The road to adaptability in real estate

Ariton Debrliev
a.debrliev@tilburguniversity.edu

Indy van Weijen
i.a.k.vanweijen@tilburguniversity.edu

Jules van Rixtel
j.f.j.vanrixtel@tilburguniversity.edu

Noortje van der Meijden
n.vdrmeijden@tilburguniversity.edu

Wessel Bootsma
w.t.j.bootsma@tilburguniversity.edu

ABSTRACT

The focus within real estate shifted from location to customer experience. Real estate companies like RXR realty implement customer experience as a real estate service.

Digital transformations change the sector as well. Due to COVID-19 the needs for more customer experience and digital transformation have increased and these changes are being implemented more quickly.

In this study the influences of COVID-19 are analyzed. COVID-19 made physical contact a negativity, changing processes throughout the sector. The crisis situation forced decision making to become more rapid.

This rapid change of digital environments, processes and decision making creates a more risky business environment. Measurements need to be implemented to nullify these new risks.

Keywords

COVID-19, Real Estate, Digital Transformation, Customer Experience, Crisis Management.

INTRODUCTION

Real estate used to be mainly about location (Safire, 2020). This changed in the way that location has become decreasingly important. Research has shown that the demand in real estate is shifting and the need for customer experience has grown (Gujral, Sanghvi & Vickery, 2020). Think about smart homes and their applications that residents can use to make their living environment more engaging, productive, and connected.

When building, selling, or renting real estate, it is interesting for investors and/or developers to take customer experience into account. RXR realty is such a company who applied customer experience in their real estate services. They built an application, which was expanded during COVID-19, which their tenants or buyers use for most processes around their building, instead of having a landlord as a middle man.

Due to COVID-19 the need for customer experience is increased, in comparison to the needs pre-COVID-19 (McKinsey & Company, 2020). There is now a greater desire for safety and a healthy environment. Pre-COVID-19, a consumer might have been more comfortable being at home when a handyman comes to your house. Nowadays, the needs have changed and people want as little as possible moments of contact with other people.

During a crisis, people's needs are changing, so if a company wants to deliver a good customer experience, they must be flexible in the way they provide their services. (Pleyers & Poncin, 2020)

Therefore, this change in the way of working brings new risks and business decisions as well. In this study the influences of COVID-19 on RXR realty's service providing will be analyzed.

RESEARCH

Objective

Companies in real estate are not yet aware of how to quickly switch and respond in a crisis situation and how to safely redesign their processes and governance to meet the needs in the new situation (McKinsey & Company, 2020). It is important to act quickly in a crisis situation, because the needs of your customers are changing rapidly. How a real estate company can best shape their business processes to be able to quickly adapt to a crisis situation, is still unknown. In this research there will be extensive attention for how businesses can anticipate this the best way.

RXR realty will be used as a case study in order to identify process changes, governance changes and risk changes. These will be used to draw more general conclusions about the whole sector.

These conclusions will be used to answer the following question: how do companies in the real estate sector change their strategy during a crisis to react to rapidly changing customer needs?

Approach

This study will examine actual and recent sector reports and company data, which in combination with prior academic literature will be used to conduct an analysis to understand the why's and how's of the pre- and post- COVID-19 differences that have taken place. The specific reasons for this approach is that, COVID-19 is a disruptive event and, because it takes quite some time to publish academic papers, the effects of COVID-19 on the real estate industry have not been extensively examined within academic literature. On top of this, because regulations are constantly changing, more recent and actual information can be deemed more valuable.

Within this study, assumptions will be made at points to perform a more complete analysis. When any assumptions take place, they will be mentioned explicitly and the decision for the assumption will be substantiated.

The study will aim to provide a comprehensive overview of the analysis regarding the real estate industry and a more specific view of RXR Realty's company processes, the risks implied by these processes, and how a decision making structure has enabled the changes within these processes. Finally, the success of this digital transformation will be elaborated upon and improvements will be suggested.

REAL ESTATE & HOUSING

The real estate industry is one of the largest industries within the US. Federal statistics estimate that the real estate industry has contributed about 13 percent of the GDP, or 2.7 trillion dollars (Amadeo, 2020). For the purpose of this project, the focus will be on one market within this industry: The Real estate investing, operating and developing companies within New York City and its surroundings. One unique aspect of real estate to other sectors is the fact that real estate has a high barrier to entry, as real estate investments tend to be very expensive.

