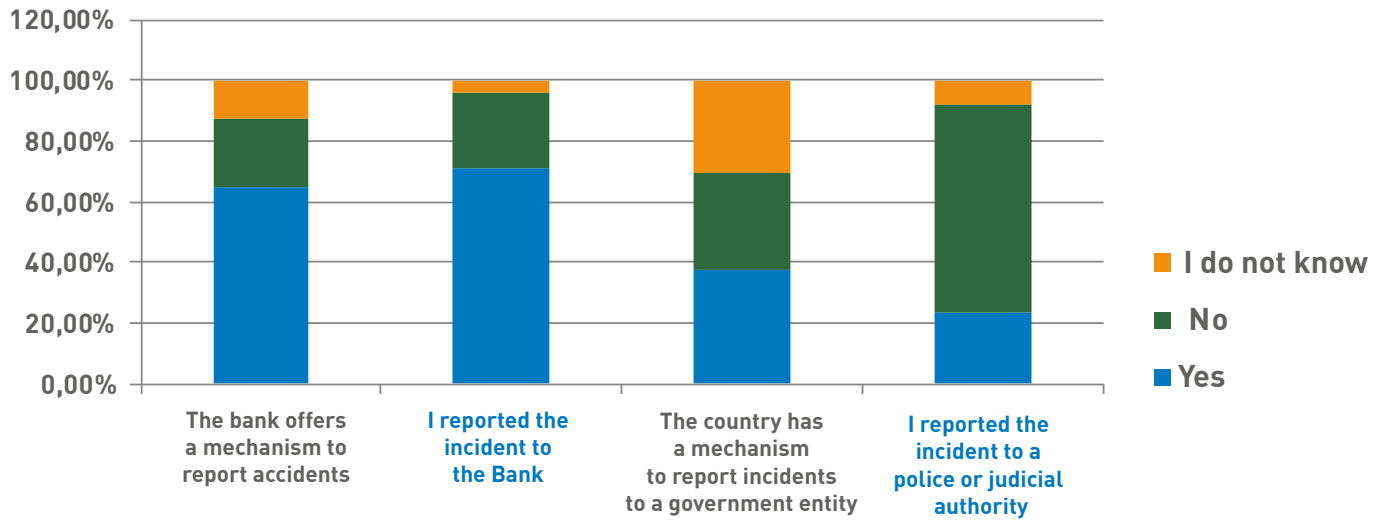
Note: 153 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

In relation to the question related to reporting mechanisms and actions when cyber incidents occur, the majority of interviewed users said that the banking institution does offer a mechanism to report incidents (64.71%) and that in effect they have reported the incident to their bank (71.24%).

On the other hand, it can be highlighted that, according to the answers, only 37.25% affirms that in their country there is a mechanism to report incidents before a governmental entity, while 32.03% indicate that it does not exist and 30.72% do not know of its existence.

The scenario is even less positive if one considers the low level of reporting before police or judicial authorities, given that, of the answers obtained, only 23.53% have reported the incidents that have affected them to these instances. This data requires analysis inasmuch as it could denote difficulties in terms of reporting channels or, low effectiveness in the investigations derived from the reported cases.

Graph 55. Reporting mechanisms and actions in relation to the occurrence of cyber incidents suffered by bank users



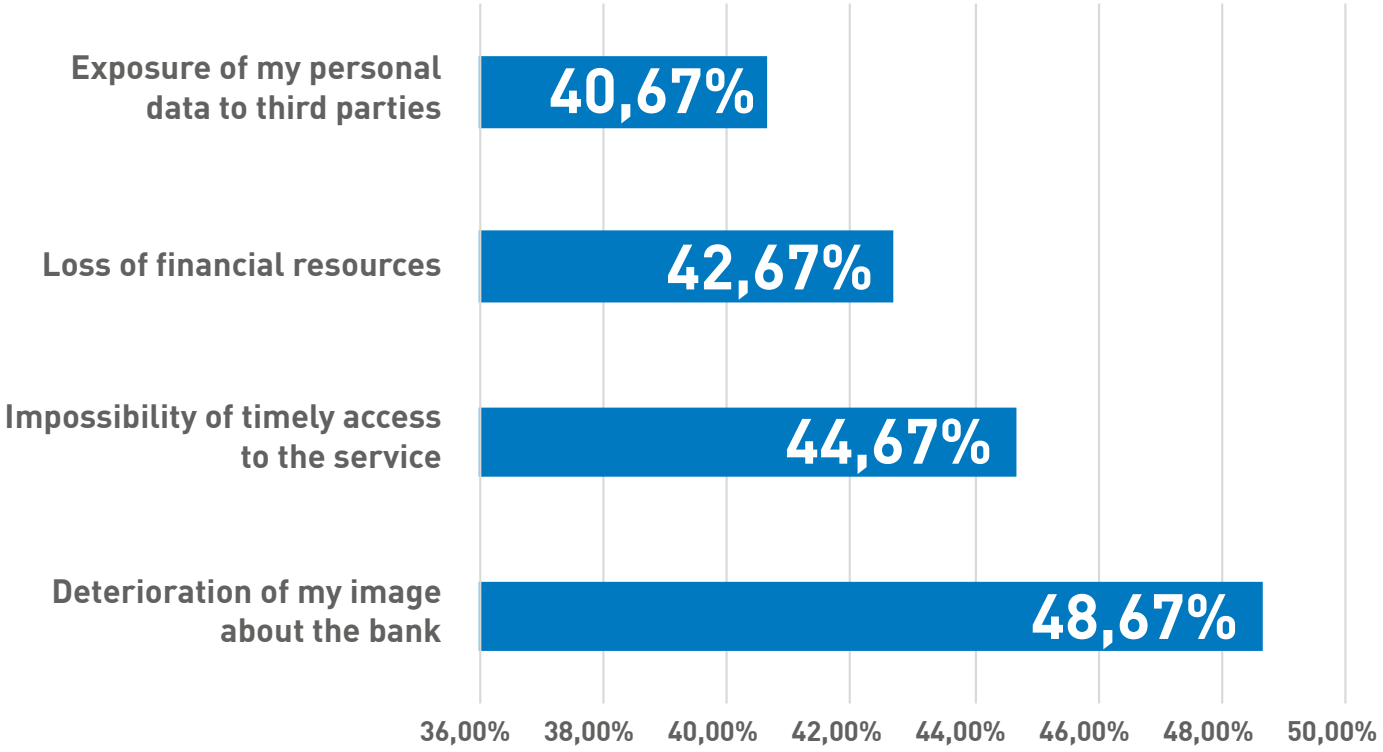
Note: 153 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

A more in-depth assessment of the impact suffered by those who said they had been the object of some type of incident finds that the aspect most negatively affected was their image of the bank (48.67%), accompanied by the impossibility of timely access to the service (44.67%), the loss of financial resources (42.67%) and the exposure of their data to third parties (40.67%).

Taking into account that this response, like many provided by the users, allowed multiple answers, and that in particular this was only answered by those who were affected by some type of cyber incident, it is noted that there is a very close allocation between the percentages of each consequence, which in insufficient to point out that the greatest impact for the user has to do with the affectation of the bank image or reputation.

Graph 56. Impact to banking users due to cyber incidents



Note: 150 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

One of the challenges in assessing the impact of cyber incidents is to determine the financial effect that the aforementioned loss of reputation can have, which, in practice, can translate into loss of clients who decide to "migrate" to another institution or organization for reasons such as distrust.

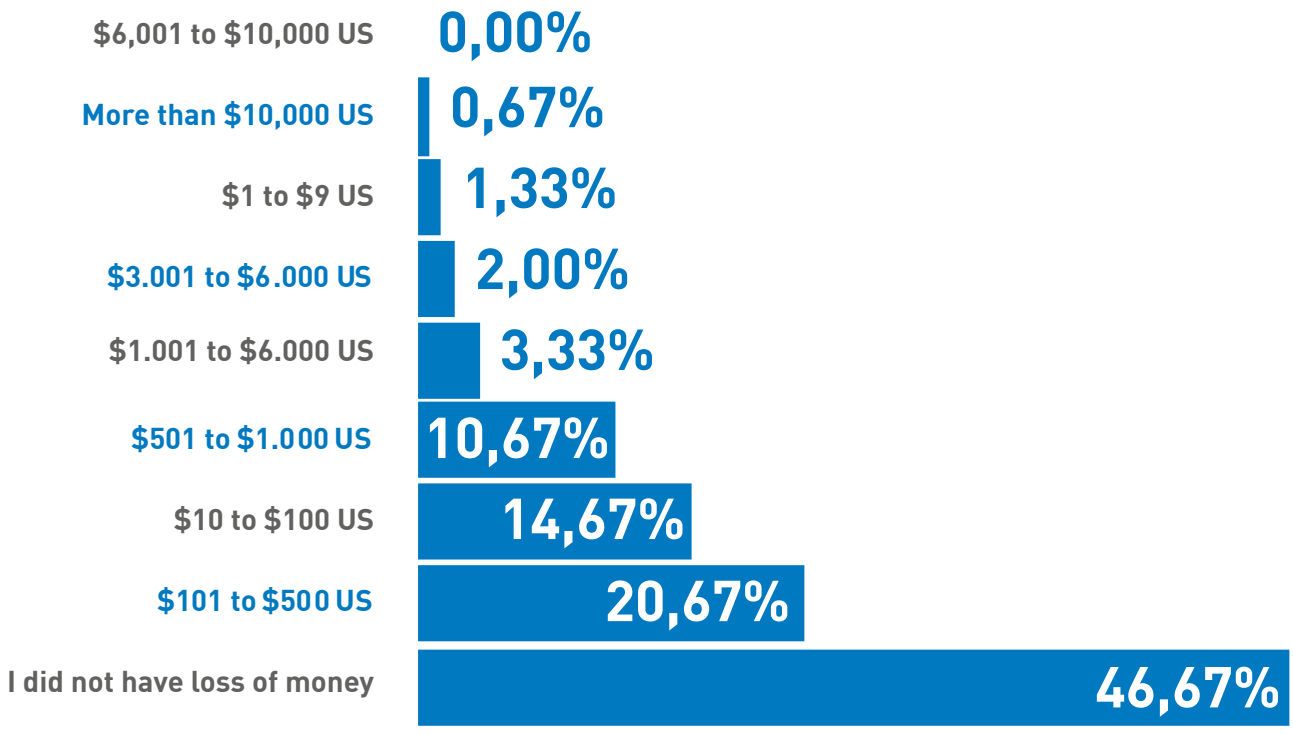
In this sense, it is necessary to highlight the conclusions obtained by the Ponemon Institute and IBM (Ponemon Institute and IBM, 2018), regarding the financial impact of the loss of reputation and brand trust after a cyber security incident, which may be significant in all industries. This report indicates that the financial sector is the second most vulnerable to the loss of clients (only surpassed by the health

