amadeus

Safeguarding information systems

A lever for revenue growth

Contents

Foreword 3
Introduction 4
Using security to grow top line revenue 7
An interview with Alex Holden, Hold Security 11
Security to manage costs 12
Q&A with Jarad Carleton, Frost & Sullivan 16
Conclusion 18

Safeguarding information systems: a lever for revenue growth is a white paper developed by Dan Greaves, Alexandra Megally and Xavier Mercè of Amadeus. With thanks to Jarad Carleton (Frost & Sullivan), Alex Holden (Hold Security) and Todd Bell (GlobalDataLock.com) for their contribution.

Foreword

As more and more of our business and personal lives are conducted online, the risks of account takeover or identity theft are ever greater. This creates very real cost for companies: according to data from the Payment Cards Industry Security Standards Council, a cyber attack costs the victim company an average of 2.6 million dollars. It also creates an opportunity: At Amadeus we believe that information security should be seen by the travel industry as a lever for revenue growth.

To achieve this, data security must no longer be the domain of a single department or executive in the IT department, it must be a focus for the whole organization. We have developed this white paper to provide talking points for security professionals looking to convince their commercial counterparts of the importance of information security and for commercial executives looking to get up to speed on how they can use security to unlock top line revenue growth.

Celia Pereiro
Amadeus Travel Payments

Introduction

In 2007, Todd Bell[1] worked as a Chief Information Security Officer (CISO) for a $2B corporation in the automotive sector. Having discovered a number of serious security vulnerabilities in his company's systems, Todd was preparing to implement enhancements that were important for the future of the business. Like most things in life, these enhancements would cost money, so Todd prepared to take his request for funds to the executive team. Todd sat with his CFO, feeling confident that he would recognise the importance of protecting their business against cyber-attack.

Todd still remembers sitting in the executive's office, sun shining through the large windows, as his CFO responded, "while cybersecurity is a nice thing, at the end of the day, we need to sell more tires."

Despite justifying his request with a solid business case, Todd's CFO didn't approve any funding to protect the personal and credit card data in the company's IT systems. Todd recalls, "this was a pivotal point in my career that stunned me."

The experience taught Mr Bell to always be aligned with the business so they could see the real value and benefits of securing sensitive data beyond compliance requirements. This is the question we look at in this white paper.

Times have changed and Boardrooms today are more aware of the importance of information security. This is partly a result of the increasing cost of hacking attacks: according to figures from the Payment Card Industry Security Standards council, a cyber-attack costs on average $2.6 million per incident.[2]

To combat the growth of data security breaches, the Payment Card Industry established a standard for handling sensitive card data: the Payment Card Industry Data Security Standard (PCI DSS). In response to an increase in fraud, the credit card schemes introduced stricter controls to ensure that the person making a purchase online is the valid owner of the card. In the e-commerce world, this standard is known as 3DSecure.

These initiatives have improved security as well as creating challenges for travel companies: PCI DSS is expensive to implement and 3DSecure can prevent sales.

"Travel executives must put complacency behind them and start looking at security as a lever for revenue growth."