Pre-COVID-19: In 2019, New York ranked 7th in the CBRE's fifth annual Global Living Report. The average property price was 674.500 dollars and the average price per square foot 526 dollars. Since 2015, the housing market within New York City has seen an annual value increase of 4.41 percent (Santarelli, 2020), which only started to drop when the COVID Crisis hit. Yet even before the Crisis, in Jan of 2020, the Wall Street Journal reported that the market value of the real estate in New York showed signs of weakening. All in all, the New York City house market tended to be a high-entry profitable market with a stable increase in size and price throughout the years (Barbanel, 2020) As discussed earlier, the real estate market has started reinventing the way it creates value through means of customer experience, as this has been a big trend in recent years (Gujral et al., 2020).

Post-COVID-19: The crisis has hit the real estate market within New York City harder than both the 2008 financial crisis and the crisis following the 9/11 terror attacks, according to the WSJ (Clarke, 2020). Because of COVID-19, companies need to reimagine several business processes from: How they sell houses to how they deliver customer experience. As one of the main points within COVID-19 regulations is reducing the amount of contact points, companies have been looking for digital ways to perform certain business activities. (McKinsey & Company, 2020)

ANALYSIS

In this part the process, the governance and a risk indication of the RXR realty application is defined. First an overview of the situation before COVID-19 is given. Then the influences of COVID-19 on RXR realty are discussed.

Pre-COVID-19

As was described before, the real estate market shifted from a location-oriented value chain towards a customer experience-oriented value chain. RXR realty used this opportunity by providing their tenants with an extra service. They developed an application to remove the middleman and make multiple processes a lot more efficient. Before the application was implemented, a limited overview of the customer's activities would have looked something like (figure 1):

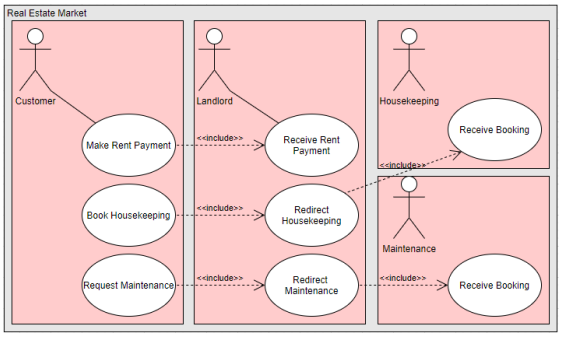

Figure 1. Use case diagram of customer activities RXR realty Pre-COVID-19

See appendix for readable image

Before COVID-19, all these functionalities would be separate processes. For example, making a maintenance request would require the customer to contact the landlord who needs to verify his tenant. The customer then has to explain to the landlord

what the problem is. The landlord has to pass this on to his maintenance company and acts as a middleman in the maintenance company making an appointment with the customer. This process takes many steps, time and therefore money and on top of that can be the cause of irritation for both the landlord and the tenant. In figure 2 a maintenance request is visualized in a Swimlane model. In this case the landlord was responsible for handling the request correctly and storing all the data safely.

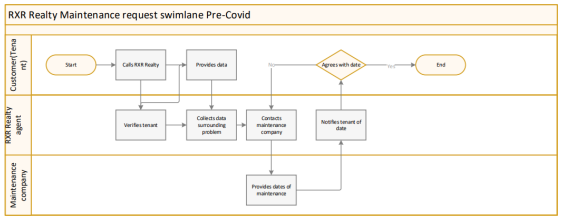

Figure 2. Swimlane activity diagram of maintenance request RXR Realty Pre-COVID-19

See appendix for readable image

The risks that apply in this situation are less relevant for cyberspace, but still could harm the privacy of the tenants. The risk analysis will also be executed according to the CIO model shown in figure 3, Confidentiality, integrity and availability are the fundamental elements of security controls in information systems (Samonas & Coss, 2014).

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (Samonas & Coss, 2014)

Integrity: Guarding against improper information modification or destruction, and including ensuring information non-repudiation and authenticity (Samonas & Coss, 2014).

Availability: Ensuring timely and reliable access to and use of information (Samonas & Coss, 2014).

Figure 3. The CIA triangle

(Samonas, 2014)

Risk 1: Logging wrong data: Human data entry can result in errors that have an impact on the integrity of the contract and appointments, which could for example result in tenants paying the wrong price for their rent, utility bills. Studies have shown that manually reporting data sets result in 23,6 incorrect values through human mistakes, and this results in a likelihood of 4. The impact of these mistakes is also 3, because financial mistakes are easily recovered by paying back the issued price. This has an impact on the integrity of the information (Barchard, 2011).

