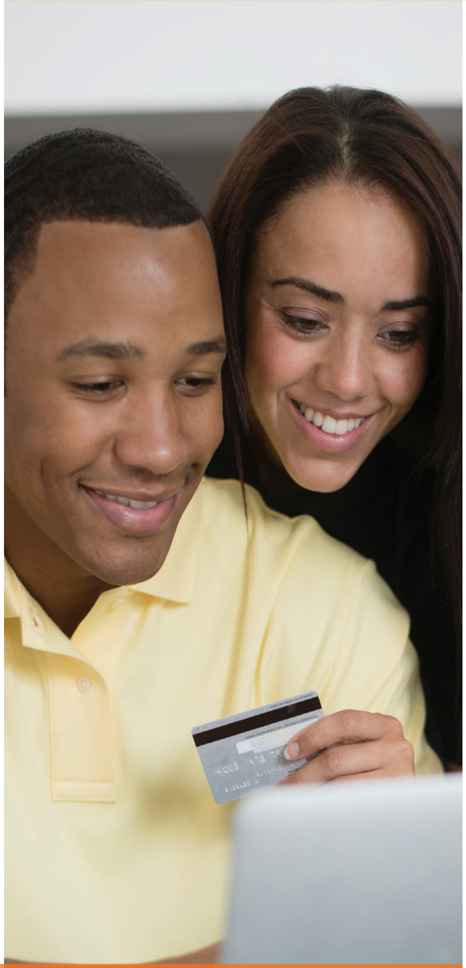
UNISYS | Securing Your Tomorrow®

IN FINANCIAL SERVICES, CUSTOMER SECURITY CONCERNS CHANGE AND INTENSIFY

By Jorge Andrés Gómez



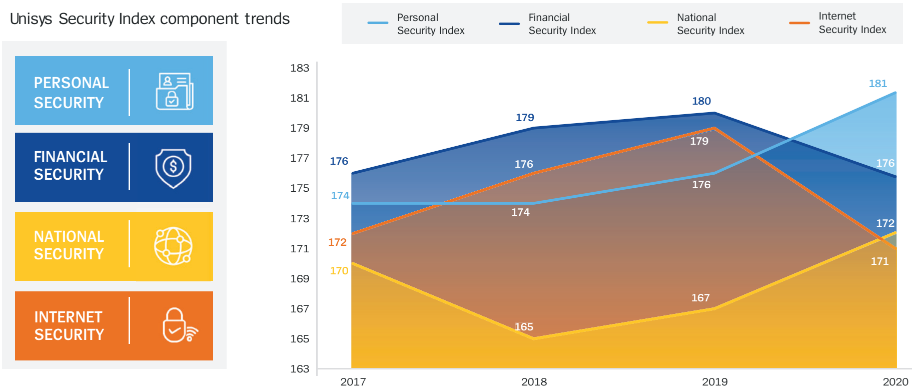
CONSUMERS ARE MORE CONCERNED ABOUT THEIR PERSONAL SECURITY AND NATIONAL SECURITY, BUT ARE LESS CONCERNED ABOUT INTERNET SECURITY.

"Worries about COVID-19 significantly diminished consumer concern about internet security – just when internet transactions came under heavy attack. This creates a timely opportunity – and obligation – for financial institutions to respond to this shift by providing consumers with targeted, relevant protective measures that compensate for their customers' diminished concern and continue to earn consumer trust."

Every year, financial institutions look to the Unisys Security Index™ (USI) for insights into consumers' concerns about security – personal, financial, national, and internet security.

This year, it is not an exaggeration to say that they will find some confronting trends. Consumers are *more* concerned about their personal security and national security – not surprising, since the survey was conducted during the COVID-19 pandemic. But, perhaps suggesting that humans can only be terrified by one thing at a time, consumers *are less concerned* about internet security. Specifically, from the USI 2020 global report:

> *While 2019 saw a slight increase across all security areas, the 2020 Unisys Security Index shows a distinct change in consumers' gaze. Looking away from Internet Security (7-point decrease) and Financial Security (4-point decrease) compared to previous years, they are diverting their attention to National Security (5-point increase) and Personal Security (5-point increase).*



Unisys Security Index component trends

The 2020 Unisys Security Index surveyed more than 15,000 consumers in 15 countries, gauging attitudes on a range of security-related issues within the categories of national, financial, internet and personal security.

On a scale of zero to 300, with 300 representing the highest level of concern, the global index is now at 175, considered a serious level of concern and tied for the highest level in the 14 years the study has been conducted.

The World Health Organization reported a five-fold increase in cyberattacks; the FBI reported that the Internet Crime Complaint Center (IC3) saw an increase in reports of online extortion scams. In a particularly insidious scheme, criminals spoofed people and businesses that suffered losses during the lockdowns, offering to help them get government funds, but instead led the innocents to a page that would capture their banking credentials. With people working from home with little preparation and probably less secure home networks, they were positioned to be hacked and/or duped more easily.