[1] Source: interview with Mr Todd Bell, CISO & CIO of GlobalDataLock.com

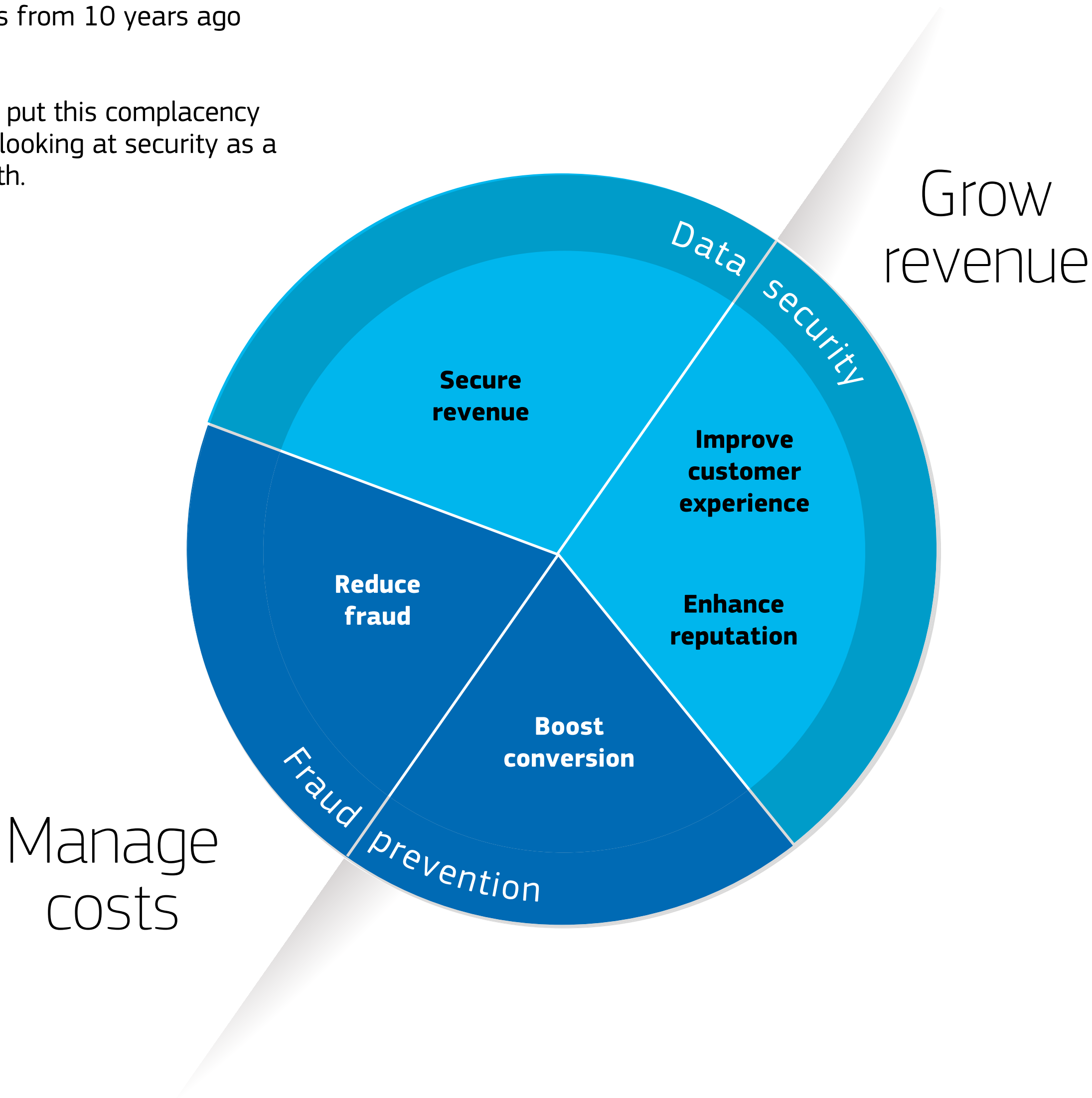
[2] www.staysafeonline.org/blog/on-the-cybersecurity-front-lines-defending-against-phishing-and-social-engineering-attacks/

