2018 UNISYS SECURITY INDEX™ REVEALS HOW TO KEEP BANK CUSTOMERS' TRUST

UNISYS | Securing Your Tomorrow®

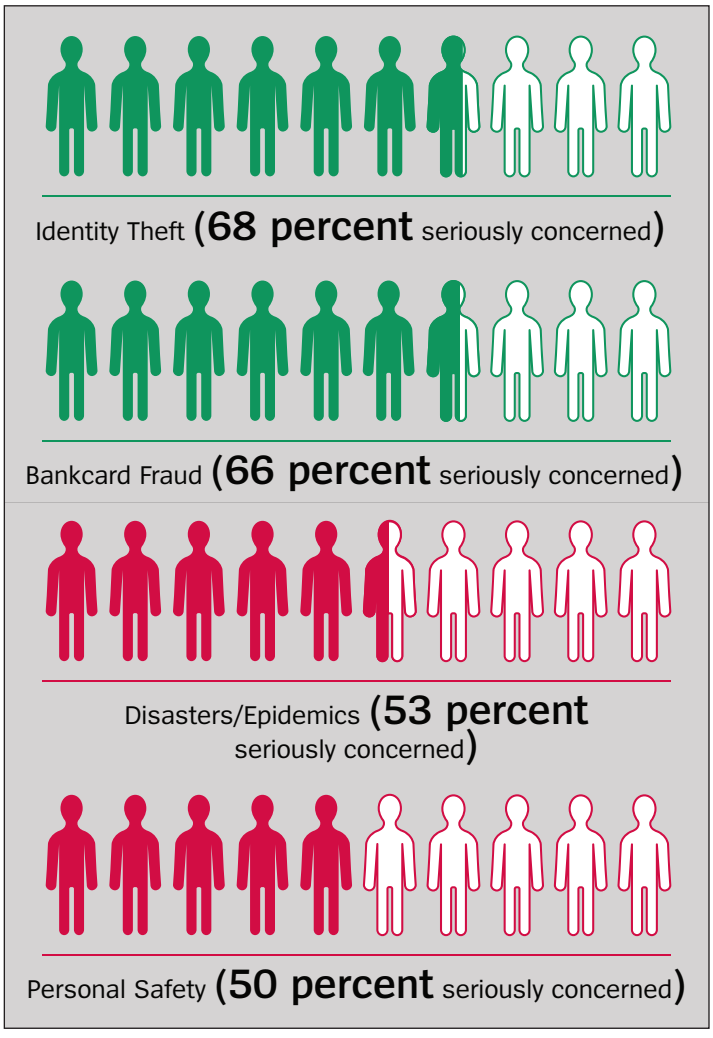
Security Concerns Are High Among Consumers Worldwide

Customer trust is critical in the financial services industry; the loss of trust can dramatically impact business. To sustain trust, banks and financial services institutions have to protect themselves and their customers' information against persistent and increasingly sophisticated threats.

Today's consumer is highly aware of and concerned about these threats. The Unisys Security Index™, the only recurring snapshot of security concerns conducted globally, gauges the attitudes of consumers on a wide range of security-related issues. In 2018, Unisys surveyed more than 13,000 consumers in 13 countries to generate the data for this report. Results showed that security concerns globally among individuals continue to hold at the highest level ever since 2007, as measured by the Unisys Security Index.

To provide the customer experience that consumers expect and demand, banks and financial services institutions must understand where and why security concerns exist and take steps to proactively address and alleviate risk from Day One.

Identity Theft and Bankcard Fraud Top the List of Consumer Fears



Among consumers, the highest security concerns are those where people feel they may have the least amount of personal control: Identity Theft and Bankcard Fraud. Globally, people surveyed are more concerned about Identity Theft (68 percent seriously concerned) or Bankcard Fraud (66 percent seriously concerned) than they are about possible physical harm related to Disasters/Epidemics (53 percent seriously concerned) or Personal Safety (50 percent seriously concerned).

Consumers have a right to be concerned. There has been a steady drumbeat of news around data breaches involving the personal and financial data of millions of consumers. By October of 2018, the number of compromised personal data records for the year had already surpassed the total number of breached records for all of 2017. This included Facebook's disclosure of 87 million records breached, Exactis' report of 340 million records breached, and Starwood's admission of 500 million records breached.

The good news is that banks and financial institutions have not been named among the top breaches of 2018. This distinction is due to the fact that the industry is on the leading edge of security compared to other commercial verticals. However, this does not mean that banks and financial institutions can afford to relax their guard. Hackers are getting more and more sophisticated, and security measures must keep pace.

In particular, banks and financial institutions need to concentrate on their authentication procedures, since this is a key juncture where identity theft and bankcard fraud occur. They must have the right processes, checks, systems, and tools in place to guarantee that when a customer signs into an account, the person is who they say they are.