sector) and it establishes that the cost of data violations is US$4.20 million for companies in the United States, and it is US$0.47 million for the only country in the region included in the study, Brazil.

Returning to the impact from the perspective of customers, users who had been victims of an incident were asked to indicate the range of the impact they suffered. 47% said they had not lost money, compared to 21% who said they had lost between US$101 to US$500, to 15% who said they had lost between US$10 and US$100, and to 11% who had lost between US$500 and US$1,000, with less relevant results for other ranges of money loss.

In the analysis of the panorama of financial threats published by the Kaspersky Lab experts (Kaspersky Lab, 2017), it was already highlighted that 47.48% of phishing attacks are aimed at the theft of the attacked users' money. The figures obtained in this study are very close to those appearing in the one by Kaspersky, given that precisely, of the response by incident type, 49.68% said that they had been subject to phishing and social engineering via email and, in addition, if the percentages that said that they had lost some amount of money are included, the result is that 53.34% of those affected by an attack actually suffered losses.

Graph 57. Range of Impact (in USD) regarding cyber incidents that affected users



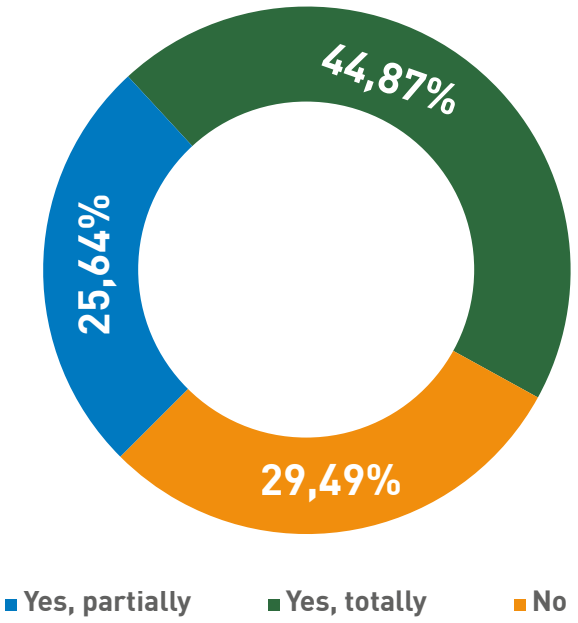
Note: 150 records

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Once the degree of impact was addressed, those who were victims of an attack were consulted if they had been compensated or repaired regarding cyber incidents. In this regard, 44.87% of users surveyed said they had been repaired or fully compensated, compared to 25.64% who said they had been partially compensated and 29.49% who said they had not received any compensation.

In this sense, it is very important to assess that those who did not receive compensation or reparation in relation to the incident suffered became very frustrated and developed other foreseeable consequences, such as an increase in distrust in the use of digital media to carry out their banking operations.

Graph 58. **Percentage of bank users who received compensation or reparation regarding cyber incidents**

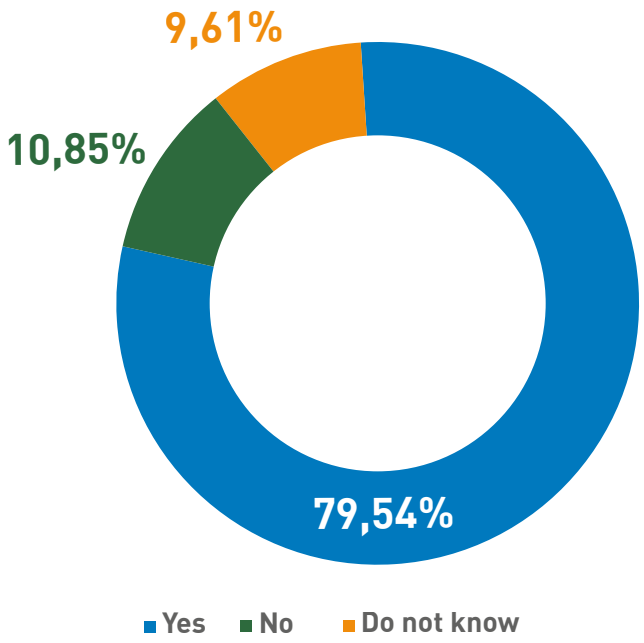


Note: 78 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Subsequently, users surveyed were asked if they considered that the risks of cyber incidents had worsened in the last year, where a majority perception of 79.54% is that this type of incidents has indeed increased, compared to a low percentage of 10.85% and 9.61% that said that they did not perceive this increase or were unaware of it, respectively.

The foregoing, in a way, reflects that the dynamics of digitalization and its inherent risks mean that traditional media, as well as social networks, are increasingly giving visibility to situations related to digital security incidents, events that users begin to see more frequently and, in this way, are deriving in the perception that the risks have worsened.

Graph 59. **Percentage of users that consider that the risks of occurrence of cyber incidents have worsened in the last year**

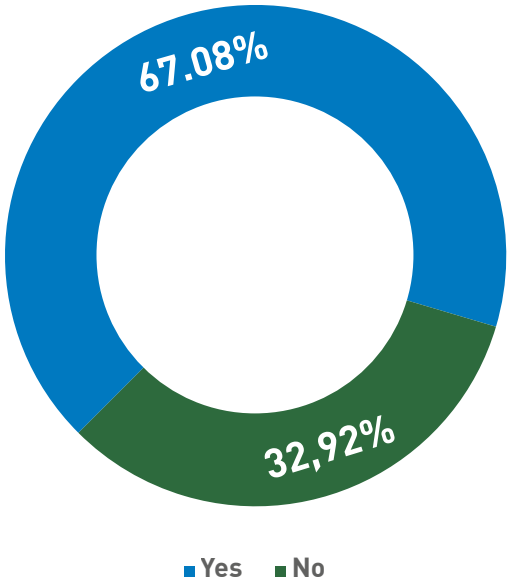


Note: 562 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Finally, users were consulted if they considered that the risks of cyber incidents occurring affected their decision to use digital media in the financial sector. The survey reveals that the majority of users surveyed, 67.08%, consider that the existence of risks derived from cyber incidents does affect their decision to use or not digital media in this sector, compared to only 32.92% that affirms the opposite.

This response begs the reflection on the importance of strengthening the management of digital security risks, comprehensively, so that users and companies find a digital environment that generates trust for all.

Graph 60. Percentage of users that consider that the risks of occurrence of cyber incidents affect their decision to use digital media in the financial sector



Note: 562 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

5.4 Econometric analysis of the results

As in the case of banking entities, econometric models were estimated for the database that contains information at the individual level as a unit of analysis. Econometric estimations that aim to find the factors that determine whether an individual has been a victim of cybersecurity incidents were conducted, based on the question *Have you experienced any incident or situation that has compromised the confidentiality, integrity or availability of your information, or your financial resources in your bank?"*

For this case, a set of indicators that tried to capture the inherent characteristics of the individual were included as dependent variables, and also incorporated were variables associated with whether the recent transactions and available balances were reviewed, the different means of depositing checks/cash, how to get cash, how to make purchases, the different ways to transfer funds, if any digital means are used for banking transactions, the security measures that have been implemented to prevent digital incidents and in the event of being a victim of an incident such as those stated above, the type of incident suffered and how the individual is kept informed of new forms of attacks and information security threats.

As in the previous case, the model used in the estimation had a discrete dependent variable {0,1}, logit or probit, chosen according to the best fit. For this particular case the dependent variable (y) took the value of 1 if the surveyed individual has *"experienced an incident or situation that has compromised the confidentiality, integrity or availability of their information or their financial resources in their bank"* and 0 otherwise. As mentioned in the previous paragraph, independent variables related to the aforementioned topics were included in order to estimate *the probability of occurrence of digital security incidents* or another interpretation to find the factors that determine that a user is a victim of this type of incidents.