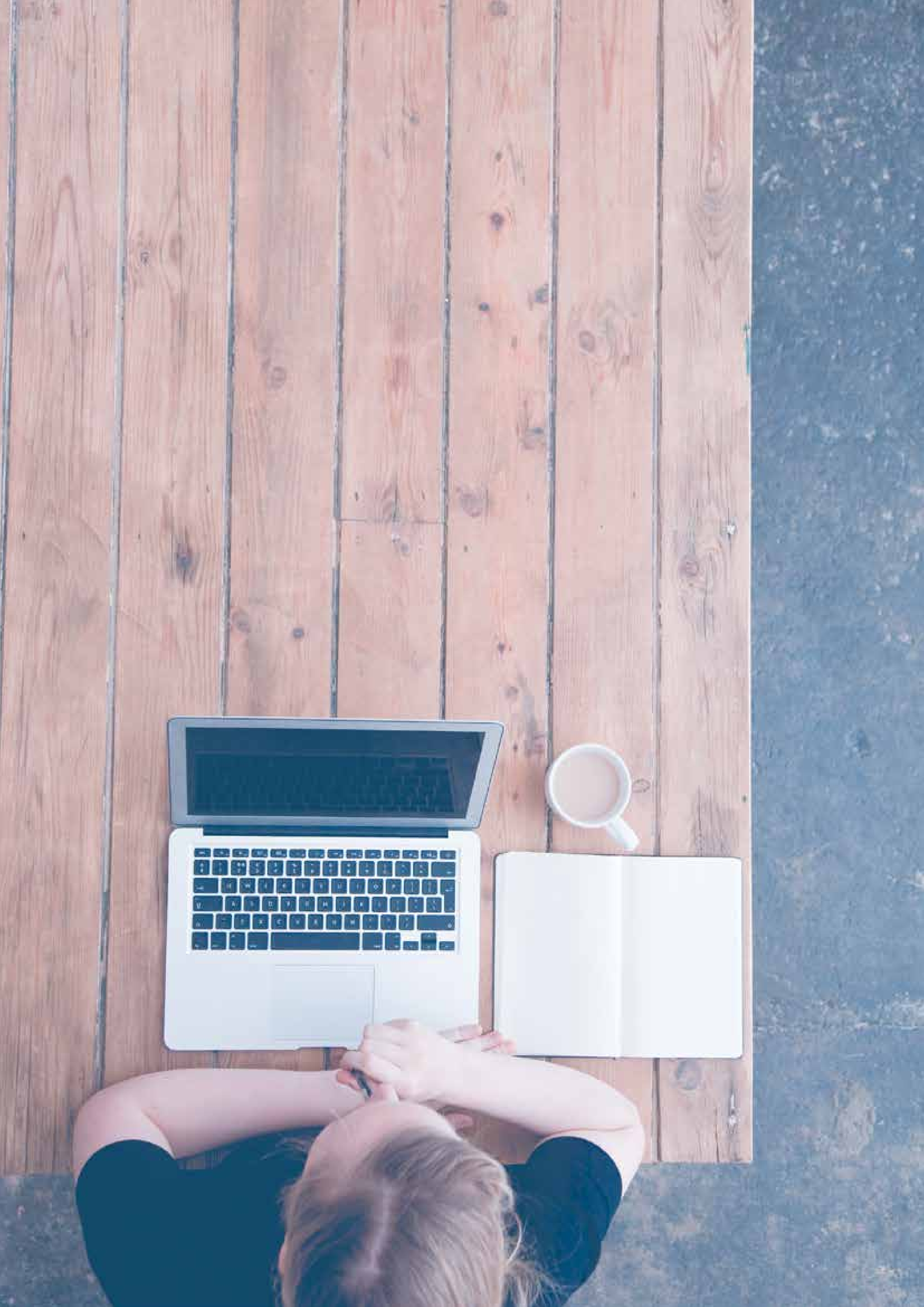
It is precisely these challenges which represent an opportunity for travel companies: because security initiatives are difficult and expensive to implement, companies which implement them well can gain advantage, either through increased sales or a reputation for security.

In his work as a CISO with GlobalDataLock.com & Board Advisor, Todd Bell still comes across complacency. “Many executives feel they are not interesting enough for hackers to even care about the company and if something happens, they have insurance. It floors me to still see the attitudes from 10 years ago to today.”

Travel executives must put this complacency behind them and start looking at security as a lever for revenue growth.

Cybersecurity: benefits beyond compliance





Using security to grow top line revenue

Data security

Consumers expect the companies they do business with to take a responsible approach to safeguarding their personal data; those companies that do that well can earn the trust of their customers and deliver a better purchasing experience.

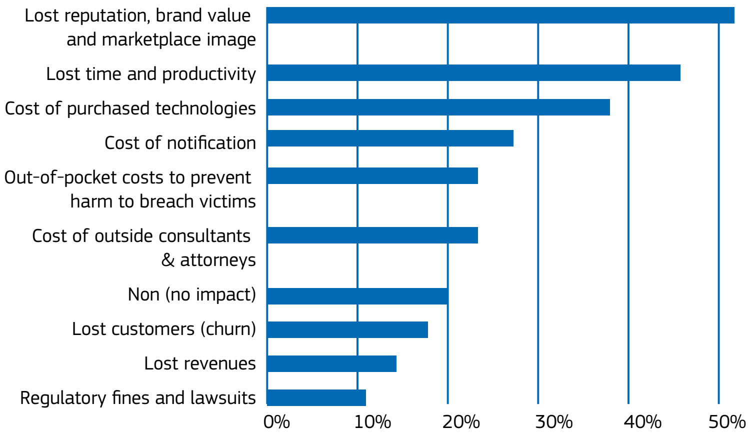
Security as a reputation driver

Consumers place the responsibility for the security of their credit card data firmly with the companies they transact with: in a 2014 study from the Ponemon Institute[3], 63 percent of consumers believe organizations should be obliged to provide identity theft protection.