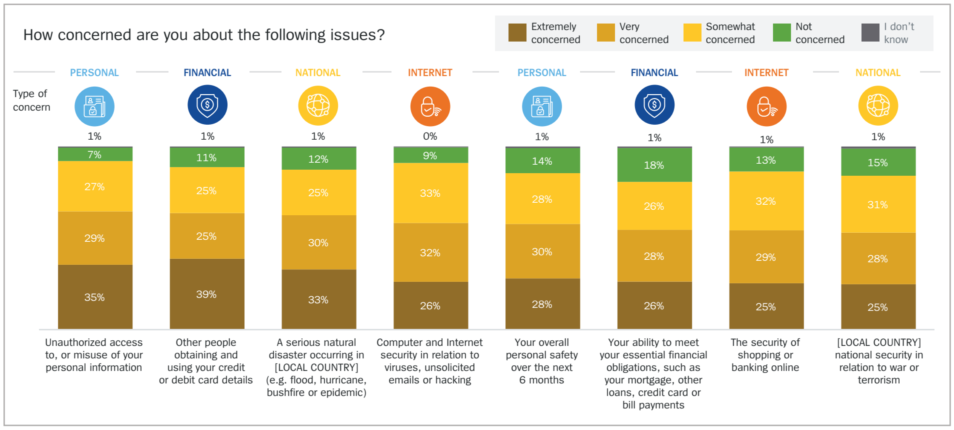
As for banks, which, along with healthcare account for almost a third of cyberattacks, in a report blaming the pandemic for a 238% surge in cyberattacks against banks, Zero Day explained, " ...Alongside a spike in attacks, techniques also appear to be improving - including the use of social engineering and more advanced tactics to exploit not only the human factor but also weak links caused by processes and technologies... "

So, given the surge in attacks and the new vulnerability of customers coupled with their reduced concern, how can banks better protect their customers throughout this period and beyond?

IDENTIFY THEFT AND BANKCARD FRAUD ARE THE TWO MOST PRESSING CONCERNS WORLDWIDE.

Increase Digital Transfers – Only the Bank Sees Sensitive Information

The USI found that identify theft and bankcard fraud are the two most pressing concerns worldwide, despite dropping from 2019 levels. Concern around Identity Theft dropped by four percentage points since 2019 but continues to rank at the top of the eight security concerns measured by the index.



With consumers quarantined at home and insisting on no- or low-contact interactions, not surprisingly there was a massive increase in card-not-present financial transactions. It was not unusual for a consumer to place a telephone order with a restaurant, paint store, or pharmacy, give their credit card number and security code, take delivery of the order, but without signing for it or even getting a receipt – one less thing to touch. For a highly trusted merchant, that was reasonably safe, and conscientious consumers might also have reset their credit card alerts to immediately notify them of *all* card-not-present transactions.

But under the circumstances, with threats so high and consumers less vigilant, the safest process for no-contact transactions, where the provider on the other side of the transaction is unknown to the consumer, would be a digital transfer conducted through the consumer's bank. Instead of the consumer giving the merchant all their sensitive information, the customer takes the merchant's bank name, routing number and account number. Zero contact involved, and the customer's information entirely contained at his trusted bank rather than the merchant or the merchant's employees. In developing countries at least, consumers trust banks to keep their information safe, where those banks have invested in sophisticated security measures like those provided by Unisys: biometric multi-factor authentication, data analytics, instant detection of intruders, dynamic isolation, encrypted microsegmentation and more – all built on a foundation of resilience and Zero Trust.

Who knows if consumers will become concerned again about internet security, after they can relax about COVID-related matters? They may not, but by familiarizing customers to this ultra-safe practice during worrisome times, banks can accustom them to making it a habit when potentially safer times return.

Regulators and banks alike are adding more and more security mechanisms that prevent identity theft and bank card fraud on both digital and physical channels. This has evolved as technology solutions become more accessible, reliable, and easy to use for customers and banks.

IN DEVELOPING COUNTRIES, THE 2020 USI RECORDED HEIGHTENED SECURITY CONCERN OVERALL.

Intensify Protection of Personal Security in Developing Countries

Clearly, security concerns are different around the globe, and in developing countries, the 2020 USI recorded heightened security concern overall:

> *The biggest increases in concern are in Latin America, where Chile's index score increased by 6 points and Brazil's by 7 points... Asia Pacific countries also saw an increase over 2019's index. The Philippines maintains its position as the most concerned country, increasing its score by 4 points. India and Singapore enter in second and sixth place, respectively. The Philippines and India are... the most concerned about Personal Security, with a score of 251 in the Philippines and 226 in India.*

Much of this rise can be attributed to concerns about personal security, including personal safety and identity theft (the top concern of all security areas measured).

Consumers in these countries have good reason for their concerns. In February 2020, Security Week attributed rising cybercrime in Latin America to "a high use of the internet among a huge population with a low awareness of cybersecurity awareness... compounded by little government security regulation forcing companies to improve their own security, and...bribery and corruption within law enforcement and government agencies." A similar environment exists in many South Asian countries. The same article also identified "a darker side to the Latin American hacking scene. Drug cartels are beginning to recruit the more sophisticated hackers to help with money laundering, ATM thefts, and breaking into bank networks."