The description of the variables used and that can potentially be part of the model is shown in the following table:

Table 19. Variables used in the LOGIT type model used - Users

TYPE	VARIABLE	DESCRIPTION
Inherent characteristics of the bank users	Gender	Female Male
Inherent characteristics of the bank users	Transaction check	Check recent transactions and available balances: Online banking transaction log (Laptop or desktop) • At ATMs • By phone • At the bank • Using mobile banking applications • By tablet • Through social networks (if the bank offers this service integrated to social networks such as WhatsApp, Twitter, etc.)
Inherent characteristics of the bank users	Make check/cash deposits	Makes check/cash deposit: • Mediante un depósito electrónico directo • En cajeros automáticos • En el banco • Por correo • Mediante depósito móvil
Inherent characteristics of the bank users	Cash	Get cash: • At the ATM • At the bank • In shops, when you make a purchase using your debit or credit card • In ATM through transactions without card
Inherent characteristics of the bank users	Purchases made	Shop: • With a check • With a credit card • With a debit card • By phone with card • On the Internet with card • On the Internet using virtual currencies (e.g. Bitcoin, Etherum, Litecoin ...) • On the mobile device with registered accounts/cards
Inherent characteristics of the bank users	Fund transfers	Transfer of funds: • ATM • With Internet banking operations (Laptop or desktop) • With mobile banking operations • At the bank • "International transfers (via electronic transfers or by ACH systems)" • With a tablet • Through social networks (if the bank offers this service integrated to social networks such as WhatsApp, Twitter, etc.)
Inherent characteristics of the bank users	Digital transactions	¿Do you use any digital means for your banking transactions? Choose the options you use the most. • Smartphone • Laptop • Desktop • I do not use

TYPE	VARIABLE	DESCRIPTION
Digital security culture	Security measures for incident prevent	What security measures have you implemented to prevent digital incidents? (multiple answers possible) • Antivirus on my computers • Security suites (antivirus plus other tools) on my computers • Antivirus on my mobile devices • I only access reliable computers • I do not access using public Wi-Fi networks • I use token - complementary means of authentication • I enable notifications of transactions via email • I enable transaction notifications via Text Message (SMS) • I do not know
Impact of digital security incidents	Experience of incidents that have affected the confidentiality, integrity or availability of infor-mation or resources	Have you experienced any incident or situation that has compromised the confidentiality, integrity or availability of your information or your financial resources in your Bank?
Impact of digital security incidents	Type of digital incidents experienced	Which? (multiple answers possible) • Infection with malicious software (malware) • Phishing fraud and social engineering by email • Phishing fraud and social engineering by text message (SMS) • Phishing fraud and social engineering by voice call • Denial of service, I have tried to access Bank services and they do not work • Other types of compromise • I do not know
	Report of incidents	In case you have been the victim of an incident such as those listed above: • The bank offers a mechanism to report incidents • I reported the incident to the Bank • The country has a mechanism to report incidents to a government entity • I reported the incident to a police or judicial authority
	Knowledge of forms of attacks	How do you stay informed of new forms of information security threats and attacks? (multiple answers possible) • Mailing lists • Cybersecurity conferences • News on websites/blogs/from the Bank, specialized sites • News in newspapers/TV/Radio and local media • Social networks • On the part of campaigns of your bank entity • I am not kept informed

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Regarding the results of the estimations, Logit type models were run, with the individuals who answered the survey as unit of analysis. Different models were estimated including the independent variables described above. Information was used from 516 observations (Individuals). After trying different functional forms and independent variables, the model with the best fit –Logit– was chosen. In general, the model presents a good global adjustment according to the statistic LR chi2(22)=63.50, with a probability close to 0.00. The above indicates that the model represents, to a large extent, the variability in the occurrence of cybersecurity events in individuals.

Table 20. Results of the Logit model estimates, the dependent variable (y) takes the value of 1 if the surveyed individual "has experienced an incident or situation that has compromised the confidentiality, integrity or availability of his/her information or his/her financial resources at his/her bank" and 0 otherwise

INCIDENT	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
gender	-.2065386	.2456746	-0.84	0.401	-.688052	.2749747
age	.0108815	.0111275	0.98	0.328	-.0109279	.032691
operInternet	.3615521	.3521736	1.03	0.305	-.3286955	1.0518
operTel	.02484	.2381028	0.10	0.917	-.4418329	.4915128
operCajAut	.3450024	.2608198	1.32	0.186	-.166195	.8561998
operBanco	-.2408654	.2749635	-0.88	0.381	-.7797839	.2980531
operBancaMov	-.3607537	.2963595	1.22	0.223	-.9416076	.2201002
operTableta	-.1534206	.3541618	-0.43	0.665	-.8475649	.5407238
operRedSoc~l	-.772404	.8930911	-0.86	0.387	-2.52283	.9780224
depositoCE	.3649712	.2510195	1.45	0.146	-.1270179	.8569603
depositoCA	**.6009711**	**.2373969**	**2.53**	**0.01***	**.1356818**	**1.06626**
deposiBanco	-.0066537	.2753938	0.02	0.981	-.5331083	.5464157
deposiCorreo	-1.969646	1.350401	-1.46	0.145	-4.616383	.6770916
depositoCel	.3746377	.3068151	1.22	0.222	-.226709	.9759843
dineroCA	.3747039	.4621943	0.81	0.418	-.5311803	1.280588
dineroBanco	**.7062953**	**.2756089**	**2.56**	**0.010***	**.166111**	**1.246479**

dineroCome~o	.0050634	.2611094	0.02	0.985	-.5067017	.5168284
dintransST	.6001545	.3933962	1.53	0.127	-.1708879	1.371197
comprasCheq	**-.9572553**	**.5761834**	**-1.66**	**0.097****	**-2.0865**	**.1720434**
comprasTC	-.0748638	.2743527	-0.27	0.785	-.6125852	.4628576
comprasDebit	-.4390602	.2930469	-1.50	0.134	-1.013422	.1353012
comprasInt~j	-.396239	.2722661	-1.46	0.146	-.9298708	.1373927
comprasIntMV	.4047265	.4051272	1.00	0.318	-.3893082	1.198761
comprasCEL	**.5082132**	**.2779714**	**1.83**	**0.068****	**-.03660**	**1.053027**
transFonCA	-.2168885	.2820771	-0.77	0.442	-.7697495	.3359724
transFonIn~r	-.0697841	.3379164	-0.21	0.836	-.7320881	.5925199
transfonBM	-.0437132	.2710962	-0.16	0.872	-.5750521	.4876256
transFonBa~o	.2205555	.2672388	0.83	0.409	-.3032229	.744334
transfonTa~e	-.2086551	.4188517	-0.50	0.618	-1.029589	.6122791
transFonRS	.3766884	1.907193	0.20	0.843	-3.36134	4.114717
transSmartF	**.6252682**	**.2909906**	**2.15**	**0.032***	**.054937**	**1.195599**
tranComPor	.4134584	.2960858	1.40	0.163	-.1668592	.9937759
transComEscr	.0360544	.2252133	0.16	0.873	-.4053557	.4774644
usaAntiv	.1587091	.3296124	0.48	0.630	-.4873194	.8047376
usaSuites	.093945	.2345227	0.40	0.689	-.3657112	.5536011
usaAVCel	.0375865	.2318763	0.16	0.871	-.4168827	.4920558
usaComConfi	**-.7369588**	**.279212**	**-2.64**	**0.008***	**-1.28420**	**-.1897134**
usaWiFiPub	.0372853	.2427845	0.15	0.878	-.4385636	.5131342
usaToken	-.0678162	.251414	-0.27	0.787	-.5605787	.4249463
usaNotiMail	**.524101**	**.2829487**	**1.85**	**0.064****	**-.03046**	**1.07867**
usaNotiCel	-.2190288	.257546	-0.85	0.395	-.7238097	.2857521
_cons	-2.29986	.7265458	-3.17	0.002	-3.723864	-.8758564

Number of obs = 516, LR chi2(41) = 63.50, Prob > chi2 = 0.0136, Log likelihood = -285.29674, Pseudo R2 = 0.1001

The inherent independent variables of the individual Age and Gender were included. Both were not significant in the model at the conventional levels of 5 and 10%. The foregoing establishes that digital security incidents occur in a similar manner in both men and women. It is also not possible to conclude that digital security incidents in individuals are related to age.

Variables associated with the means for the review of recent transactions and available balances of the individuals surveyed were added in bloc. This factor was classified as a record of online banking operations (laptop or desktop), at ATMs, by telephone, at the bank, using mobile banking applications, by tablet, by social networks (if the bank offers this integrated service to social networks such as WhatsApp, Twitter, etc.). Each of these characteristics was included in the model through dummy variables: 1 if the characteristic is present and 0 otherwise. None of these variables was significant in the estimated model, considering levels of significance of 5 and 10%.

On the other hand, a block of variables related to the way in which users (individuals) make deposits by check or cash was also added to the model. This is done through different channels such as: Direct electronic deposit, at ATMs, at the bank, by mail, through mobile deposit. Each of these characteristics was included in the model through variable dummies: 1 if the characteristic is present and 0 otherwise. In this block of variables, "depositoCA" resulted significant, that is, an ATM deposit. This variable is highly significant in the model, presenting a positive sign, which would lead to the conclusion that insofar as individuals use means of direct deposit in an ATM, the probability of the occurrence of digital security events increases. However, it was not possible to definitely establish a reason or explanation on the result of this dependent variable, considering that ATM deposits do not in themselves represent a risk factor inherent in digital security incidents, in the same way that a user could be exposed when using other digitally-based media, such as mobile applications or the bank's website.