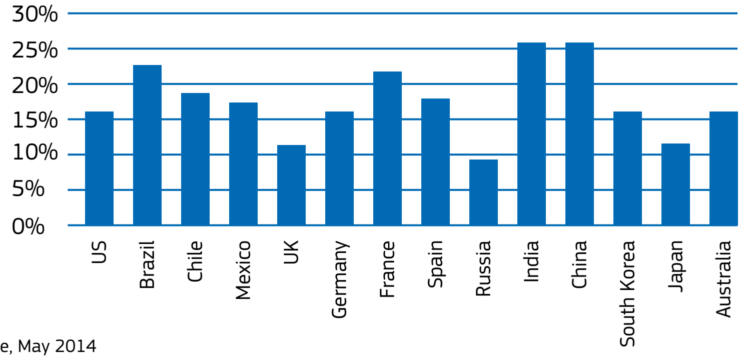
It follows, therefore, that a company's reputation is at risk in the event of an attack. Indeed, most companies report lost reputation, brand value and marketplace image[4], as well as an increase in churn rate (customers leaving to the competition) of 15% following a cyber-attack[5].

The good news is that those companies which can demonstrate that they take security seriously will be rewarded by customers. Research by Worldpay[6] found that, between 10% and 25% of consumers in countries as diverse as Australia and Brazil drop out of an online checkout because they felt concerned that the website was insecure.

How did the data breach affect your company?



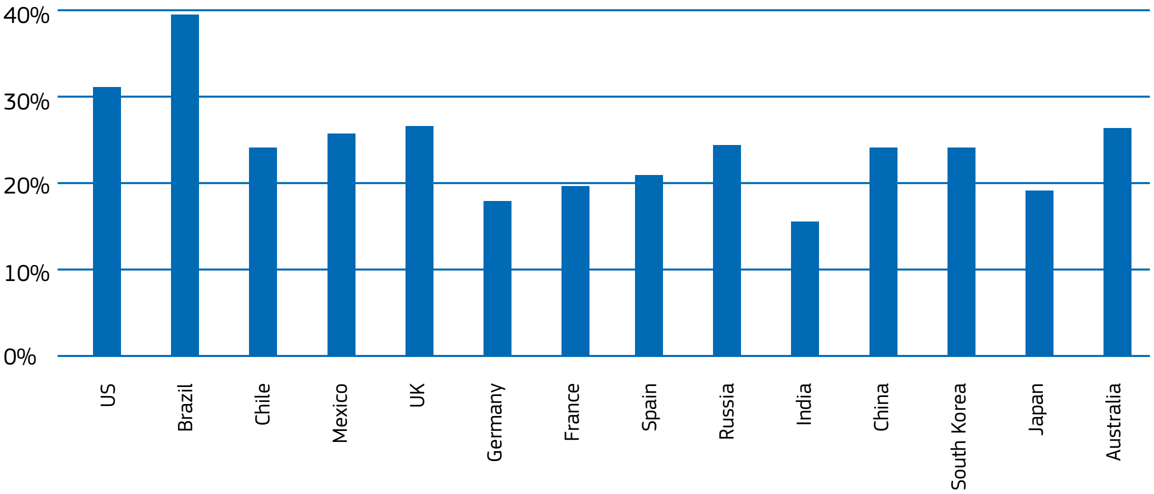
In the last 12 months, have you dropped out of the checkout and, if so, what are the reasons? "I was concerned if the website was secure."



3. "Aftermath of a Mega Data Breach: Consumer Sentiment," Ponemon Institute, May 2014
4. 2014: A Year of Mega Breaches, Ponemon Institute, January 2015
5. "Cost of Data Breach Study: United States" Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, Ponemon Institute, May 2014
6. The Online Payment Journey, April 2015 by Worldpay http://onlinepaymentjourney.worldpay.com/travel

The same survey found that the availability of authentication and digital certificate logos is either the most, or one of the most, important factors in trusting a website for consumers in all the countries surveyed.

Q: Thinking about the entire payment process, starting with the information displayed on the homepage and all the way through to the checkout, which of the following is the most important factor that would make you feel secure about paying on the website?
A: The website is a well-known and reputable brand.



Putting security at the heart of customer experience

Entering credit card details is – in internet terms – a laborious process during which consumers may change their minds about the purchase, enter their details incorrectly, or the internet connection might drop; all of which adversely affects sales. Such problems are even worse when booking on a mobile device where the screen is smaller and the connection less reliable. To counter this, companies launched one-click purchasing; today Amazon is estimated to have a little over 200 million customer credit card details on file; this number is dwarfed by Apple which, through iTunes, has 800 million cards stored on file[7]. If companies store credit card data to simplify repeat purchases, then they must do so securely.