Risk 2: Leaking personal information: By accident or on purpose personal information could be leaked. A lot of companies are hacked on a yearly basis, during these hacks the personal information of the users are accessed. In 2013 Adobe was hacked and the hackers had access to 153 million user records. In May 2019 Canva was hacked and access was gained to 137 million accounts (Swinhoe, 2020). The impact of such an event is 4, because personal information can be gained which can be held against the user. The likelihood this risk will happen is 5, because this happens frequently, when the correct measures are not applied. This risk mainly has an impact on confidentiality and integrity, because information can be seen and adjusted.

Risk 3: Absence of landlord: When the landlord is not available due to work overload, malfunctioning network, sickness etc., the tenants cannot arrange an appointment. The impact of such an event is 4, because there are issues which need to be solved quickly, because otherwise the problem will get worse. The likelihood of such an event is 3 because there are several events which might happen. This has an impact on the availability.

Impact						
Very high to certain	5					
High to very high	4	Risk 2		Risk 3		
Middle to high	3		Risk 1			
Low to middle	2					
Zero to Low	1					
		5	4	3	2	1
		Likelihood				

Table 1. Risk assessment RXR Realty Pre-COVID-19

See appendix for readable image

RXR realty is an innovative company in the real estate industry. Reading about successful projects of RXR realty, in this study it is assumed that RXR realty is a top-performing company ("Our Company | RXR Realty", 2020). Going on the results of research done by Weill (2004), it can be concluded that top-performing enterprises succeed by implementing effective IT governance to support their strategies and institutionalize good practices. Additionally, he wrote that companies which

performed above-average on IT governance followed a specific strategy, such as customer intimacy. These successful companies had 20% or more profitability than firms with the same strategy, but poor governance. Customer intimacy is a business strategy where they focus on customer needs, and it measures a company alignment and prioritization to those needs (Weill, 2004). RXR Realty has a focus on customer experience which is a form of customer intimacy.

As discussed, the app of RXR realty was created before the outbreak of COVID-19. The app was developed by 'The RXR Lab' of RXR realty, where they develop technologies and services that reimagine value creation within Real Estate ("RXR Lab | RXR Realty", 2020). By analyzing the management team of RXR realty ("Our Company | RXR Realty", 2020), we saw there was only a 'head of development', who might be part of IT decisions. We found no reason to speculate that the Leadership team is 'tech-savvy' or that any other members of the leadership team were responsible for certain IT decisions. Therefore, we presume that there is an IT monarchy at RXR realty made up of the team within the RXR lab to make the 'tech-savvy' decisions regarding IT architecture and IT infrastructure. Furthermore, we assume that IT principle decisions were made by this group of IT specialists within the lab in collaboration with top business executives, forming an IT-Duopoly. As the app focuses on customer experience, we expect the app was created with the important decisions regarding business applications needs and inputs taken on a federal level, as it is important to be close to the customer to investigate customer needs. As digitalization and customer experience is a big part of the strategy of RXR Realty, we expect that IT investments and prioritization decisions were taken by the same IT-duopoly as that which determines the IT-Principles. Looking at the governance matrix below, we see that we have theorized that the matrix is similar to a top-performing matrix as described by Weill and Woodham (2002).

	IT principles	IT architecture	IT infrastructure	Business application needs	IT investment and prioritization
Business monarchy					
IT monarchy		x	x		
Feudal					
Federal				x	
Duopoly	x				x
Anarchy					

Table 2. IT governance RXR Realty Pre-COVID-19 (Weill & Woodham, 2002)

See appendix for readable image

Post-COVID-19

As COVID-19 catapulted the need for customer experience and digital transformation with tenants, RXR realty underwent a digital transformation by creating the application that served new needs created by this crisis situation. Maintenance and other concierge services could in this case be dealt with more efficiently and safely. Additionally, this app also enabled safety regulations during a crisis, such as COVID-19, to be implemented. Consumers can now simply open the application on their phone and send requests. This process is visualized in the following UC diagram, figure 4:

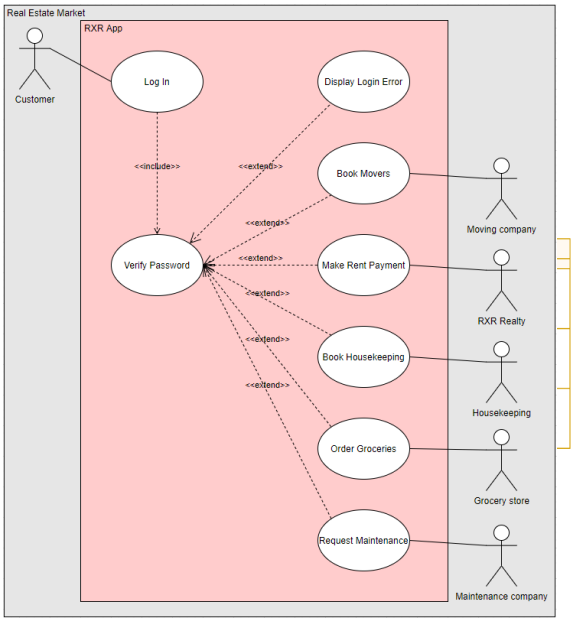

Figure 4: Use case diagram of customer activities RXR realty Post-COVID-19

See appendix for readable image

Several steps are removed from the process, such as the entire role of the landlord. The downside of customers having a method to have direct input to the 'third parties' like the maintenance company is that the third parties will be likely to have more work translating that input into the job that they actually need to do.

Specifically for COVID-19, we have hypothesized the existence of a process which checks and informs the tenant regarding possible regulations. This makes it possible for RXR realty to manage the regulations not only during the COVID-19 Crisis, but also any following Crisis more effectively and efficiently. See figure 5.

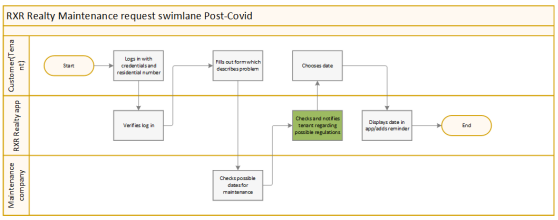

Figure 5. Swimlane activity diagram of maintenance request RXR Realty Pre-COVID-19

See appendix for readable image

With the digital shift to an application which allows residents to manage elements of their personal lives there are multiple risks that need to be considered. The entire experience is powered by a robust data and analytics infrastructure that is located online instead of in physical activities. The impact and likelihood per risk of this digital transformation are analyzed and assessed in this section. The likelihood for each risk defined in the context of minimal control measures. The countermeasures to mitigate these risks will be defined in section (*Cyber Security Report*).

Risk 1: Payment fraud (credit card fraud): RXR realty must make sure that payment fraud will be safely processed, so it could not be accessed by potential attackers. Four restaurant chains in the United States were affected by payment fraud. Approximately 4 million cards were retrieved during the breach and their reputation was harmed (Krebsonsecurity, 2020). For that reason the impact is 5, and the likelihood is 4. This risk will mainly have an impact on confidentiality.

Risk 2: Private agenda: It is important that the appointments which have been made are not accessible for external actors, since awareness of the absence of residents could result in burglary. Unfortunately this happened before. Kaspersky (2019) recently detected that users of Google Calendars got notifications, where they shared their personal data, like credit card info, by clicking on the link. When 'calendar phishing' would happen by the RXR realty app, the impact of this event would be 5. After such an event residents might not be feeling safe at home and if RXR is held accountable it will influence their image. The possibility of such an event is 3, because hackers are not often capable of breaking into other people's homes. This risk will mainly have an impact on confidentiality.

Risk 3: Insider risks: Insider threats via a company's own employees is 50 percent of the reason that cyber breaches occur. Briefly, there are two kinds of risks: the negligent employee and the malicious employee. Malicious Employees know how to harm the system for their own benefits. Negligent employees could affect the integrity of the data by processing wrong data. In these two cases the impact was different, there were high value events in which customer data was stolen and some of the lost hundreds of million dollars (Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D., 2018). The impact of this risk is 5, because in such an event tenants will be harmed and likelihood for this risk is 4. This risk has an impact on confidentiality and integrity.

Risk 4: Hacking database: RXR realty needs a database which includes the personal information of tenants. The tenant also has to log in to enter the limited database to use this data. There is a risk that hackers enter this database or hack the single log-in of the customer. According to the U.S. Department of Justice, social engineering attacks are one of the biggest threats over the world. It is stated that in 2016 the estimated cost was 121.22 billion dollars (Salahdine & Kaabouch, 2019). The impact of this risk will be 5 and the likelihood is 5 as well. The confidentiality and integrity of data will be harmed.