Likewise, variables associated with the way in which individuals procure cash were included. Dummies were created to represent the following situations for the individual: When the individual obtains money at the ATM, at the bank, at stores when making a purchase using a debit or credit card, and at the ATM through transactions without a card. From this set of variables "dineroBanco", was significant, which would suggest that those individuals who obtain money directly in banking entities are more likely to experience digital security incidents. This variable was significant in the model at 5% levels. As in the previous case, it was not possible to definitely establish a reason or explanation about the result of this dependent variable, considering that the withdrawals of money at the bank do not represent in themselves an inherent risk factor for digital security incidents.

In the econometric model variables were also included on the way in which individuals make purchases. To this end, a set of variables was included to represent the different ways in which individuals buy goods and services classified in: Purchases with check, purchases with a credit card, with a debit card, by telephone with a card, purchases online with a card, online purchases using virtual currencies (e.g. Bitcoin, Etherum, Litecoin ...) and purchases with the mobile device with registered accounts/cards. Dummies were used for each of these variables: 1 if the individual has the respective characteristic and 0 otherwise. Of this set of variables, "comprasCheq" was significant at the level of 10%. The estimation resulted with a negative sign, indicating that individuals who have this way of paying for purchases, have a lower probability of safety incidents. For its part, the variable "comprasCEL" was also significant at 10%, estimated with a positive sign. This suggests that individuals who use this form of shopping, that is, through mobile devices, are more likely to have digital security incidents.

In addition to the above variables, indicators were included at the individual level that describe the form of funds transfer. For the above, the following indicators were considered which were included through dummies: Taking the value of 1 if the individual has the characteristic and 0 otherwise. In total, the following ways of transferring funds were considered: Through an ATM, with Internet banking operations (laptop or desktop), through mobile banking operations, at the bank, with international transfers (via electronic transfers or through ACH systems), using a tablet and through social networks (if the bank offers this service integrated to social networks such as WhatsApp, Twitter, etc.). In this set of independent variables, "transSmartF" was significant at 5% and with a positive sign. The foregoing is interpreted in the sense that those individuals who transferred funds through Smartphone have a higher probability of events of digital security incidents.

Regarding the security measures that have been implemented to prevent digital incidents, information was collected at the individual level about a series of behaviors to defend against attacks. The following options were considered: Use of antivirus on computers, installation of security "Suites" (antivirus and other tools) on computers, use of antivirus on mobile devices, access only on reliable computers, avoiding access to public Wi-Fi networks, use of token (complementary means of authentication), enabling notifications of transactions via email and enabling notifications of transactions via Text Message (SMS). From the estimation it is observed that the variable "usaComConfi", which refers to the use of a reliable computer, presents a negative and significant sign at 1%. This suggests that users who have this strategy to defend against possible attacks actually experienced a lower probability of digital incidents. For its part, the variable "usaNotiMail", which refers to the authorization of transaction notifications via email, was significant, although at levels of 10%. This variable resulted in a positive sign, indicating that individuals who use this type of mechanism, on average, had a higher probability of digital security incidents. This can be explained in the ease for the user to learn of any fraudulent access or operation when the user receives notifications from the bank. Otherwise, when users do not have this type of service activated and they only realize the irregularity when checking their bank movements (although they can sometimes go unnoticed or not to be checked by the banking user) or when facing atypical situations that are too obvious.

The following table presents the marginal effects of the independent variables calculated on the average:

Table 21. **Results of the marginal effects of the LOGIT model**

Variable	dy/dx	Std. Err.	z	P>|z|	95% C.I.]		X
Deposi~A*	.1255893	.05097	2.46	0.014	.025687	.225492	.335271
Deposi~o*	-.2325664	.07071	-3.29	0.001	-.371161	-.093971	.015504
Diner~co*	.1453612	.05721	2.54	0.011	.033241	.257481	.408915
Compra~q*	-.1538175	.0695	-2.21	0.027	-.290044	-.017591	.04845
Compra~L*	.1068385	.0606	1.76	0.078	-.011926	.225603	.281008
TransF~A*	-.0424785	.05368	-0.79	0.429	-.147686	.062729	.228682
TransS~F*	.1208319	.0535	2.26	0.024	.015981	.225683	.631783
UsaCom~i*	-.1594545	.06338	-2.52	0.012	-.283673	-.035237	.76938

Marginal effects (ME) show the change that is created in the probability of "having experienced an incident or situation that has compromised the confidentiality, integrity or availability of user information or financial resources in user's bank", given a change in each dependent variable keeping the other variables constant. In other words, the ME is estimated as the partial derivative of the probability function with respect to the vector of independent variables, evaluated in their means. For example, the use of a reliable computer "usaCom~i", which was a significant variable to the model, of a negative sign, is interpreted to decrease the probability of incident occurrence by 0.15%.

06

CYBERSECURITY RECOMMENDATIONS FOR THE LATIN AMERICA AND THE CARIBBEAN BANKING SECTOR

Based on the findings, a set of cybersecurity recommendations was established for the banking sector in Latin America and the Caribbean. For this purpose, the recommendations targeted three (3) groups: i) the banking entities of Latin America and the Caribbean, ii) the users of said entities in the region and iii) the government agencies, regulators and agencies of application of the law.

6.1 For banking entities in Latin America and the Caribbean

It is important to note that these suggestions are prepared in a general manner and may be obvious for some organizations. But they have been included, considering the heterogeneity of the banking entities in the region and their different digital security development and maturity levels. The recommendations are grouped using the same thematic structure utilized in the information collection instrument.

6.1.1 In aspects of preparedness and governance

- Where possible, have a single responsible level or corporate governance body to lead the Digital Security risk management (including aspects of information security, cybersecurity and fraud prevention using digital media).

- Although the aim is to specialize several areas of the organization–in matters of information security, cybersecurity and fraud prevention using digital media–as the banking entity grows, it must be guaranteed that they work coordinatedly and effectively to achieve an efficient Digital Security risk management.

- Properly size the work teams dedicated to Digital Security aspects, carry out safety evaluations of the associates, adequately segregate roles and functions, guarantee knowledge management processes that break down "unipersonal" departments, and establish mechanisms to increase loyalty and retention in the officers relying on the development of human talent and considering incentive plans.

- Have formal mechanisms for the selection of outsourced service providers associated with Digital Security, with adequate selection criteria and with clear contractual conditions that guarantee the protection of personal data, confidentiality, service level agreements and other requirements that "shield" outsourced activities.

- Establish clear mechanisms to ensure knowledge of Digital Security risk management by the decision-making bodies in the organizations (senior executives and other leadership teams) and conduct awareness-raising processes periodically with the active participation of its members, in order to raise the priority and support for these issues.

- Carry out a regular review of the best practices and/or applicable international standards around Digital Security, as well as the local and international regulatory framework applicable to the banking entity, performing a mapping and prioritization process for application. The process must include the analysis of gaps in relation to what is required, the valuation of resources for the adoption of processes, tools and technologies, as well as required personnel training and change management processes, among others.

- It is of the utmost importance to carry out the processes of adoption and implementation of regulatory frameworks (local and international), best practices and/or international standards, with a guide that goes beyond verification "checklists" and that they actually become positive transformation processes, with the purspode of the continuous improvement and even the strengthening of the culture of security.

6.1.2 In aspects of detection and analysis of digital security events

- Guarantee that the prioritization of Digital Security actions, processes and technical measures to protect the banking entity's critical information systems correspond to a plan considering the needs of adoption and implementation of regulatory frameworks (local and international), best practices and/or international standards. It is vital that one of the objectives of this plan be to raise cyber resilience[28].

- Mechanisms should be in place tp check the detection and analysis of security events, preferably through collaboration with public or private incident response teams. This means validating whether the developed capacities are being able to predict or detect threats with the same degree of effectiveness as other response teams.

- Prioritize the development of capacities using emerging digital technologies, such as Big Data, Artificial Intelligence and related (such as cognitive computing and Machine Learning), which have an important potential in the optimization of resources destined for detection and prevention.

- Extending the detection and prevention layer to the sphere of interaction carried out by users, for example, incorporating detection or prevention solutions[29] that users can install on their devices, on a voluntary basis, which also increases the perception of trust in the service by users.

6.1.3 In aspects of management, response, recovery and reporting of digital security incidents

• Guarantee the design and implementation of a strategy of prioritization, containment, response and recovery of digital security incidents (successful attacks), which must articulate the participation of third parties, as appropriate to the different stages, processes or associated protocols. Particularly important is the designation of responsibilities and intervention moments by suppliers, escalation or intervention of response teams that are external to the bank (for example, sector or country incident response teams, if applicable).

• Support investigations and follow the protocols required by law enforcement authorities and the best practices applicable to the chain of custody of digital evidence (for example, facilitating transnational cooperation), which are relevant to the investigative processes.

• Perform processes to assess the maturity of Digital Security on a regular basis by suitable external agents, to establish opportunities for improvement, prioritization and updating of plans and strategies related to Digital Security (including aspects of security of the information, cybersecurity and fraud prevention using digital media).

• Guarantee adequate communication to clients of the reporting mechanisms available to them by the bank in the event that they are victims of digital security incident

6.1.4 In aspects of training and awareness

- Inculcate cybersecurity concepts and good practices, especially with a focus on those areas most related to innovation and digital transformation processes.

- Assimilate design criteria for digitally-based products and services under the principle of "security from the start".

- Provide training plans with specific target audiences (internal employees, bank insourcing, suppliers, customers, etc.) that are aimed at raising the digital security culture, the development of skills and awareness (as the case may be), guaranteeing their periodic implementation and establishing evaluations in order to determine their impact.

- Actively participate in discussion spaces (forums, work tables, conferences, etc.).