Additionally, banks and financial institutions need to secure data as it moves between systems across multiple companies. The socioeconomic environment is shifting to require the sharing of data between financial institutions and organizations that may not be regulated as rigorously as their financial counterparts. This increases risk and exposure, creating the opportunity for data breaches to occur.

Consumers Want Data Privacy and Customer Convenience

Data privacy concerns appear prominently in the Unisys Security Index this year as well. For example, nearly two-thirds (64 percent) of Argentinians surveyed reported that they do not trust the organizations that store their data in the cloud to protect it. In Brazil, only nine percent of respondents say they are highly confident that the country's new General Data Protection law will be effective. In the Netherlands, only a third (34 percent) believe their privacy is sufficiently protected within the new 'De Sleepwet' law.

In light of these concerns, banks and financial institutions need to demonstrate to their customers that they can uphold the swiftly-evolving data privacy regulations being put in place worldwide without compromising the customer experience. That is, customers want to be able to transact their financial business anytime, anywhere, and on any device. They also want the convenience of institutions being able to share data safely. For example, if Fidelity manages their investment portfolio, they expect that the security standards, protocols, and tools will be in place to allow Fidelity to pull in their data from a JP Morgan bank account or a Bank of America mortgage account.

Meeting the dual – and sometimes competing – goals of protecting data privacy while also providing a great customer experience is a definite challenge. However, it is a challenge that banks and financial institutions must meet if they are to continue to grow and thrive in today's marketplace.

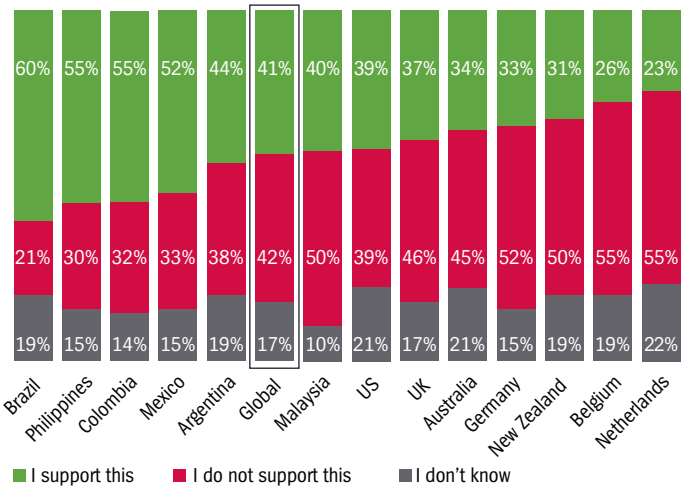
Data Security Is a Concern with Connected Devices

Connected devices are multiplying exponentially in every industry, bringing both opportunity and risk. The Unisys Security Index noted that consumers largely support the use of connected devices globally. However, data security has become a rising concern, forcing many to rethink the wisdom of sharing information among these devices.

Relevant to banks and financial institutions, the Unisys Security Index reported that 41 percent of respondents would support an application on their smartwatch from their bank or credit card company that would allow them to make payments from their watch (up from 36 percent in 2017). However, an almost identical proportion of respondents (42 percent) said they would not support such an application. Support tended to be higher in less-developed nations compared to more developed nations.

Low support for payments from watch apps in developed nations

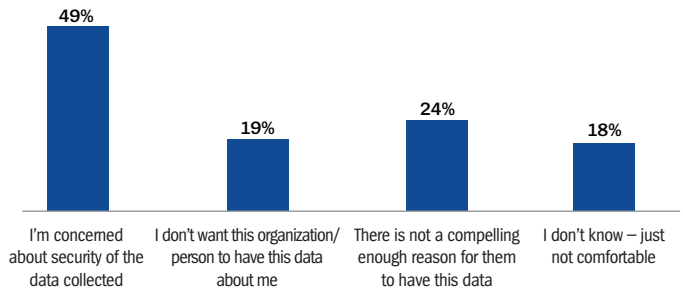
An app on your smartwatch from your bank or credit card company to make payments from your watch



Of those respondents who would not support such an application on their smartwatch, the top concern they had was regarding the security of the data collected (49 percent).

When money is involved data security is the highest cocern

Why don't you support having an app on your smartwatch from your bank or credit card company to make payments from your watch?



There is potential for biometrics to enhance the perceived safety of such transactions. In Argentina, there has been a concerted effort by the government to implement regulations around data privacy and security. As a result, nearly two-thirds (63 percent) of Argentinian consumers have confidence that their government authorities will develop a set of regulations to enhance the security of biometric technology.

Authentication, of course, is the key when considering connected devices. There are two aspects to this authentication. First, there is the hardware: the smartphone, smartwatch, or other device the consumer is using to connect to their bank or financial institution. Many of these devices today have authentication protocols that protect the device – often biometric in nature.