Risk 5: system overload: RXR tenants have a direct input in the RXR application, which makes it potentially vulnerable for attacks on its server capacity. Every year a lot of companies are harmed by DDOS attacks. In 2016 the following big companies were harmed: Netflix, Amazon, Spotify, Airbnb and many others (Strawbridge, 2019). The goal is to bring the service down or to create a system failure, so this has a high impact of 4. The likelihood of this happening without any security measures on this topic is high, 5. This risk has an impact on the availability of the system.

Impact							
Very high to certain	5	Risk 4	Risk 3	Risk 1 & 2		
High to very high	4	Risk 5				
Middle to high	3					
Low to middle	2					
Zero to Low	1					
		5	4	3	2	1
		Likelihood				

Table 3. Risk assessment RXR Realty Post-COVID-19

See appendix for readable image

	Confidentiallity	Integrity	Availabillity
Risk 1	X		
Risk 2	X		
Risk 3	X	X	
Risk 4	X	X	
Risk 5			X

Table 4. CIA assessment Post-COVID-19

Also the decision making on processes and risks has changed due to the unexpected arrival of COVID-19. Companies had to respond quickly with resilience. We saw many digital transformations which have taken place in 2 months, which normally takes 2 years (Nadella, 2020). Quick decisions can be made because there was a common purpose, so operations teams can achieve goals that would have been considered impossible before the crisis (Barriball, George, Marcos & Radtke, 2020). Because of the COVID-19, changes needed to be made within the app. For instance, it needed to become possible to book certain concierge services without contact points. Also, it had to be made easier to reduce the amount of contact points whenever a concierge service, such as a cleaner, would come by. To take decisions more quickly and safely during a crisis such as COVID-19, companies tend to employ a more centralized decision making structure (Weill, 2004). Because of this, we speculate that the main difference within the before and after matrices, lies within the business application needs and investments. As the business application needs changed because of this crisis, we believe that the decisions were made with a more centralized business Monarchy, consisting of the top-level management. As for investments, we believe that to facilitate these changes the IT-investments decisions were also made by a business monarchy. This helped to centralize the decisions and is a usual strategy within crisis scenarios. Furthermore, we believe that the other decisions such as IT principles, IT architecture and IT infrastructure were not any more centralized as this crisis had a more immediate impact on the RXR realty app. A representation on the new decision making architecture is shown below in table 5.

	IT principles	IT architecture	IT infrastructure	Business application needs	IT investment and prioritization
Business monarchy				x	x
IT monarchy		x	x		
Feudal					
Federal					
Duopoly	x				
Anarchy					

Table 5. IT governance RXR Realty Pre-COVID-19 (Weill & Woodham, 2002)

See appendix for readable image

DISCUSSION

This paper aimed to see how a disruptive situation, such as COVID-19, can push companies to pursue digital transformation. Within this research, the case of RXR Realty was taken. The New York-based real estate company is a highly innovative company that has developed an application which aims to fulfill the rising need for customer experience within the real estate industry. This need for customer experience has grown much faster by the COVID-19 crisis, as now concierge services such as grocery delivery and mechanics needed to take place with a minimum amount of possible contact points. The minimization of contact points are precautions specific to a crisis such as COVID-19. However, they do serve as an example to illustrate how RXR Realty needed to adapt to this new 'normal'. To facilitate these safety-oriented measures, RXR Realty reimagined some processes by digitalization, such as the process of scheduling a mechanic. The newly digitized process would now be done through the application which increased the efficiency and potentially reduces the costs for RXR realty as less time is needed to facilitate each mechanic request. On top of this, we hypothesized that the app contains an activity within the process which checks current regulations. For the case of COVID-19, the regulations might be that contact points need to be minimized. However, this activity might be interesting for prospects, as future crises might introduce new regulations that need to be maintained.

The digital transformation to a customer-focused online application resulted in more risks concerning the online environment. Before the digital application, the risks were mainly caused by personal failure or mistakes, but this shifted to malicious cyber-attacks such as credit fraud, hacking database, system overload, insider risks, and private agenda. It is concluded that these cyber risks have a higher likelihood since the U.S. Department of Justice stated that the number of cyberattacks is increasing. The impact of the risks increased, as more sensitive information is stored online. To successfully work out the digital transformation these risks need to be mitigated, otherwise, it will affect the company's confidentiality, integrity and availability.