- Carry out campaigns to prevent i) phishing, ii) social engineering and iii) spyware (malware or Trojans), aimed at its financial services users.

6.1.5 In aspects related to the impact of digital security incidents

- Establish responsibilities within the banking entity to concentrate or centralize the registry of digital security incidents and determine the quantification methods of their economic impact for the organization.

- Make available cost centers or other methods to determine the classification of investments and recurrent expenses related to digital security, so that its weight can be accurately assessed compared to the organization's other items and its behavior.

- Establish, as precisely as possible, the rate of return of investments made in relation to digital security. Starting from an adequate valuation of the banking entity's assets, as well as estimating the costs associated with the impact derived from possible digital security incidents.

- Communicate strategically to senior management and government bodies that the resources allocated to digital security are not a cost, but really an investment and that protection against digital incidents should be an integral part of the business strategy, given the high impact and repercussion that can be derived from occurrence.

6.2 For users of banking entities in Latin America and the Caribbean

Users are and will continue to be the weakest link in the chain of digital security, hence the importance of strengthening their capacities in the face of digital incidents directed against them and promoting practices that make them less vulnerable. Here are some recommendations:

- Avoid the use of links sent by email

- Avoid the use of links sent by email or text messages, as a supposed access channel to the bank. Keep in mind that these entities never make requests for access data information (credentials) by these means, nor by phone or text message.

- In all cases, directly type in the address of the financial institution's portal and determine the authenticity of the bank's access website by checking that the connection is secure (an image of a padlock must appear next to the address line of the website).

- Establish robust authentication or identification mechanisms with your bank, for example, of multiple authentication factors, such as physical token, passwords for one-time use (One-Time-Password),

and the use of virtual keyboards during access, among others. It is important to find out the authentication or identification mechanisms the bank offers to provide more security in carrying out transactions.

• Use strong passwords (sequences of at least eight characters that combine uppercase letters, lowercase, as well as numbers and special characters) and not use the same password for different online services, including electronic banking. The fact that a password is exposed could facilitate access to fraudulent operations, which is why they should also be changed periodically.

• Avoid storing passwords to access banking entities automatically by the browser on personal devices. Although it is a convenient option because it speeds up access, it should be considered that access to a third party could be facilitated in case of theft or loss of the device.

• Activate notifications of transactions and operations with the bank through email or text messages to the mobile phone. Verify what options the bank offers to send these notifications, including access through virtual channels.

• Periodically access the respective electronic banking account to verify the accounts that have been registered to make transfers to third-party accounts of the same bank and inter-bank. Make sure that there are no registered accounts other than those that have been effectively registered.

• Have antivirus solutions or security suites (antivirus and other tools) on devices, in order to be alerted to possible infections with malware or access to potentially risky links.

• Perform banking transactions only from reliable computers, that is, the security conditions of which are previously known. Avoid using public access computers and in case you do not have another option, be sure to erase browsing history, temporary Internet files and turn off the computer when finished.

• Do not carry out banking transactions through public WiFi-connected devices, given that they do not offer the adequate security conditions for this type of operations.

• Stay informed of new forms of digital security threats and attacks. In particular, pay special attention to communications or campaigns related to digital security performed by the bank.

• Faced with any type of incident, report to the bank through the mechanism established for this purpose. Find out if, in addition to reporting the incident to the bank, it is necessary to carry out any other type of management or procedure, for example, before law enforcement authorities, and offer all the relevant information about the incident.

6.3 For government agencies, regulators and law enforcement agencies

- Carry out the review of the catalog of critical infrastructure, in order to assess its current status, the prioritization of the management of its associated risks and in particular the impact and effects of attacks to other infrastructures (for example, telecommunications or energy) that could affect the banking system.

- Coordinate efforts with trade associations or banking associations aimed at the development of digital security capabilities, preferably regulated through an agenda with expected results, milestones, resources and responsible parties.

- Develop knowledge management networks based on the capacities of the different response teams of the banking sector, other sector teams and the national focal point, incorporating the voluntary participation of other government levels, the private sector, academia, technical and professional communities and Non-Governmental Organizations, interested in contributing.

- Evaluate the relevance of developing cyber-exercises that generate challenging spaces to promote the development of digital security capabilities.

- Raise the capacities of law enforcement authorities regarding support for the response, investigation and prosecution of cybercriminals.

- Establish and socialize protocols for the management of digital evidence and guarantee its chain of custody.

- Issue guidelines, recommendations and instructions, as the case may be, derived from the periodic review of best practices and/or applicable international standards regarding digital security, as well as the international regulatory framework applicable to the banking sector, and if necessary issue the necessary legal instruments for application.

- Evaluate the relevance of establishing the mandatory reporting of digital security incidents by banking entities, of the incidents suffered, mainly to the incident response team of a national nature or focal point in the matter. It should be ensured that the aim of this report be the basis for the inquiries, investigations and associated work required for the understanding of the incident and its scope, as well as the understanding of the context where it occured in order to alert and take complementary measures by other banking entities or actors.

- Require banking institutions to provide reporting mechanisms their clients can use to report, if they have been victims of digital security incidents. Evaluate the effectiveness of their dissemination and socialization processes.

- Promote knowledge transfer and capacity development processes through collaboration, assistance and cooperation at local and international levels.

BIBLIOGRAPHY
ANNEX 1
ANNEX 2
ANNEX 3
REFERENCE NOTES

07

Bibliography

Accenture Security. (2017). Building Confidence - Solving Banking's Cybersecurity Conundrum, High performance security report.
Retrieved from www.bankdirector.com;
www.bankdirector.com/files/4515/1982/3582/2018_Risk_Survey_Report.pdf

Bankdirector. (2018). 2018 Risk Survey.
Retrieved from www.accenture.com;
www.accenture.com/t20170419T051104Z__w__/us-en/_acnmedia/PDF-49/Accenture-Building-Confidence-Solving-Bankings-Cybersecurity-Conundrum-Info.pdf#zoom=50

BDO. (2017). Cyber Security in Banking Industry. Our perspective.
Retrieved from www.bdo.in;
www.bdo.in/getmedia/b478e1ec-a9a3-4afe-997a-3aed7d190164/Cyber-Security-in-banking-industry.pdf.aspx?ext=.pdf&disposition=attachment

BID & FELABAN. (2014). PYME y Bancos en América Latina y el Caribe el "Missing Middle" y los Bancos - Séptima Encuesta 2014.
Retrieved from www.felaban.net;
www.felaban.net/archivos_publicaciones/archivo20150702202150PM.pdf

Capgemini. (2017). Top 10 Trends in Banking – 2017.
Retrieved from www.capgemini.com:
www.capgemini.com/wp-content/uploads/2017/07/banking_trends_2017_web_version.pdf

Cisco. (2018). Reporte Anual de Ciberseguridad CISCO 2018.
Retrieved from www.cisco.com:
www.cisco.com/c/es_co/products/security/security-reports.html#~stickynav=3

Ernst and Young . (2018). Global banking outlook 2018 - Pivoting toward an innovation-led strategy.
Retrieved from www.ey.com:
www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2018/$File/ey-global-banking-outlook-2018.pdf

Felaban. (2018). Informe Quarterly Económico Bancario Regional FELABAN, Edición No. 9 / 30 de abril de 2018 Cifras con corte a diciembre de 2017.
Retrieved from www.felaban.net;
www.felaban.net/archivos_publicaciones/archivo20180509104600AM.pdf

Global Knowledge. (2017). 2017 IT Skills and Salary Report. A comprehensive Study from Global Knowledge.
Retrieved from www. mindhubpro.pearsonvue.com;
https://mindhubpro.pearsonvue.com/v/vspfiles/documents/2017_Global_Knowledge_SalaryReport.pdf

ISACA. (2017). State of Cyber Security 2017 - Resources and Threats.
Retrieved from https://cybersecurity.isaca.org/;
https://cybersecurity.isaca.org/static-assets/documents/State-of-Cybersecurity-part-2-infographic_res_eng_0517.pdf

ISACA. (2018). State of Cybersecurity 2018 - Contours of the Skills Gap.
Retrieved from https://cybersecurity.isaca.org/;
https://cybersecurity.isaca.org/state-of-cybersecurity

Kaspersky Lab. (2017). Informe de amenazas financieras: Cada segundo un ataque de phishing apunta al robo de su dinero.
Retrieved from Kaspersky Lab;
https://latam.kaspersky.com/about/press-releases/2017_informe-de-amenazas-financieras-cada-segundo-un-ataque-de-phishing-apunta-al-robo-de-su-dinero

Office of Financial Research. (2017). Cybersecurity and Financial Stability: Risks and Resilience.
Retrieved from www.financialresearch.gov;
www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf

Ponemon Institute e IBM. (2018). Cost of a Data Breach Study.
Retrieved from Cost of a Data Breach Study;
www.ibm.com/security/data-breach

Price Waterhouse Cooper. (2017). Top financial services issues of 2018.
Retrieved from www.pwc.se;
www.pwc.se/sv/pdf-reports/finansiell-sektor/top-financial-services-issues-of-2018.pdf

PwC. (Junio de 2018). PwC's 2018 Digital Banking Consumer Survey: Mobile users set the agenda.
Retrieved from PwC Financial Services;
www.pwc.com/us/en/financial-services/publications/assets/pwc-fsi-whitepaper-digital-banking-consumer-survey.pdf

Symantec .(2017). Internet Security Threat Report - Financial Threats Review 2017, An ISTR Special Report.
Retrieved from www.symantec.com;
www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pd