Booking flights in two clicks with Travelstart: a case study

Flapp is a smartphone booking application developed by online travel agency Travelstart which uses data security technology to enable commuters to book a flight between Cape Town and Johannesburg in just a few swipes. Cape Town to Johannesburg is the 10th busiest air corridor in the world with more than 4 million passengers making the two-hour flight each year. Thanks to all this traffic, there is an overwhelming number of flight options: on Saturday, the quietest day of the week, there are 38 direct flights from Cape Town to Johannesburg; commuters coming home for the weekend on a Friday have nearly 60 direct flights to choose from!

[7] www.businessinsider.com/credit-cards-on-file-apple-vs-amazon-2014-4?IR=T

The team at Travelstart saw an opportunity in all this choice. Since its beginnings in a coffee roasting house in Malmö, southern Sweden, Travelstart has aimed to make travel simple. “There is so much choice in the travel industry that you can easily spend two or three hours looking for the right flight,” says Stephan Ekbergh, CEO and Founder of Travelstart Group, “It shouldn’t take you as long to book a flight to Jo’burg as it does to fly there.”

That’s why, when they set about designing their new mobile flight application Travelstart cut out all the extras. “We wanted to make it really simple to book a flight from Cape Town to Jo’burg,” says Stephan.

“A lot of the user experience focus in travel has been around helping customers to pick the right flight option and for sure that is a key part of the experience, which is why we include all flight options in our search results page.” says Stephan, “But the second part of booking a flight is paying for it. Entering a 16-digit credit card number is cumbersome on a mobile device; add in the name, expiry date and CVC security code and your customer has to click well over thirty times just to enter their payment details.”

To simplify the payment process in Flapp, Travelstart had to store their customers’ credit card details, “That puts us in a position of responsibility. Our customers need to trust that we are handling their credit card details securely.”

To ensure there is no risk to their customers’ sensitive data, the Travelstart team, working with Amadeus, converts all credit card details into “tokens”.

“When it comes to making data safe you’ve got two options: encrypt it or tokenise it,” explains Celia Pereiro, “With encryption, an algorithm converts the data into a code which can be stored. The problem with this is that a powerful enough computer can crack the code and convert the encrypted data back to the original sensitive data. With Tokenization, you convert credit card data into tokens with no logical link between the original data and the token so a hacker who accesses stored tokens has no way of converting that data back into useful credit card details.”

Travelstart leveraged this Amadeus technology to make Flapp, “the two-tap booking app” a reality. Once you have downloaded the app and entered your personal and credit card details the flight app lets users book a flight between Cape Town and Johannesburg in just two swipes. At the time of writing, the app which is available from Apple’s App Store and Google Play, has been downloaded 20 555 times and has received extensive coverage in South African and international media. The average Google Play rating is 4.5 stars out of 5. One happy customer wrote, “An app you can do a quick check on flights available saves a lot of time and money and also very secure (sic)”.

With more than 20 000 downloads across Android and iOS since launching in June 2015, Flapp is well on its way to becoming the go-to app for customers who fly between Johannesburg and Cape Town regularly. This is exactly where Flapp wants to be in the South African market; effectively creating an additional and highly targeted sales channel for Travelstart.

Fraud prevention

Unfortunately, there will always be those who look to game the system. The way which travel companies respond and control fraud can unlock missed opportunities.

Focus on false positives

Historically, airlines have taken a binary approach to fraud controls – applying 3DS security or not; or applying fraud management or not. Some airlines even block transactions from entire countries or even regions to minimise the risk of fraud. Such an approach will reject valid transactions. On average, airlines reject 3.3% of bookings due to suspicion of fraud[8].

It is impossible to know exactly how many rejected bookings would have been valid. However, if we assume that the false positive rate is 5%, then even small airlines could be missing out on hundreds of thousands of dollars' worth of revenue (see table).

Airline profile	Passenger revenue ($m)	Value of bookings rejected due to fraud suspicion ($m)	Value of accepted bookings ($m)	Potential value of rejected vaid bookings* ($m)
Major global airline group	$35,000	$1,155	$33,845	$220
Large network carrier	$12,000	$396	$11,604	$75
Mid-sized airline	$5,000	$165	$4,835	$31
Small airline	$500	$17	$484	$3

* If false positives = 5%

To be able to realise these savings the airline industry should look at smarter anti-fraud solutions which uses the traveller data at their disposal to check for indicators that a transaction is fraudulent or not. For example, historical data which shows that a traveller has a history of making similar trips – even on different airlines – would add significantly to the accuracy of fraud checks.

