Security in an Omni-Channel Environment

Karmen Natalie Naidoo
University of Johannesburg
Department of Applied Information Systems
karmennatalie@yahoo.com

Dr Roelien Brink
University of Johannesburg
Department of Applied Information Systems
rbrink@uj.ac.za

***Abstract*— Omni-Channels ensure that customers have the same shopping experience online as they do in a physical store. Customers should be able to view products online and pay for them accordingly. Customers should also be assured that when they are paying for their items online, all their information is safe and secure. This study examines what organisations use to ensure that their customers private information remains safe at all times. Encryption, one time passwords, audit trails and various other components will be explored. The researcher will also investigate how all these components work together to ensure maximum protection of information at all times. A structured questionnaire was used to measure and rate the overall security features that are used to protect a customer when purchasing online. The results display the preferred features and functions for customers.**

Keywords*— *Information security, encryption, Omni-Channel, fraud, one-time password

I. INTRODUCTION

In 2015 PriceWaterHouseCoopers (PWC) reported that security breaches in organisations have increased by 14%[5]. Fraud in the Omni-Channel environment has also increased by 10% [15]. Hackers are developing new unique methods of stealing a customer's information or tricking a user into giving them their private banking details or other confidential information. These attacks have resulted in customers being afraid of sharing their private details online. Customers are reluctant to shop online because they would have to provide potentially sensitive information such as their banking details. Once customers stop purchasing items online, online stores may become dormant, and organisations may suffer a significant financial loss.

In 2015 iSheriff submitted a report which stated that 52% of customers prefer to shop online rather than in a traditional retail store [12]. They further assert that customers find it easier to purchase items online and have it delivered to them in the comfort of either their home or office. Online stores provide customers with a variety of payment options. Types of payment options include online transactions, electronic funds transfer (EFT), payment through a payment service provider (PSP) such as Paypal and paying on delivery [1].

Symantec Corporation is an international software development company based in Mountain View California which develops and produces software that can assist an organisation regarding online storage and information security. In 2013 Symantec published a report that displays the top ten types of confidential information that is usually stolen from online users [6]. Seen in Figure 1 are the top ten types of confidential information.

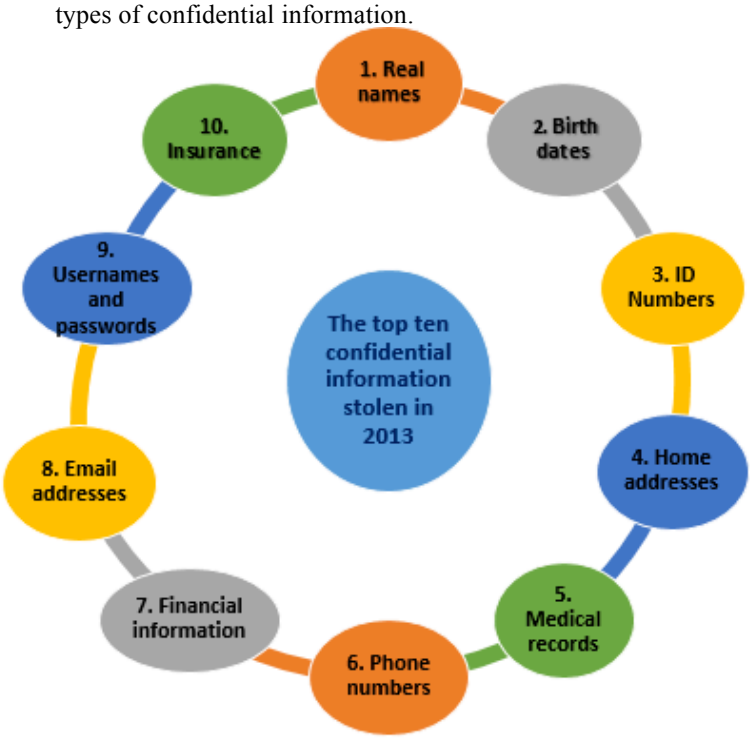

Figure 1 Top 10 information stolen in 2013. Adjusted from [4]

Should a criminal get hold of this kind of information, they can cause a lot of damage to a customers lives. Criminals can create false identity documents by simply having access

to your real name and identity number. They can open a variety of accounts in a customers name and incur a significant amount of debt for that particular customer. In Figure 1, we can see that email addresses are usually stolen. Criminals send emails to people that contain malicious software embedded in the email. The malicious software is programmed to obtain more information from the customer or to exploit them by demanding customers to pay a ransom fee to gain access to their computer again.