The Financial Brand. (2018). Mobile banking features digital security.
Retrieved from The Financial Brand;
https://thefinancialbrand.com/74044/mobile-banking-features-digital-security/

v. (2018). Revitalizing privacy and trust in a data-driven world - Key findings from The Global State of Information Security® Survey 2018.
Retrieved from www.pwc.com;
www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

World Bank Group. (2018). Financial Sector's Cybersecurity: Regulations and Supervision.
Retrieved from documents.worldbank.org;
http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf

World Economic Forum. (2018). The Global Risks Report 2018, 13th Edition.
Retrieved from www3.weforum.org;
www3.weforum.org/docs/WEF_GRR18_Report.pdf

ANNEX 1

Table 22. Information on the Latin America banking sector based on 2017 data from FELABAN

Country	Banking Institutions FELABAN Dec 2017	Bank Branches FELABAN Dec 2017	Branches by Entity Dec 2017	Total Assets Dec 2017 USD Bil	Accumulated Net Income Dec 2017 US$Bil	Bank with the greatest assets in the country Jun2017 US$Bil		% share of bank assets with the greatest assets in the Total Assets of the country
Argentina	78	4.480	57	USD 185.261	USD 4.578	USD 36.096	Nación (Argentina)	19%
Bolivia	16	1.276	80	USD 29.838	USD 298	USD 4.482	Mercantil Santa Cruz	15%
Brazil	155	21.062	136	USD 2.492.225	USD 28.839	USD 451.114	Do Brasil	18%
Chile	20	21.080	1054	USD 358.246	USD 3.636	USD 54.731	Estado	15%
Colombia	25	5.722	229	USD 194.859	USD 2.545	USD 47.282	Bancolombia	24%
Costa Rica	16	797	50	USD 46.316	USD 297	USD 12.136	Nacional (Costa Rica)	26%
Ecuador	24	1.300	54	USD 38.975	USD 396	USD 10.296	Pichincha	26%
El Salvador	14	424	30	USD 17.072	USD 152	USD 4.376	Agricola	26%
Guatemala	18	3.572	198	USD 41.675	USD 574	USD 10.707	Industrial (Guatemala)	26%
Honduras	15	5.054	337	USD 21.246	USD 220	USD 3.785	Ficohsa	18%
Mexico	53	12.744	240	USD 458.598	USD 7.018	USD 107.439	BBVA BANCOMER	23%
Nicaragua	8	672	84	USD 8.070	USD 171	USD 2.220	De la Producción	28%
Panama	49	561	11	USD 101.410	USD 1.505	USD 15.131	General	15%
Paraguay	17	547	32	USD 20.852	USD 435	USD 3.384	ITAU (Paraguay)	16%
Peru	16	2.120	133	USD 111.295	USD 1.670	USD 36.909	Credito (Perú)	33%
Dominican Republic	18	963	54	USD 29.557	USD 482	USD 9.431	De Reservas	32%
Uruguay	10	286	29	USD 36.352	USD 356	USD 16.465	Rep Oriental de UY	45%
TOTAL	**552**	**82.660**	**150**	**USD 4.191.847**	**USD 53.172**			**24%**

Profits/Assets 1,27%

Note 1: The information in columns (A), (B), (D) and (E) was taken from https://indicadores.felaban.net/indicadores_homologados/index.php

Note 2: The information in column (F) was taken from www.americaeconomia.com/negocios-industrias/ranking-2017-conozca-los-250-mayores-Bancos-de-america-latina

Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

ANNEX 2

Table 23. Frequency of occurrence by type of digital security event against banking entities (part 1 of 2)

Social engineering

	Large	Medium	Small	**Total**
Daily	5	12	3	**20**
Monthly	6	11	4	**21**
Weekly	5	6	5	**16**
Quarterly	8	24	11	**43**
There is not	4	35	42	**81**

	Large	Medium	Small	**Total**
Daily	18%	14%	5%	**11%**
Monthly	21%	13%	6%	**12%**
Weekly	18%	7%	8%	**9%**
Quarterly	29%	27%	17%	**24%**
There is not	14%	40%	65%	**45%**

Malicious code or Malware

	Large	Medium	Small	**Total**
Daily	10	21	4	**35**
Monthly	6	19	5	**30**
Weekly	6	12	10	**28**
Quarterly	3	24	25	**52**
There is not	3	12	21	**36**

	Large	Medium	Small	**Total**
Daily	36%	24%	6%	**19%**
Monthly	21%	22%	8%	**17%**
Weekly	21%	14%	15%	**15%**
Quarterly	11%	27%	38%	**29%**
There is not	11%	14%	32%	**20%**

Spear Phishing to access bank systems

	Large	Medium	Small	**Total**
Daily	7	12	4	**23**
Monthly	1	15	6	**22**
Weekly	2	6	4	**12**
Quarterly	9	25	13	**47**
There is not	9	30	38	**77**

	Large	Medium	Small	**Total**
Daily	25%	14%	6%	**13%**
Monthly	4%	17%	9%	**12%**
Weekly	7%	7%	6%	**7%**
Quarterly	32%	28%	20%	**26%**
There is not	32%	34%	58%	**43%**

Data loss

	Large	Medium	Small	**Total**
Daily	1	1	1	**3**
Monthly	3	4	1	**8**
Weekly	2	2		**4**
Quarterly	5	21	3	**29**
There is not	17	60	60	**137**

	Large	Medium	Small	**Total**
Daily	4%	1%	2%	**2%**
Monthly	11%	5%	2%	**4%**
Weekly	7%	2%	0%	**2%**
Quarterly	18%	24%	5%	**16%**
There is not	61%	68%	92%	**76%**

Loss or theft of equipment or devices

	Large	Medium	Small	**Total**
Daily				**0**
Monthly	4	8	1	**13**
Weekly	4	1		**5**
Quarterly	9	36	12	**57**
There is not	11	43	52	**106**

	Large	Medium	Small	**Total**
Daily	0%	0%	0%	**0%**
Monthly	14%	9%	2%	**7%**
Weekly	14%	1%	0%	**3%**
Quarterly	32%	41%	18%	**31%**
There is not	39%	49%	80%	**59%**

Attack of denial of service (DoS / DDoS)

	Large	Medium	Small	**Total**
Daily	1	3	2	**6**
Monthly		10	3	**13**
Weekly	5	3	4	**12**
Quarterly	10	14	4	**28**
There is not	12	58	52	**122**

	Large	Medium	Small	**Total**
Daily	4%	3%	3%	**3%**
Monthly	0%	11%	5%	**7%**
Weekly	18%	3%	6%	**7%**
Quarterly	36%	16%	6%	**15%**
There is not	43%	66%	80%	**67%**

DNS theft

	Large	Medium	Small	**Total**
Daily		1		**1**
Monthly	2	3	1	**6**
Weekly		1	1	**2**
Quarterly	5	5	1	**11**
There is not	21	78	62	**161**

	Large	Medium	Small	**Total**
Daily	0%	1%	0%	**1%**
Monthly	7%	3%	2%	**3%**
Weekly	0%	1%	2%	**1%**
Quarterly	18%	6%	2%	**6%**
There is not	75%	89%	95%	**89%**

Table 24. Frequency of occurrence by type of digital security event against banking entities (part 2 of 2)

Violation of clear desk policies

	Large	Medium	Small	**Total**
Daily	4	11	3	**18**
Monthly	8	23	6	**37**
Weekly	6	7	2	**15**
Quarterly	6	20	18	**44**
There is not	4	27	36	**67**

	Large	Medium	Small	**Total**
Daily	14%	13%	5%	**10%**
Monthly	29%	26%	9%	**20%**
Weekly	21%	8%	3%	**8%**
Quarterly	21%	23%	28%	**24%**
There is not	14%	31%	55%	**37%**

Internal sabotage

	Large	Medium	Small	**Total**
Daily		1		**1**
Monthly	2	3		**5**
Weekly	2	1		**3**
Quarterly	4	10	6	**20**
There is not	20	73	59	**152**

	Large	Medium	Small	**Total**
Daily	0%	1%	0%	**1%**
Monthly	7%	3%	0%	**3%**
Weekly	7%	1%	0%	**2%**
Quarterly	14%	11%	9%	**11%**
There is not	71%	83%	91%	**84%**

Internal fraud

	Large	Medium	Small	**Total**
Daily		1		**1**
Monthly	10	7		**17**
Weekly	1			**1**
Quarterly	11	34	10	**55**
There is not	6	46	55	**107**

	Large	Medium	Small	**Total**
Daily	0%	1%	0%	**1%**
Monthly	36%	8%	0%	**9%**
Weekly	4%	0%	0%	**1%**
There is not	39%	39%	15%	**30%**
No hay	21%	52%	85%	**59%**

Defacement

	Large	Medium	Small	**Total**
Daily	1			**1**
Monthly		3		**3**
Weekly	1	1		**2**
Quarterly	5	3	2	**10**
There is not	21	81	63	**165**

	Large	Medium	Small	**Total**
Daily	4%	0%	0%	**1%**
Monthly	0%	3%	0%	**2%**
Weekly	4%	1%	0%	**1%**
Quarterly	18%	3%	3%	**6%**
There is not	75%	92%	97%	**91%**

Backdoor (code developed to enable subsequent access)

	Large	Medium	Small	**Total**
Daily	1		1	**2**
Monthly	3	5		**8**
Weekly	1		1	**2**
Quarterly	9	11	2	**22**
There is not	14	72	61	**147**