Boost conversion rates with anti-fraud controls

3DSecure is a way to authenticate a cardholder online – customers are redirected to a hosted page where they must enter additional information to identify themselves. Technically, and from a usability perspective, there are many reasons for it to damage conversion rates – and that is why many online merchants don't use it. However, the practice is enjoying something of a resurgence following research from Adyen which shows that, in some countries, 3DSecure actually increases the conversion rate[9].

In India, where use of 3DSecure is a legal requirement and therefore its absence is very suspicious to consumers, 3DSecure had the greatest positive impact on conversion ratios. Similarly, consumers in other markets, like the Russian Federation, Qatar, Czech Republic, Vietnam and Great Britain, also prefer sites with 3DSecure.

[8] Airline Online Fraud Report, Cybersource, 2012
[9] "Optimizing payments to increase revenues" – Adyen and Edgar Dunn & Company

Cyber-crime and the travel industry

An interview with Alex Holden, Chief Information Security Officer of Hold Security.

As of today, travel merchants have managed to avoid some of the bigger data breaches which have beset the wider retail sector. However, it is at the other end of the value chain – monetizing stolen data – where Alex Holden, Chief Information Security Officer of Hold Security, sees risks for travel merchants.

“The main idea [of cybercrime] is to get some kind of financial benefit. The end game from a credit card for example is to buy something with it,” explains Mr Holden, “International shipping is unusual; but international travel is not unusual. If I am buying a physical product online it would be relatively unusual to have it shipped internationally. However, if I am booking a hotel it would not be unusual for me to book a hotel in Rome for example. I can book a business class ticket to Singapore for 2,000 dollars and sell it to you for 1,000 dollars. It’s not my problem if you get stopped when you turn up at the airport. This allows the hackers to separate themselves from their ill-gotten gains”.

Hold Security helps organizations defend against attacks as well as to recover data once it has been stolen. It found fame in August 2014, when the New York Times published the story of the company’s discovery that a group of Russian cybercriminals had gathered the largest collection of stolen personal data to date: 1.2 billion user names and passwords, and more than 500 million email addresses.

Mr Holden and his team monitor the “dark web” for evidence that hackers have access to a site or are selling data from a site. In the course of this work, Mr Holden sees “a continuous stream of travel sites and rewards sites” which have had their data compromised. In particular, Mr Holden urges travel companies to educate their customers on data security, because “the credentials and itineraries are becoming a very marketable asset”.

When thinking about future risks, Mr Holden points to loyalty programmes. “This is something that we see as a huge change in the environment.” Consumers typically don’t check their loyalty accounts very often so the time between the hack and the discovery can be very large. People are also less protective of their loyalty points because they don’t see them as real money. “Sometimes you don’t even expect to get a free night: it’s just something you hope to get. Hackers know that, they understand that”.

Security to manage costs

Data security

Securing data is expensive but the cost of not doing so can be ruinous. By reducing their exposure to cyber-attack, travel companies can reduce both the cost of security and the consequences of becoming victim to an attack.

Fines can be an unnecessary drain on revenues and even prevent businesses from being able to accept credit cards

Merchants which do not comply with PCI DSS, and have credit card information stolen, may receive fines. Depending on the size of the breach, PCI related fines can be as high as $500,000 per incident[10].

In severe cases, merchants can even be given the 'Death Penalty,' preventing them from accepting credit cards. On the top, the payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations; typically, these fines will be passed to the non-compliant merchant.

Achieving and maintaining compliance with the PCI-DSS standard is surprisingly difficult… and expensive. This difficulty is borne out by a recent finding by Verizon[11], which assesses companies for compliance against the standard, that only 20% of companies tested are fully PCI-DSS compliant.

Being able to clearly demonstrate compliance with the PCI-DSS standards can give merchants a clear competitive advantage.

As well as being generally good practice for any business which handles sensitive credit card data, PCI-DSS is used by card schemes to ensure their members are maintaining good security practice. For example, Visa Europe has issued a deadline to acquiring banks using its network that all airline merchants should be fully compliant with the Payment Card Industry Data Security Standard by 31 December 2017.

