STRENGTHENING SECURITY WITHOUT COMPROMISING THE PASSENGER EXPERIENCE:

A REVIEW OF THE 2018 UNISYS SECURITY INDEX™

UNISYS | Securing Your Tomorrow®

Security Concerns Are High Among Consumers Worldwide

Security issues are rampant throughout the travel and transportation industry, and are especially troubling for airports and airlines. As passengers and cargo move within and between countries, there are a multitude of opportunities for identity theft, bankcard fraud, data privacy breaches, cyberattacks, and other threats.

Today's consumer is highly aware of and concerned about all these risks. 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, airports and airlines must understand where and why security concerns exist and take steps to proactively address and alleviate risk.

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).

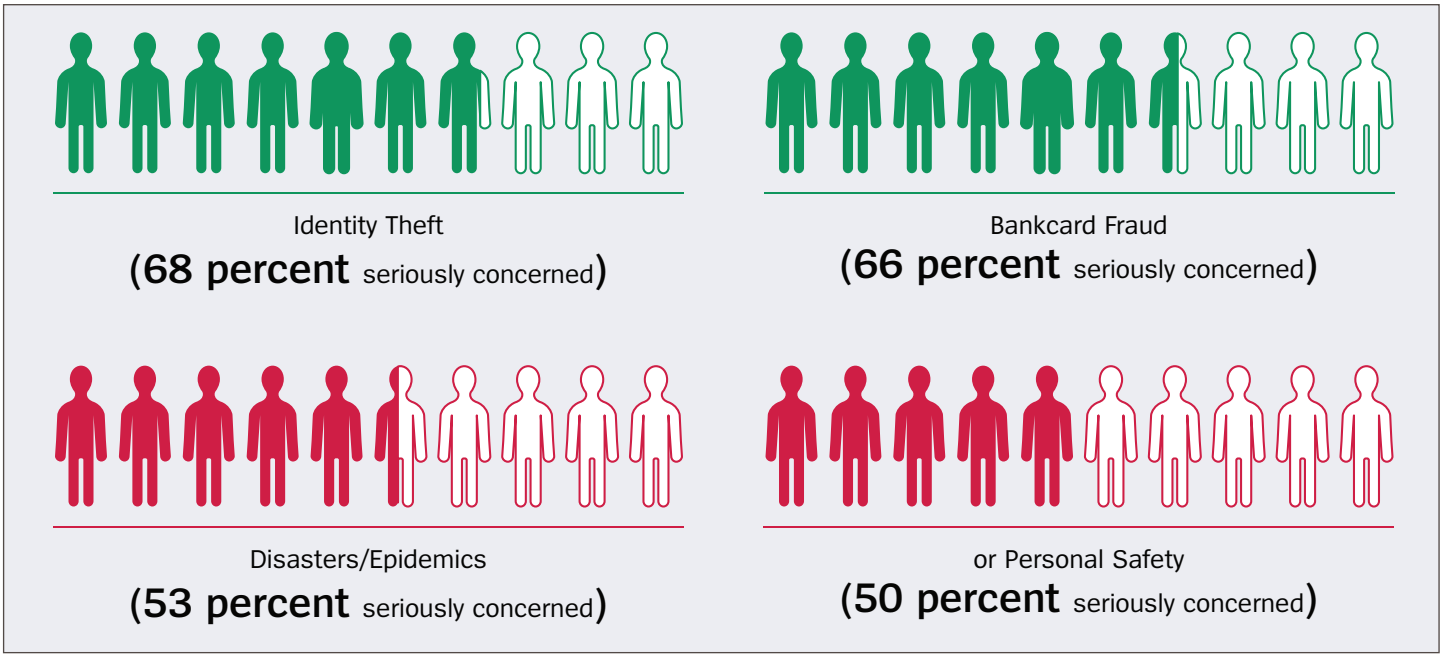
Consumers have a right to be concerned. There has been a steady drumbeat of news around data breaches involving the personal and financial data of millions of consumers. By October of 2018, the number of compromised personal data records for the year had already surpassed the total number of breached records for all of 2017.

In a headline that is close to home for the travel and transportation industry, the Federal Trade Commission (FTC) reported in December 2018[1] that a data breach of Marriott International's Starwood guest reservation database exposed the personal information of up to 500 million people, including names, addresses, phone numbers, email addresses, passport numbers, dates of birth, gender, Starwood loyalty program account information, and reservation information. Some payment card numbers and expiration dates were also stolen, although these were encrypted.

Airlines retain such personal information and more in their own loyalty databases and use it daily to market to consumers, promote ancillary sales, facilitate online transactions, and record passenger preferences. The data is constantly being shared between airports, partners, vendors, and government agencies to optimize the passenger experience. Consumers interact with and add to this data with every tap on their mobile devices and with each purchase.

The risk of identity theft and bankcard fraud exists in large part within airlines and airports because point solutions have been deployed over the years to provide new functions and services to keep pace with customer demands and expectations. These points solutions have resulted in an eclectic mix of systems that cannot be easily integrated with each other or with emerging solutions and software.

[1] https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach



The lack of integration makes it difficult to guard against intrusions. For example, hackers can gain access to the loyalty database through passenger applications, smart devices used by employees or customers, and unsecured connections. This places airlines and airports in an unenviable position. They cannot limit data access because that would negatively impact their own revenue and operations as well as the consumer experience, but unlimited data access brings with it unacceptable levels of risk.

Privacy Concerns Cause Tension

Data privacy is another area of concern for consumers. In the report "Future of the Airline Industry 2035" put out by the International Air Transport Association (IATA) and the School of International Futures (SOIF), one of the major drivers of change identified was the tension between data privacy and surveillance.