In 2016, it was discovered that Acer, a popular technology company, suffered a major security breach which affected over 30 000 customers from various countries [2]. Hackers obtained customers names, addresses, credit card numbers and CVV security codes. Hackers were able to steal information that had been stored dating back to May 2015. Hackers are now able to use the data that they have stolen to exploit customers.

This study identifies what security mechanisms are used by organisations today to ensure the protection of customers information in an Omni-Channel World. According to Zou [16], information security is the act of ensuring that an organisation's most crucial resource is kept safe at all times. Security in this environment is critical and is not only required to ensure the protection of information, but also to make sure that fraud is prevented, if not eliminated, in an Omni-Channel environment [11].

From the literature gathered, the researcher investigates the various techniques available and which of them are used by different organisations in an Omni-Channel World to protect customer information. Not only will these features have to protect customer information, but also prevent, if not eliminate, exposure of the confidential information of clients resulting in fraud in an Omni-Channel World.

II. LITERATURE REVIEW

According to Fairchild [8], an Omni-Channel consists of creating a relationship between traditional retail stores and online retail stores. It ensures the experience customers have in an online store is similar to the experience customers have in a physical retail store. Another significant trend is shopping using mobile devices. According to the Deloitte Omni-Channel retail report [15], in Sweden, online shopping has increased by 15%. Many customers around the World prefer to purchase items from their mobile device, as it is usually always with them. Having customers shop directly from their mobile device is a greater security risk as retailers do not have any control as to what applications mobile customers install on their mobile devices. Customers may have downloaded and installed malicious applications on their mobile devices, which can steal information and use it for illegal activities [3]. Mobile devices include cell phones, smart phones and tablets.

Al-Dala'in, Summons and Luo [3] state that a form of trust needs to formed if customers are to pay for their products via their mobile device. They concluded their research by recommending that a Mobile Device Payment System (MDPS) model should be implemented in online stores to support mobile payment options.

MDPS is a model that online retail stores should consider adopting to allow customers to pay directly from their mobile devices. These days, retailers have mobile applications available to customers to install onto their mobile devices. Customers are then able to purchase items directly by using the application. The use of MDPS will not only ensure that customers have a high level of service, but such a model will assist in ensuring that customer information is kept safe at all times.

With the increase in online shopping, the need for IT security has also increased. When a customer enters their private details into an online store, they are putting their trust that their details are only being used for one purpose only, and that is to purchase goods. Activities that require a customer to provide private information include, but are not limited to, paying for products online or even logging on to your online account. A customer is putting their trust in the company and, they believe that the necessary security policies will be enforced to protect their private information online [7].

Chakraborty and Chung state that organisations in an Omni-Channel World face various cyber security risks. Organisations are always at risk of having vital information stolen from their network. Omni-Channels allow a customer to start an activity on one channel, and complete it on another channel. Customers can transact from their computer, laptop or mobile tablet. It is the organisations responsibility to ensure that the customers experience is the same on all channels. Most importantly, they have to ensure that customer information is safe, which ever channel they choose to work from[19].

In 2015, Universal Payments released a report called Managing Fraud in an Omni-Channel World. The report stated that 74% of online users prefer to pay for their items online and collect it at the store [13]. Once at the shop, they are required to produce proof of payment and an

identification document, to prove that they have purchased the item. Having customers present their identification document at the store will assist organisations in an Omni-Channel World prevent, and possibly eliminate fraud.
Information in an Omni-Channel World needs to have good security protocols, not just from attackers on the internet, but also from any unforeseen disasters that could occur.

According to Schwartzel and Mnkandla [17], disasters such as hurricanes or a fire in a server room can cause a severe loss of information for any organisation. Should such an incident occur, organisations need to have a contingency plan in place to ensure that information is kept safe and can be accessed to ensure the organisation can operate as per normal. Information is a critical asset for any organisation. Should an organisation suffer such a loss, they will not be able to perform essential daily activities.