Second, there is the application itself. Currently, there does not tend to be a second level of authentication at the application level, unless an especially large or complex transaction is requested. If that is the case, the customer is usually routed to a company representative who requests an in-person meeting to complete the matter.

However, given today's trends, more and more consumers are going to be using their devices to do greater numbers of large-scale and complex transactions – such as opening a mortgage or transferring significant sums of money. Banks and financial institutions need to consider providing an extra level of security within their applications to protect their customers, such as requiring authentication by voice or some other mechanism at the application level. All this must be done while providing a great and secure customer experience, which is central to maintaining a competitive advantage.

Cybersecurity Ranks as the Third Greatest Global Security Concern

Internet attacks are specifically called out in the results of the Unisys Security Index. The threat of viruses and hacking was reported as the third greatest global security concern in 2018, with 62 percent of respondents reporting that they are seriously concerned. Indeed, seven out of thirteen countries have increased levels of concern about Viruses/Hacking since the 2017 index.

It is important to recognize that it is impossible to be 100 percent impervious to getting hacked. Instead, it is helpful to take the approach of "how can an attack be contained and damage limited?" Banks and financial institutions need to take steps to prevent hackers from taking control of the entire system, or from moving across the network horizontally. By compartmentalizing the network (e.g., through microsegmentation), attacks can be contained and the impact mitigated.

Take Action Today

Banks and financial institutions are facing a dynamic threat landscape that calls for risk-relevant security solutions. These solutions cannot interfere with efficient business operations or negatively impact the consumer experience. As an industry leader in security for the financial services industry, Unisys recommends the following action items to secure systems and promote customer trust:

1. **Pay attention to security basics.**
   With cyber threats growing around the world, banks and financial institutions may be tempted to immediately adopt the latest and greatest technology – without first covering the basic precautions that are foundational to any successful strategy. While the latest security innovations can be important tools for addressing cyber challenges, they will not help if organizations fail to address commonsense security practices such as password protection.

2. **Get a professional cybersecurity assessment.**
   Before security can be strengthened, it is necessary to know exactly where risks and vulnerabilities lie. Detailed risk assessments enable banks and financial institutions to determine the likelihood and success of different attacks against the existing technology infrastructure and data assets. This insight can then be used to prioritize security spend based on potential business impact, maximizing the return on investments and protecting what is most valuable to the organization's long-term success. One particular area of concern for banks and financial institutions is that of open APIs. With the move to digital and open banking, it is critical to ensure that all such connections are well protected.

3. **Approach security with the customer in mind.**
   To build trust among customers, banks and financial institutions must communicate the steps they are taking to safeguard their customers' personal information, and educate customers on steps they themselves should take to bolster security. For example, banks can create awareness programs to teach vulnerable customers (such as the elderly) about phishing scams or how to verify if a website provides for secure transactions. Constantly reinforcing security messages at physical branches, on websites, and within messaging centers is one of the greatest services banks and financial institutions can provide for their customers.

4. **Adopt a zero-trust security model.**
   A zero-trust approach to security means that internal network traffic is not trusted as legitimate, nor are employees and partners trusted to always be well-meaning and careful with systems and data. Research conducted by Forrester Consulting in 2018 and sponsored by Unisys found that 58 percent of respondents agreed that network perimeters are indefensible in today's technology ecosystem of distributed cloud workloads and mobile/remote users. Consequently, Unisys recommends embracing a zero-trust approach that is identity- and data-centric, based on network segmentation, data obfuscation, security analytics, and automation.

5. **Collaborate with the financial community to address common challenges.**
   A complex network of business relationships exists within the financial community. It benefits every member of that community to work together on matters common to all. For example, if a certain type of fraud is perpetrated on Barclays, it is almost guaranteed that the fraud will subsequently strike HSBC and Lloyds. It will then jump across country lines to infect banks worldwide. However, by cooperating with each other as well as with governmental and policing organizations to share information, set standards, and address challenges, banks and financial institutions can present a united and secure front to hackers.

6. **Evolve continually to ensure ongoing robust security.**
   The biggest threat to banks and financial institutions is complacency. In order to grow and scale – which always involves delivering better products and services while eliminating security threats and lowering risk – banks must engage in constant vigilance. Security requires continually re-evaluating and modifying processes, devices, risk frameworks, and tools. Know Your Customer (KYC) initiatives are an important part of this process. Whereas the industry has historically performed KYC initiatives on an annual basis, increasing regulatory scrutiny and fraud risk is influencing many institutions to increase the frequency to quarterly.

About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most demanding businesses and governments on Earth. Unisys offerings include security software and services, digital transformation and workplace services, industry applications and services, and innovative software operating environments for high-intensity enterprise computing. For more information on how Unisys builds better outcomes securely for its clients across the Government, Financial Services and Commercial markets, visit www.unisys.com.

For more information on Unisys security offerings, visit: www.unisys.com/security

For more information visit www.unisys.com

Printed in the United States of America 02/19 19-0039