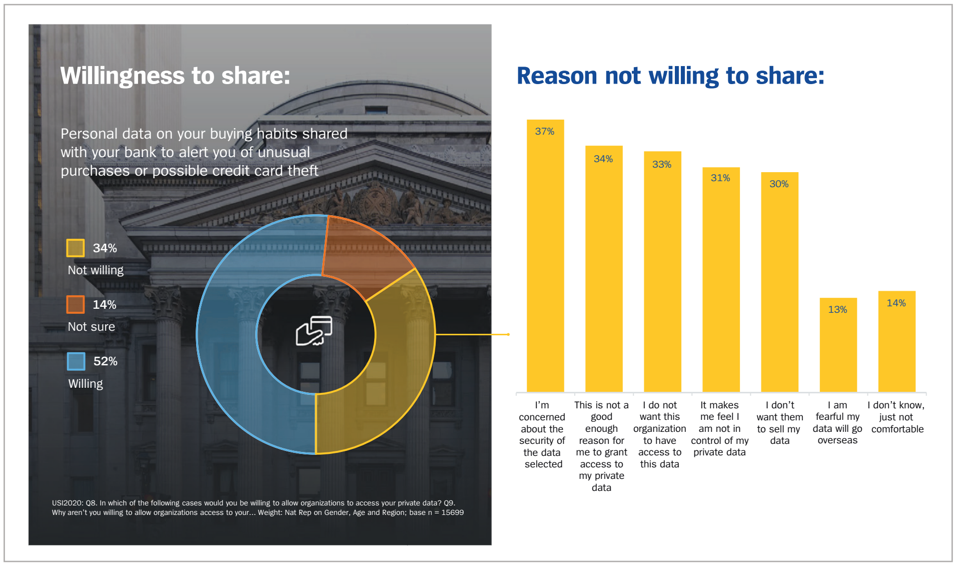
Banks in these developing countries have been increasing their security investments, but many still lag the developing world. They can start with working together on campaigns with the specific goal of reinvigorating consumers' concerns about internet security – in part by making the direct connection between personal and internet security – it's not an either/or – it's both.

In addition, banks can also take advantage of increasingly effective technology solutions like biometrics, credential management, restricted access, network monitoring, and rapid isolation of intruders.

REGULATORS WORLDWIDE ARE PROMOTING, AND IN SOME CASES MANDATING BIOMETRIC AUTHENTICATION FOR ONBOARDING, CUSTOMER IDENTIFICATION AND MOBILE ACCESS.

Recognize the Time Is Ripe for Exploiting the Power of Biometrics

Security concerns morph over time; the USI 2020 and the banking industry's growing acceptance of cloud computing after years of resistance on security grounds are good examples. Slightly more than half of consumers are willing to share personal data with their banks so that banks can in turn employ biometrics to better protect customers.



USI2020: Q8. In which of the following cases would you be willing to allow organizations to access your private data? Q9. Why aren't you willing to allow organizations access to your... Weight: Nat Rep on Gender, Age and Region; base n = 15699

That level of willingness can be expected to increase as consumers become more accustomed to the resulting convenience. They are wearying of the burden of creating, storing, remembering, changing, and remembering again all their usernames, passwords, and answers to security questions. Then there is the challenge problem of keeping all that sensitive information easily accessible for their purposes but still secret from everybody else. And finally, there's the inescapable fact that when consumers must use insecure online connections, they are leery of entering their credentials and having them stolen.

Consumers' readiness for biometrics is also spurred by COVID-19 which drove out other security concerns while elevating consumers' preference for no- low-contact interactions – and by sheer familiarity. What sounded la-la a few years ago – fingerprint phone unlocking, facial recognition at customs and on social media sites, speech recognition – is now utterly ordinary to many consumers, thanks to steady exposure without incident. And as is the habit with consumers, acceptance quickly becomes expectation becomes demand – they now want the same ease of use in all their online interactions. To reduce identity theft, regulators worldwide are promoting, and in some cases mandating biometric authentication for onboarding, customer identification in branches and mobile access for reducing identity theft cases.

Banks have long been ready with rudimentary biometric offerings, but the technology has advanced considerably, thanks to data analytics and artificial intelligence. Banks that can quickly incorporate more advanced offerings such as telephone voice authentication, real-time facial recognition for ATM authentication and digital onboarding will be best able to compete against their often nimbler fintech competitors.

Of course, getting customers to provide more personal information comes with the added obligation for banks to employ advanced security measures of their own like those named above.

Unisys serves more than 380 financial institutions around the world with Omnichannel Banking Solutions, Digital Workplace, Cloud and Infrastructure Services and award-winning Security Solutions and Services that help banks to modernize their operation, protect their data, and improve the customer experience.

GETTING CUSTOMERS TO PROVIDE MORE PERSONAL INFORMATION COMES WITH THE ADDED OBLIGATION FOR BANKS TO EMPLOY ADVANCED SECURITY MEASURES.

Jorge Andrés Gómez is the Industry Director for Financial Services at Unisys.

He can be reached at Jorge.gomez@co.unisys.com or connect with him at LinkedIn.

To learn more about financial services, visit www.unisys.com/industries/financial-services

For more information visit www.unisys.com