According to the iSheriff Omni-Channel Needs Omni-security report, it states that with an Omni-Channel strategy, one needs to focus on three major factors of security which are [12]:

1. Protecting multiple points of exposure,
2. Enchancing security visibility and policy enforcement and
3. Addressing new device specific malware

A good way to explain these main focus points is by using an example. If an employee of a business brings his own laptop to his office to complete his daily activities, the business needs to ensure that no vital information will pass through it as they do not know what threats or malware will be on the employee's computer. It is in the companies best interest to ensure that the correct policies are in place when employees bring in their own computers to work to complete daily tasks [13]. If an employee connects to the network of the business, they should not be allowed access straight away; the organisation's IT department needs to first scan the laptop to ensure that it is secure and will not bring in any malicious software that can harm the organisation's network.

One of the main security threats is having data stolen or leaked from a business. Swart, Grobler and Irwin [14] wrote a paper that explained what the Impact would be if any important information had leaked onto the internet. They stated in their research that should an organisation suffer a data leakage; the results could be "catastrophic". Through their research, they also determined that most of the attacks that occurred on different companies were a result of a Structured Query Language (SQL) injection. Eighty percent of online attacks on retail websites are as a result of SQL attacks [14].

III. RESEARCH METHOD

The researcher made use of a quantitative methodology throughout this research project. Following a quantitative methodology has assisted the researcher in objectively gathering the necessary data. Once the data was collected, it was quantified. Creswell and Plano state that structured questionnaires and experiments are data gathering tools that can be used in a quantitative study. A quantitative methodology was used with an explanatory approach which allowed the researcher to identify and explore factors that contribute to securing information in an Omni-Channel World [18].

A structured questionnaire was used in this study which allowed the researcher to distribute the questionnaire to numerous amounts of participants. The use of a structured questionnaire also allowed the researcher to investigate and evaluate the different types of security features that are used by organisations in an Omni-Channel World to ensure information security. The researcher was also not limited to the number of participants who could complete the questionnaire.

The questionnaire consisted of 14 closed-ended questions. Multiple choice questions, rating scales and polar questions were used in the questionnaire. Polar questions either have a yes or a no answer [9]. The rating scales allowed the researcher to rate how effective various encryption methods are. The multiple choice questions allowed the researcher to identify what the general access roles are that one can typically find in an online store. The polar questions allowed the researcher to determine if they were satisfied with other security features that can be found in an online store.

One hundred questionnaires were distributed to various IT professionals in an Omni-Channel World. From the one hundred that were distributed, fifty were completed and returned to the researcher. All fifty questionnaires were valid. The researcher then analysed the data using a technique called cross tabulation, which is also known as contingency tables. Cross tabulation assisted the researcher in evaluating the results in a table with the necessary numeric values gathered [4]. The researcher was able to identify and compare the themes that were found in the data collected.

Participants had the option to either complete the questionnaire via a link online or complete a hard copy. The questionnaire provided a description to participants before they start answering the questions. This description reminded the participants of the topic as some participants completed the questionnaire at a later stage.

IV. RESULTS AND DISCUSSION

Once cross tabulation was done, the following key themes were identified:

- Access roles
- Access control
- Fraud
- Encryption
- Legislation
- Digital trails

These themes have been grouped together and are now analysed in the following three groups:

- Access to customer information
- Online payments and
- Fraud in an Omni-Channel World

Grouping the results gathered, allowed the researcher to identify and explain key factors that contribute to the improvements of security in an Omni-Channel World.

Group 1: Access to customer information

It was clear that 93% of participants felt that granting access to customer information based on employee job role is an appropriate feature. This feature assists in ensuring that only authorised individuals have access to personal customer information. The best way to explain this concept is by using an example. An intern would not have access to personal customer information. They are not authorised to do so since they do not need access to a customer's private information to complete their daily tasks. Should an intern try to access classified information in an organisation's network, they will be denied access. Every activity that an employee performs on the network leaves behind a digital trail.

Group 2: Online payments

Once a customer has selected the different product they would like, they will need to pay for what they have ordered. Customers have a variety of options available to choose from to pay for the products. Most customers prefer to pay for these products by credit card. Organisations need to ensure that the appropriate encryption tool is used to scramble credit card numbers to ensure the protection of customers credit card details.