Reducing Total Cost of Compliance

The cost of compliance for each individual travel company will be different. It is important to build a true picture of the total cost of ownership of compliance. To do this, travel companies should consider the following areas.[12]

Infrastructure:
Additional IT hardware and software for encryption, anti-virus, firewalls, intrusion detection, log management, and more, with associated purchase, licensing, installation, migration and integration, upgrade, operation and support costs.

Services:
Consulting, assessment and regular vulnerability scanning services, as well as process changes, staff training and user

education during change-management activities. Given how fast-paced the security market is, it's important to factor in ongoing upgrades and changes to security frameworks.

Staff time:
IT and business staff will devote some or even all of their working week to planning, actioning, reporting on and auditing PCI DSS controls, instead of their 'day job'.

Once an organisation has understood the cost of upgrading, and maintaining, IT systems and processes to ensure PCI-DSS compliance, the next important question should be how to reduce that cost. Modern IT systems are large complex and highly integrated, which makes becoming and remaining compliant more expensive.

The travel industry is a uniquely complex environment

The travel industry – airlines in particular – have some of the most complex and integrated systems in the world. The challenges of operating in such a global environment, with multiple commerce domains, integrated systems, and back-end partners can make PCI-DSS scoping and compliance overwhelmingly complex. Any secure Cardholder Environment must consider all sales channels (Front office, eCommerce sites, Call Centres, Departure Control Systems at the Airport, Mid- and Back-office systems); must support direct and indirect sales; and most importantly support the transmission of payment and sales information to external payment partners: the merchant's payment service provider, acquiring banks, GDS, IATA BSP.

The key is to reduce the scope of compliance from the beginning. Reducing the scope of the Data Security Standard for businesses reduces the initial cost of compliance, reduces the ongoing costs of maintenance and annual audits and reduces the ultimate risk of becoming victim to a data breach.

10. www.braintreepayments.com/blog/pci-compliance-basics-for-credit-card-security
11. "PCI COMPLIANCE REPORT", Verizon, 2015
12. "PCI COMPLIANCE REPORT", Verizon, 2015

The cost of fraud

The International Air Transport Association estimates that airline fraud costs the airline industry one billion dollars a year. According to the United Kingdom's Fraud Intelligence Network (FIN) and National Fraud Intelligence Bureau (NFIB), each fraudulent transaction costs a long-haul airline £1,561 (€2,189). The costs for travel agencies are slightly lower but harder to bear since a travel agency's revenue is only a fraction of the total ticket price.

The cost of fraud goes beyond the money lost to chargebacks. Tracking and responding to chargebacks is a manual process and can take a significant amount of time for airlines. One mid-sized airline we spoke to for this study estimated that they dedicate three full time employees to managing fraud and chargebacks coming from the travel agency channel.

A survey of UK travel companies by the Fraud Intelligence Network found that the total cost of fraud, including the cost of chargebacks, staff costs associated with managing chargebacks and the cost of fraud prevention measures, can run into many thousands (see table below).

Organisation	Average fraud per booking	Total yearly costs*	Staff costs	Fraud prevention measures	Annualised total costs
Low-cost airline	€701	€70,131	€210,392	€28,052	€308,574
Long-haul airline	€2,189	€70,131	€210,392	€28,052	€308,574
Accomodation only operator	€1,808	€35,065	€42,078	€14,026	€91,170
OTA - 25 million revenue	€1,262	€21,039	€28,052	€14,026	€63,117
OTA - 50 million revenue	€1,262	€42,078	€56,104	€21,039	€119,222
TA - 25 million revenue	€1,262	€21,039	€14,026	€7,013	€42,078
TA - 50 million revenue	€1,262	€42,078	€42,078	€14,026	€98,183
Budget hotel	€637	€35,065	€56,104	€7,013	€98,183
Luxury hotel	€1,122	€35,065	€56,104	€7,013	€98,183

"…the total cost of fraud, including the cost of chargebacks, staff costs associated with managing chargebacks and the cost of fraud prevention measures, can run into many thousands…"

The hidden costs of fraud

The table opposite only shows the most obvious costs of fraud. It does not include some of the more hidden costs, such as those surrounding chargebacks: On top of paying for the chargeback, the merchant is required to pay a penalty for each chargeback incurred regardless of how that chargeback is resolved; typically, this penalty is between USD 10 – USD 50. Similarly, in certain regions, card schemes apply an additional fee for Card Not Present fraud.