	Large	Medium	Small	**Total**
Daily	4%	0%	2%	**1%**
Monthly	11%	6%	0%	**4%**
Weekly	4%	0%	2%	**1%**
Quarterly	32%	13%	3%	**12%**
There is not	50%	82%	94%	**81%**

SQL Injection

	Large	Medium	Small	**Total**
Daily	4	3	2	**9**
Monthly	1	9		**10**
Weekly	4	3	3	**10**
Quarterly	9	18	6	**33**
There is not	10	55	54	**119**

	Large	Medium	Small	**Total**
Daily	14%	3%	3%	**5%**
Monthly	4%	10%	0%	**6%**
Weekly	14%	3%	5%	**6%**
Quarterly	32%	20%	9%	**18%**
There is not	36%	63%	83%	**66%**

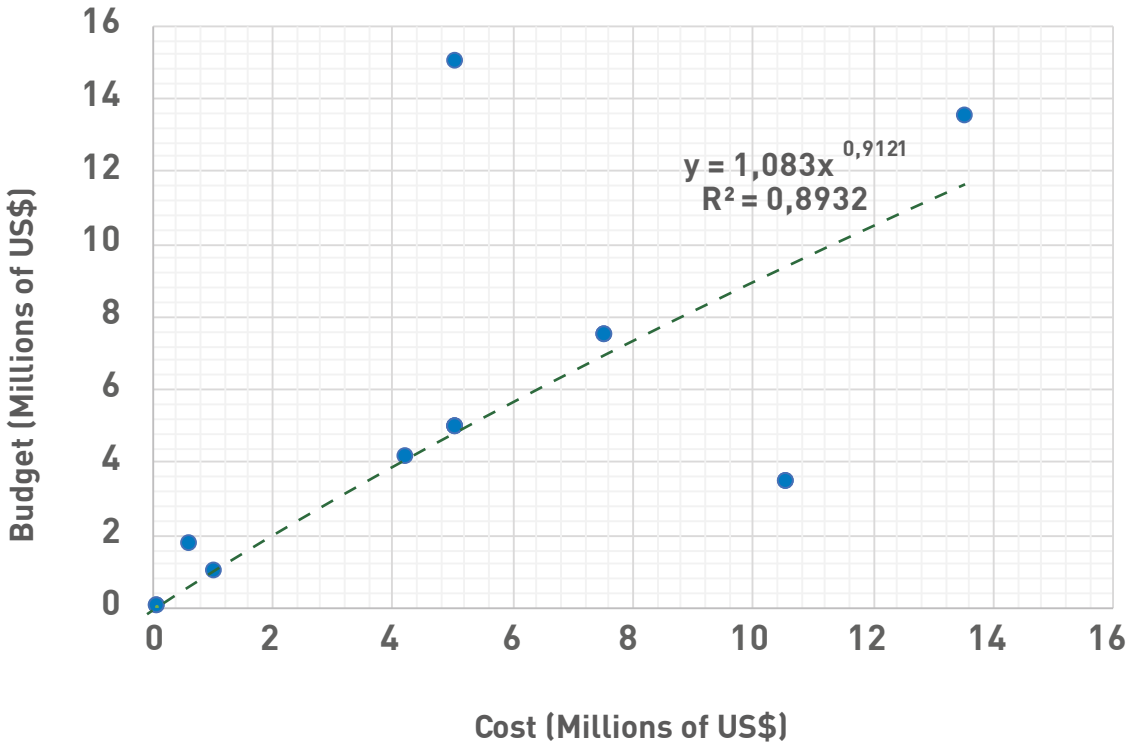
Brute force attack

	Large	Medium	Small	**Total**
Daily	4	1	3	**8**
Monthly	1	8	1	**10**
Weekly	4	2	1	**7**
Quarterly	6	18	7	**31**
There is not	13	59	53	**125**

	Large	Medium	Small	**Total**
Daily	14%	1%	5%	**4%**
Monthly	4%	9%	2%	**6%**
Weekly	14%	2%	2%	**4%**
Quarterly	21%	20%	11%	**17%**
There is not	46%	67%	82%	**69%**

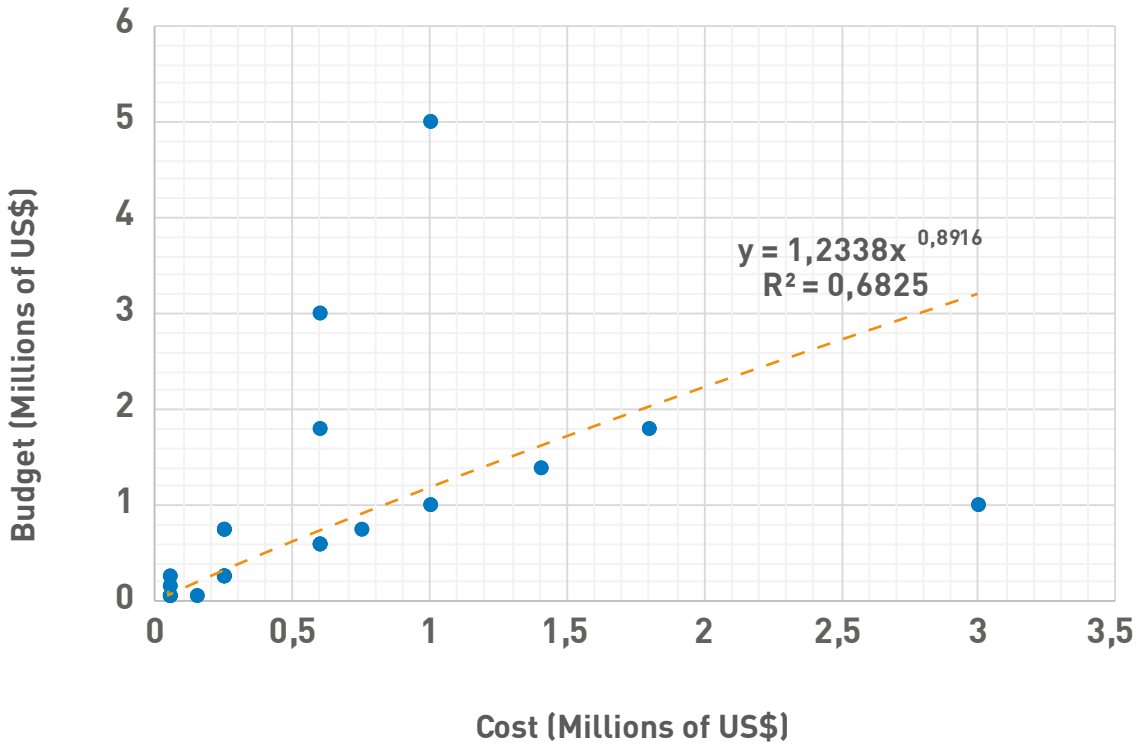
ANNEX 3

Graph 61. Relationship between the Budget for Digital Security and the Total Cost of Response and Recovery in the Event of Security Incidents for Large Banks in Latin America and the Caribbean



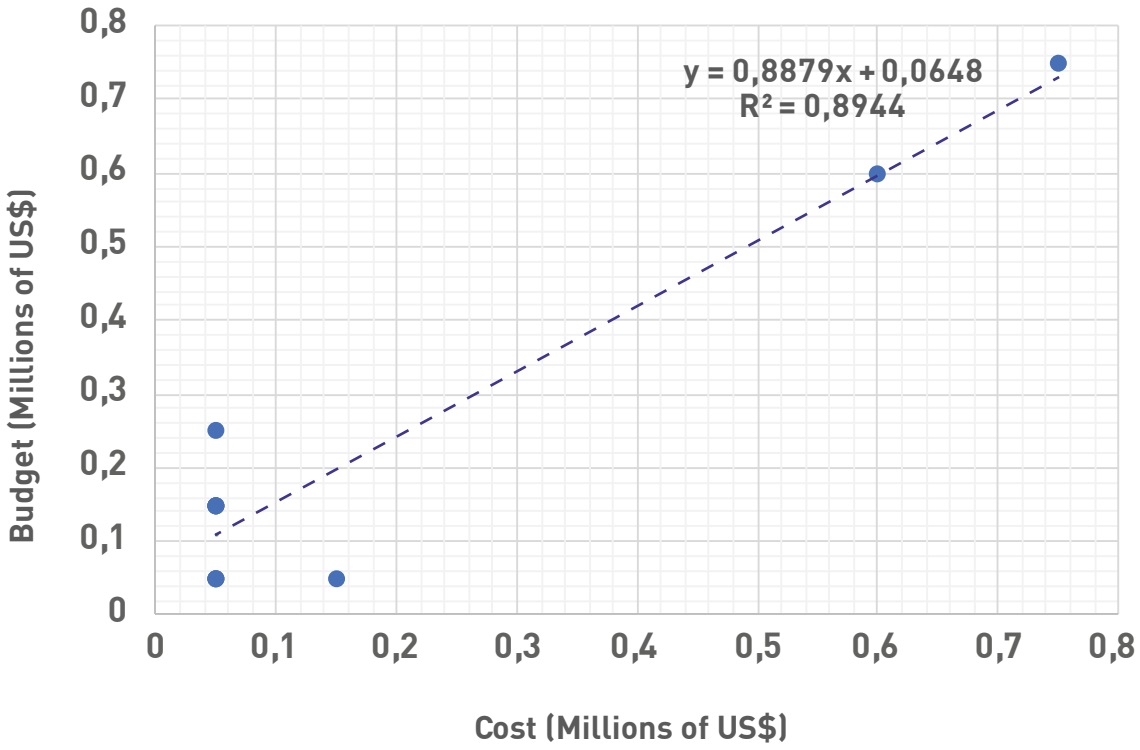
Note: 14 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Graph 62. Relationship between the Budget for Digital Security and the Total Cost of Response and Recovery in the Event of Security Incidents for Medium Banks in Latin America and the Caribbean



Note: 21 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Graph 63. Relationship between the Budget for Digital Security and the Total Cost of Response and Recovery in the Event of Security Incidents for Small Banks in Latin America and the Caribbean



Note: 11 records
Source: GS/OAS based on information collected from banking entities in Latin America and the Caribbean

Reference notes

1. Participating banks have a total of assets close to US$1 trillion and accumulate net profits of US$10.5 billion (as of December 31, 2017) and according to their size are distributed as follows: 35% Small Banks, 48% Mediums Banks and 17% Larges Banks; according to their composition they are: 79% Private Banks, 13% Public Banks and 8% Mixed Banks

2. Participating users reported being 72.44% male, 27.42% female and 0.14% "not defined". Regarding the age range of the users interviewed, 33.66% are between 35 and 44 years old, 33.52% between 25 and 34 years old, 20.08% between 45 and 54 years old, 6.23% between 55 and 64 years old, 5.40% between 18 and 24 years old and only 1.1% are over 65 years of age.