The report states:

> *"Advances in connectivity and sensor networks are likely to empower citizens by providing real-time accountability and transparency. At the same time, privacy and surveillance are likely to be high on the list of military and government concerns over the next two decades. How much privacy will people be willing to give up in return for convenience, economic benefit, and security? For corporations, data breaches and cybercrime may require new measures to protect data; privacy itself could become a valuable commodity."*

Airports and airlines need to confront this tension head on. For instance, consider biometrics. On the one hand, consumers appreciate the fact that biometric solutions have the potential to streamline the passenger experience and facilitate seamless travel. Such technologies also provide protection against terrorist attacks by identifying potential bad actors through biometric analysis.

On the other hand, biometric technologies record personal data of an incredibly intimate nature. This data must be stored securely, and many consumers are unconvinced that airlines and airports are equipped to protect their networks from being hacked. The fact that such biometric data may become a requirement for travel – particularly for international travel – simply adds to the tension since a consumer would not, in that case, be able to "opt out" of providing this data.

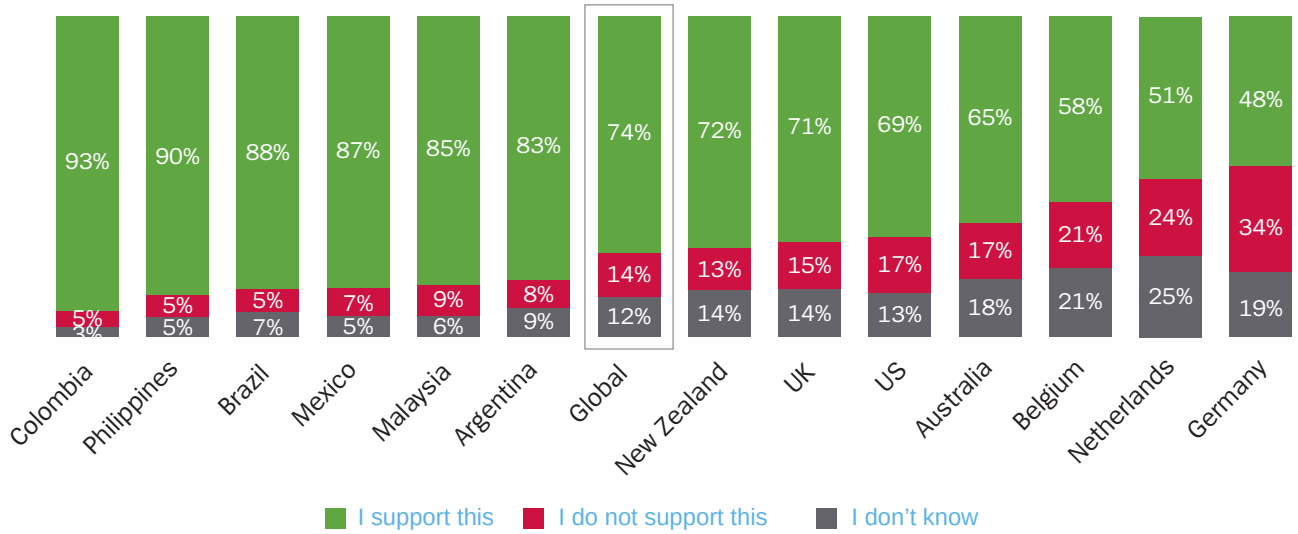
Connected Devices Create Opportunity and Risk

Connected devices are multiplying exponentially within airlines and airports, 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 airlines and airports, almost three-quarters (74 percent) of survey participants indicated that they would support a sensor in their luggage and a mobile application to tell them if their luggage has been unloaded and what carousel it will be on. Support is significantly higher in developing countries compared to developed countries.

High support for luggage sensors in developing countries, less so in developed

Sensors in luggage that communicate with an airport's baggage management system and an app on your mobile phone to tell you if your luggage has been unloaded and what carousel it will be on.



*Developing countries are defined as <$12,000 per capita GDP

To maximize the opportunities that connected devices provide – such as the ability to track luggage or to facilitate pet travel by allowing owners to monitor their pets before, during, and after a flight – airports and airlines must demonstrate that they can protect the data that these devices draw on, generate, and transmit.

Cybersecurity Measures Needed for Legacy Infrastructures

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.

While matters of cybersecurity underlie each of the concerns addressed above, it is important to call out airports here for a very particular reason: airports in large part control air travel. They serve as the hub of operations and the center of security in ways that had not been anticipated decades ago. Aircraft type, origin, destination, and flight information originates with and is maintained by airports.

Protecting this information against viruses and hacking is critical to ensure safety at all levels, lest bad actors plan and carry out a physical attack that could result in multiple fatalities. However, airport infrastructures were not designed with this massive volume of sensitive data in mind. Consequently, airports are racing to "cordon off" vulnerable data and strengthen end-to-end cybersecurity. This includes securing APIs that are now being used to publish flight information to customers, airlines, and partners alike.

Take Action Today

Airlines and airports are facing a dynamic threat landscape that calls for risk-relevant security solutions. Those solutions cannot interfere with efficient business operations or negatively impact the consumer experience. As an industry leader in travel and transportation security, Unisys recommends the following action items to strengthen airline and airport security systems and promote customer trust:

1. **Pay attention to security basics.**
   With cyber threats growing around the world, airlines and airports 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 airports and airlines 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 airlines and airports 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 airline's or airport's long-term success.
3. **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.
4. **Approach security with the customer in mind.**
   To build trust among customers, airlines and airports 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.
5. **Collaborate with business partners to address common challenges.**
   Airports and airlines maintain a complex network of business relationships. Each business partner has their own separate systems, yet these systems are deeply intertwined. Therefore, it is to the benefit of each member of the value chain to ensure a robust holistic security profile.

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 19-0037