From all the responses that the researcher has received, 87% of participants are satisfied with the use of Transparent Attribute Encryption (TAE) to protect their financial details. TAE encrypts and decrypts data between the database and the application being used by a customer. This encryption uses a 256-bit key to encrypt a customer's personal information. The use of this encryption will assist in ensuring that customer details are safe at all times and they can feel at ease when using their credit cards to shop online.

All participants who completed the questionnaire have stated that it is safer for an organisation to form a partnership with another organisation that is already Payment Card Industry (PCI) compliant. PCI is a standard that organisations who would like customers to purchase online with their credit cards need to adhere to. To become PCI compliant is complicated and difficult to achieve and maintain. Some organisations are PCI compliant in an Omni-Channel World. A good example is PayPal. PayPal is a Payment Service Provider (PSP). A PSP is already PCI compliant, and they take on the various activities to ensure that they remain PCI compliant. Organisations who are not PCI compliant can form a partnership with a PSP to mitigate the risk that the organisation could face with regards to protecting customers financial information. This risk is transferred to the PSP. The PSP will be responsible for ensuring that those risks are avoided to ensure that the daily activities are not interrupted in any way.

In South Africa, there is an act called The Protection of Personal Information Act (POPI). This act has been put in place to protect customer information. Should a customer give consent for their information to be used by one company for one reason only, then that company must adhere to the request of the customer. They may not in any way use customers information for anything other than it was intended and authorised for, or to share it without the customers consent [10]. This act also ensures that the customers information is kept safe at all times. Once the customer requests their information to be removed from the organisations database, the organisation will have to comply and remove all traces of it [10]. Organisations form a partnership with a PSP so that the PSP will handle all transactions on behalf of them. When a customer agrees to make a payment through a PSP, they will need to tick a declaration box which states that the PSP will be able to use information provided to the organisation to start the transaction process for the product they would like to

purchase. The PSP will only be allowed to use the information for that one transaction and is legally bound not to distribute any information they obtain about the customer to any other organisation.

The results from the questionnaire displayed that 97% of participants felt that the use of an audit trail for information security is necessary. An audit trail will assist in ensuring that employees only have access to information according to their job role. This feature assists managers of an organisation to monitor and observe who has accessed what document and what information they have changed, deleted or added. This feature assists in ensuring that information cannot be manipulated or leaked in any way without a digital trail left behind. An example of how an audit trail could be useful in an organisation is that a manager will be able to see all the interns' activities on the organisation's network. The manager will be able to query why the intern was trying to access classified customer information as it is not allowed according to their job role.

Group 3: Fraud in an Omni-Channel World

Fraud is a major concern in an Omni-Channel World. These days, customers credit cards are stolen by criminals. These criminals then try to use these credit cards to purchase a variety of products online. A One Time Pin (OTP) can be used in the fight against preventing fraud in an Omni-Channel World. The result from the questionnaire indicates that 70% of participants have stated that this is a secure feature based on their personal experience. When customers make a purchase online using their credit card, an OTP is sent to their mobile device that is registered to their credit card. Customers will then have to enter their pin as proof that they are authorising this transaction. Customers have found that this is a fast and effective way to authenticate themselves when purchasing online.

The research results also show that 30% of participants state that this is not a good feature to have. There are various reasons to this response towards an OTP. Since fraud is increasing in Omni-Channel Worlds, some customers do not find this feature safe [20]. Even though some find it a powerful security feature, there are various risks associated with an OTP. Since an OTP is sent to the customers mobile device that is registered to the customer's credit card. Sim card fraud is also a risk. Sim card fraud is when an attacker does a sim swap and receives the OTP which will allow them to confirm transactions without the owner of the credit card being aware of the fraudulent transaction.

V. CONCLUSION

The researcher of this study conducted a detailed evaluation and analysis as to what security features organisations should enforce in an Omni-Channel World to ensure customer information is protected at all times. Features such as OTP, TAE, access control and audit trails assist in ensuring customer information is safe, and these features also assist in ensuring that fraud in an Omni-Channel World is prevented.

It is imperative for organisations to ensure that their customers information is protected at all times. Should customers have a bad experience with regards to their private financial or contact details being stolen, or even leaked to another organisation, without their consent, they will stop purchasing products online or provide any personal information online when asked. As a result, organisations in an Omni-Channel World will lose customer, and they will be at risk of losing money and be forced to shut down.