Cover all channels

If you sit on one side of a half-full water bed, the other side will rise as the water sloshes away from under you. Much the same effect can be seen in fraud: tighter controls in one channel force fraudsters into less heavily-controlled channels. This points to two areas which may see increased risk of fraud in coming years.

Indirect channel

The payment related fraud risk on an airline's website is well-documented. The issue of fraudulent sales in travel agencies, however, remains a black box for airlines. It is hard to know exactly why; perhaps the challenge of fraud on the airline's website is already big enough and, with fewer intermediaries to co-ordinate, seems easier to tackle. Nevertheless, fraudsters who cannot make bookings direct on an airline's website will try to book the same flight via a travel agency. A truly holistic approach to fraud management, therefore, should include fraud screening on GDS sales as well as airline websites.

At the Airport

Payment at the airport remains one of the least secure environments to make a credit card payment: the card details are either "swiped" in a card reader which copies the card details unencrypted into the point of sale, or entered manually by a desk agent. Check-in and sales offices in airports are nearly always shared between different airlines, so any physical payment infrastructure must be able to process payments made to many different merchants, each with different acquiring banks. So far no solution exists for this problem. Although fraudulent transactions at airports are small compared with other channels, two factors point to increased risk in this area: airlines are selling more and more services at airports, whether excess baggage, last minute upgrades or lounge-access, increasing the opportunities for fraud; simultaneously, airlines are closing the net on fraud in other channels, forcing fraudsters to look creatively at new opportunities.

A Q&A session with security expert Jarad Carleton of Frost & Sullivan

Do you think there is a sense in which concerns about security could slow innovation?

"It should slow down innovation so that people aren't throwing out new applications before they have fully tested and vetted [them]. I think that is by and large a disease that the American economy has imposed on the rest of the world... what merchants really need to be doing is thinking about how they secure their systems and if they are putting mobile apps out there they really need to be thinking about how they secure the data that is put into that application."

How has the cyber-threat changed over the past 10 – 15 years?

"When you consider what is going on today cybersecurity and cyber-crime are inevitably linked. You don't really have what you had in the 90's where you had people breaking into networks and just looking around to see what could be done. Today you don't really have people that are just curious. Inevitably they become linked to organized crime."

What do you think are the organizational challenges faced by security experts in large organizations?

"I think what we have a lot of times is CFOs that don't understand what the risks are. They are not providing the right kind of budget to prevent fraud. And then you have people heading up the IT departments which may not be security experts and they may not have the right people. And then things get overlooked."

FROST & SULLIVAN

What role do today's interconnected systems play in increasing the cyber-threat?

"[The] Target breach was due to the fact that [cyber-criminals] wanted to steal credit card details, [and] they realized Target would be a good place to do it. They targeted the provider of Target's Heating, Ventilation and Air Conditioning systems. If you speak to security experts they will say that applications need to be physically separated – not just logically separated but physically separated."

What is the future for personal data security?

We are getting to a time where everything about us is going up into different business clouds. There are security experts who believe that we are getting to a time where you can have your online persona obliterated. [If that happened to you] none of the companies that you do business with online [would] believe that you are you.

Conclusion

High-profile data breaches have made Boardrooms sit up and take notice of security in a way that they weren't doing 5 years ago. However, security is still seen as a cost; those companies which look to leverage security as an opportunity can open pockets of untapped revenue to help improve their top line results.

Security should be a driver for growth: companies can use a reputation for handling customer data with care to drive more sales to their websites; by saving their customers' credit card details securely, companies can also streamline the payment process, improving the customer experience.

When it comes to fraud prevention, airlines reject on average 3.3% of bookings because they look suspicious. While most of these bookings will be fraudulent, some will be genuine; identifying and accepting the "good" bookings in amongst these 3.3% of rejected bookings could offer some low-hanging fruit for travel businesses to improve top line revenue.

The opportunities also lie in streamlining security and fraud processes to deliver bottom line results. Storing sensitive data as tokens allows travel companies to eliminate sensitive data altogether from their organisations which greatly reduces the burden of meeting regulatory obligations as well as reducing the risk of being hacked. Similarly, automating fraud management controls can not only reduce the level of fraud which a company is exposed to but also reduce the hidden cost of fraud – manually reviewing suspicious bookings.

> "Companies which look to leverage security as an opportunity can open pockets of untapped revenue to help improve their top line results."

Find out more

For further information, visit amadeus.com/blog/category/travel-payments
or contact travel.payments@amadeus.com