3. Users can be more aware that they are being affected by an attack with solutions such as alerts provided by security suites (as a result of real-time protection), as well as notifications of access to virtual platforms or notifications by transactions or operations that can be scheduled with the bank.

4. See FIN7 Arrest paper. Use of "legitimate" Israeli and Ukrainian companies for funnelling of funds.

5. Federal Bureau of Investigation of EE. UU (FBI), "Three members of notorious international Cybercrime Group "Fin7" in custody for role in attacking over 100 U.S. Companies", August 1, 2018
www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

6. Federal Bureau of Investigation of EE. UU (FBI), "Three members of notorious international Cybercrime Group "Fin7" in custody for role in attacking over 100 U.S. Companies", August 1, 2018
www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

7. Bloomberg: "Mexico foiled a US$110 million Bank Heist, Then Kept it Secret", August 29, 2018
www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret

8. Reuters: "Bank of Chile trading down after hackers rob millions in cyberattack" 11 June 2018:
www.reuters.com/article/us-chile-banks-cyberattack/bank-of-chile-trading-down-after-hackers-rob-millions-in-cyberattack-idUSKBN1J72FC

9. See Zingbox "Meet Piolin, the first ATM Malware Jackpotting ATMs in US
www.zingbox.com/wp-content/uploads/2018/03/Meet-Piolin.pdf w8 February 2018

10. CyberScoop, "North Korea to blame for string of Latin American bank hacks, insiders say", 18 June 2018
www.cyberscoop.com/north-korea-swift-hacks-bancomext-bank-of-chile/

11. See Group-IB "Moneytaker: in pursuit of the invisible" and "Moneytaker: 1.5 years of silent operations," both dated December 11, 2017: www.group-ib.com/blog/moneytaker

12. Bloomberg, "Mexico tells banks to take steps to Guard against suspected hacks" 30 April 2018
www.bloomberg.com/news/articles/2018-04-30/banorte-is-said-to-be-among-mexican-banks-targeted-by-hackers

13. https://m.theepochtimes.com/exclusive-chinese-state-hackers-started-cyber-bank-robberies_2085775.html

14. www.fsisac.com/

15. www.europol.europa.eu/es/about-europol

16. www.nomoreransom.org/es/index.html

17. The Cyber Defense Alliance of the United Kingdom (UK Cyber Defense Alliance) does not have a public website. You can find a description of the structure, location and objectives of the organization in Financial Times, "Banks join forces to crack down on fraudsters". August 9, 2017
www.ft.com/content/6c9030ca-7937-11e7-90c0-90a9d1bc9691

18. The Global Risks Report, World Economic Forum, published on January 17, 2018

19. Georges Bataille

20. www.fatf-gafi.org/recommendations

21. www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

22. www.fatf-gafi.org/publications/fatfgeneral/documents/universal-procedures.html

23. www.fatf-gafi.org/publications/mutualevaluations/documents/more-about-mutual-evaluations.html

24. World Economic Forum.(2018). Thee Global Risks Report 2018, 13th Edition. Ginebra, Suiza: World Economic Forum.

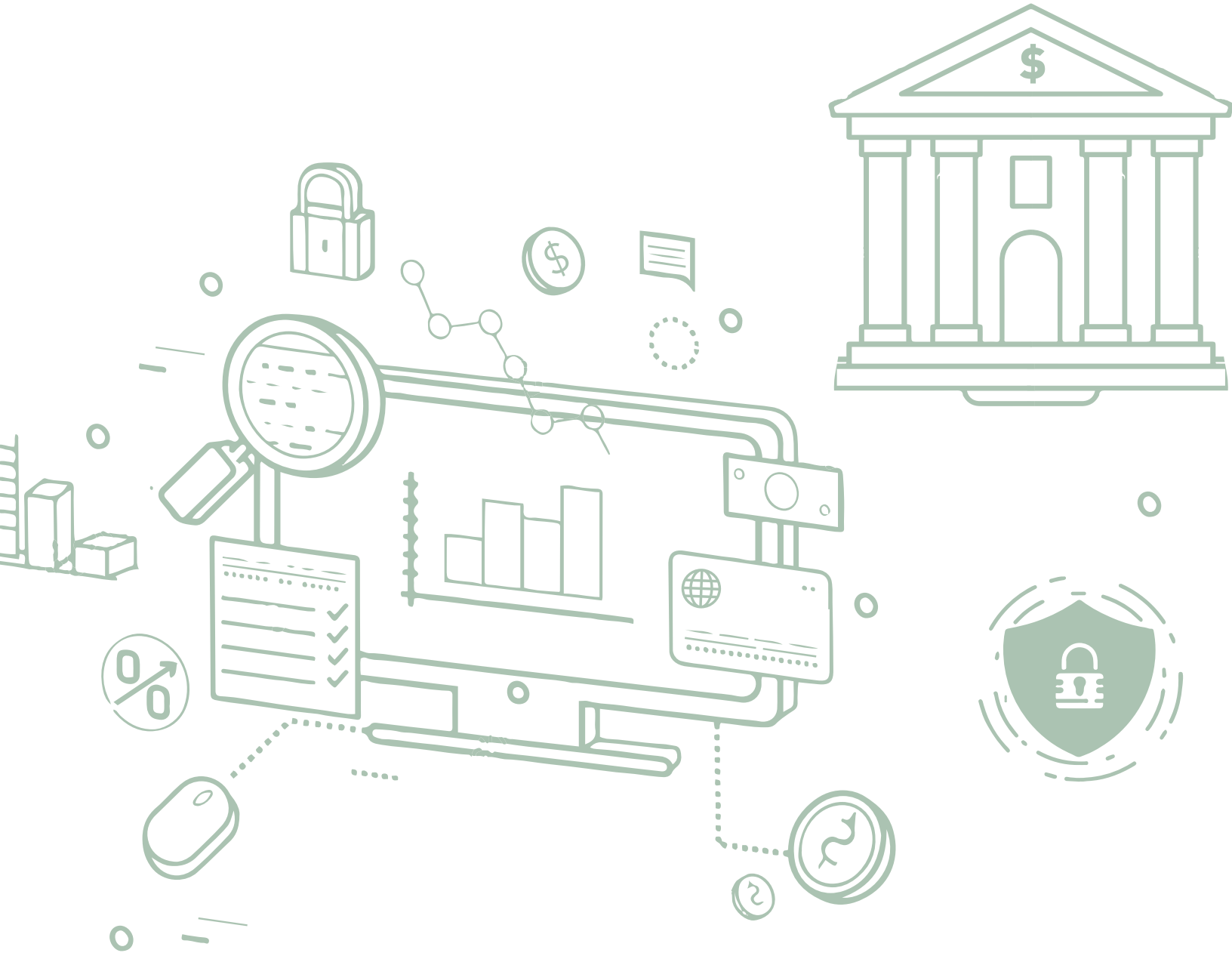
25. Wright, A., Kellman, B., & Kallicharan, S. (2018). CBR Withdrawals:Understanding the Uneven Occurence Across the Caribbean. Washington: Inter-American Development Bank.

26. Inter-American Development Bank (2018, June 29). What will the Caribbean's financial sector of the future look like? Retrieved from the Inter-American Development Bank
https://blogs.iadb.org/caribbean-dev-trends/2018/06/29/8736/

27. Ernst and Young. (2016). CAACM: Cybersecurity Risks: Is your Organization Prepared. Trinidad and Tobago: Ernst and Young.
PricewaterhouseCoopers LLP. (2014). Threat Smart: Building a Cyber resilient financial institution. Delaware: PricewaterhouseCoopers LLP.

28. The concept of cybernetic resilience is defined as the degree of capacity that an organization has to feel (predict and detect), resist and react to threats of a cybernetic nature.

29. These types of solutions include resources such as: i) transactional protection software on the Internet, which is offered for download from the bank's website in order to prevent fraud threats through modalities such as Malware, Phishing and Pharming, and ii) Identity protection mechanisms in applications that offer improved systems for authentication, as well as the recognition of frequently used devices, specifically aimed at preventing threats of fraud through Phishing, among others.



OAS | More rights for more people

State of **Cybersecurity** in the **Banking Sector** in **Latin America** and the **Caribbean**