Fraud is also a major concern in an Omni-Channel World. Organisations will need to ensure that customers are authenticated. The use of an OTP can be seen as an appropriate way to authenticate a customer. An OTP is sent to the number registered to the credit or debit card which was used to purchase online. At times the OTP can also be emailed to the customer. Though the study has shown that an OTP is an efficient technique, it is also a risk due to the ongoing fraud that is occurring in an Omni-Channel World.

This study betokens that various security mechanisms and protocols should be implemented in organisations that operate in an Omni-Channel World. Not only will it assist in security but also in preventing fraud in an Omni-Channel World.

VI. BIBLIOGRAPHY

[1] S. Hybris, "Hybris Architecture and technology," SAP, South Africa, 2015.

[2] I. Paul, "PC WORLD : Massive Acer security breach exposes highly sensitive data from 34500 online shoppers," 20 June 2016. [Online]. Available: http://www.pcWorld.com/article/3085650/security/massive-acer-security-breach-exposes-highly-sensitive-data-of-34500-online-shoppers.html. [Accessed 20 April 2017].

[3] T. Al-Dala'in, P. Summons and S. Lua, "The relationship between a mobile device and a shoppers trust for E-Payment systems," *Information Science and Engineering (ICISE), 2009 1st International Conference,* vol. 1, pp. 3132-3135, 2009.

[4] B. Blumberg, D. Cooper and P. Schindler, Business reseach methods, 3 ed., New York: Mc Graw Hill, 2011.

[5] P. W. H. Coopers, “2015 Africa Capital Markets Watch,” 2 September 2015. [Online]. Available: https://www.pwc.co.za/en/assets/pdf/africa-capital-markets-watch-2015.pdf. [Accessed 23 October 2016].

[6] S. Corporation, “ISTR Internet Security Threat Report,” *2013 Trends,* vol. 19, pp. 1-98, April 2014.

[7] T. Dyck, “Keeping the faith,” eWeek Labs, California, 2009.

[8] A. Fairchild, “Knowledge Management Metrics via a Balanced Scorecard Methodology,” *Proceedings of the 35th Hawaii International Conference on System Sciences ,* vol. 3, no. 2, pp. 1-8, 2002.

[9] I. Fiedler, “Polar questions in Ama*,” Berlin, 2013.

[10] G. Gazette, “Protection of Personal Information Act,” 26 November 2013. [Online]. Available: http://www.justice.gov.za/legislation/acts/2013-004.pdf. [Accessed 3 February 2017].

[11] J. Howard, D. Hudson and N. Kiri, “Recent developments in the fight against fraud and financial crime,” *Information Security Journal ,* vol. 1, no. 7, pp. 293-304, 2015.

[12] iSheriff, “Omni-channel needs omni-security,” iSheriff, USA, 2015.

[13] U. payments, “Managing fraud in an omni-channel World,” ACI Worldwide, 2015.

[14] P. Swart, M. Grobler and I. Irwin, “Visualization Of A Data Leak,” *How Can Visualization Assist To Determine The Scope Of An Attack?,* no. 1, pp. 1-8, 2013.

[15] C. Ternstrand, “Omni-channel retail: A Deloitte point of view,” Deloitte, Sweden, 2015.

[16] H. Zou, “Protection of Personal Information Security in the Age of Big Data,” *Computational Intelligence and Security (CIS), 2016 12th International Conference ,* pp. 586-589, 2016.

[17] T. Schwartzel and E. Mnkandla, “The impact of critical business data on organizations,” *African Journal of Business Management ,* vol. 6, no. 26, pp. 7705-7713, 2011.

[18] J. Creswell and C. V. Plano, Designing and Conducting Mixed Methods Research, Thousand Oaks: SAGE, 2011.

[19] S. C. a. I. Chung, “Challenges and Opportunities of Omnichannel Retailing,” *Europeans Journal of Risk Regulation,* vol. 5, no. 3, pp. 386-388, 2014.

[20] G. Bharath, S. Charan and M. Gangadhara, “Cross refferal validation for sim card validation using one time token and image split/ merge,” in *Tiruchengode, India*, IEEE, 2013.