To facilitate these decisions, the IT governance of RXR realty was analyzed. The pre-COVID-19 situation seemed to follow one of the three top-performing governance structures. However, we hypothesized that because of COVID-19, and the decisions that needed to be made to facilitate the changes within the app, RXR Realty used a more centralized decision structure with more centralized business unit needs as the application directly plays into this aspect. This reflects how companies tend to use more centralized structures in terms of crises as discussed by Weill and Woodham (2002).

CONCLUSION

Within this research it is examined how a company, such as RXR Realty, can use digital means to cope with shifting customer needs during a crisis such as COVID-19. Despite the fact that only theoretical and secondary sources are used for this

study, we can conclude that RXR realty quickly responded to the changes in needs; from location-oriented to customer experience-oriented. For this study, no direct contact has been made with RXR realty, this means that our analysis was solely based on information that was available through RXR realty's website and reports, where academic literature was used to form an understanding and perform the analysis. Making contact with RXR Realty would have benefited the research as a more precise picture could have been drawn. To gain more insight into decision-making on developments, such as the RXR realty application, we would recommend to perform an internal study, so that a more extensive analysis can be done which would result in a more specific conclusion that RXR realty has gone through a successful digital transformation.

ACKNOWLEDGMENTS

This template is based on the template for the International Systems for Crisis Response and Management (ISCRAM) - proceeding format, originally developed by Bartel van de Walle in 2004. We thank the ISCRAM community for sharing, developing and maintaining this template.

CYBER SECURITY REPORT

In this cyber security report the risks will be analyzed with the observe, orient, decide and act (OODA) loop shown in figure 6 (Boyd, 1987). According to Brehmer (2015) this model provides guidance to do systematic research. In the main paper the first step of the loop 'observed' is handled by identifying the possible risks of the digital transformation. The cyber security paper starts with the orient phase by illustrating the identified risks within the online environment using the Use Case Measures Description Generic Model. Also, it will describe the possible countermeasures to mitigate the risks. The 'act phase' describes how the oriented counter measurements will mitigate the identified risks. Lastly, the 'act phase' reviews the process by creating a new risk assessment for the applied counter measures.

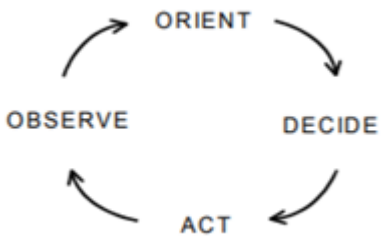

Figure 6. Observe-Orient-Decide-Act (Brehmer, B., 2005)

Orient

The identified risks from the 'observe phase' are shown in figure 7. This Use Case Measures Description Generic Model illustrates the identified risks within the online environment of the RXR realty app. below the possible countermeasures for the risks in this model are described.

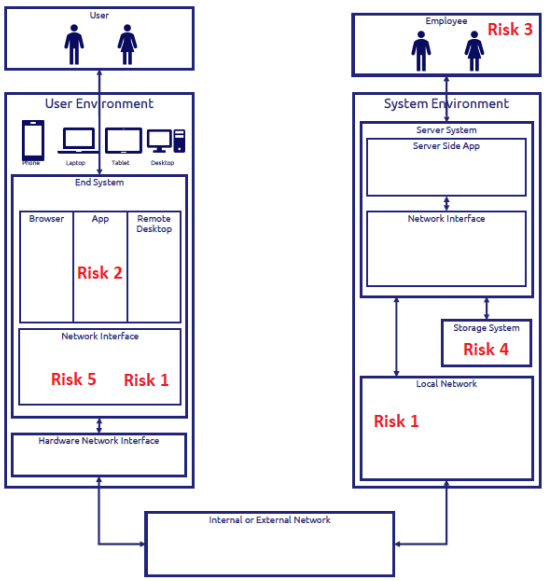

Figure 7. Identified risks 'Observe phase' (Slot, R., 2019)

See appendix for readable image

Management

The management is responsible for minimizing the attack surface, through application updates and configuration. According to Anderson (2020), "people are not paying attention to the costs as they are immediate and determinate in time, storages and bandwidth, than the unpredictable future benefits. This present Bias causes many people to decline updates, which was the major source of technical vulnerabilities." Viruses and other attacks have made it crucial to patch vulnerable systems and software. Security needs to be in mind when designing an automated update process. This will contribute to reducing the cyber risks within an organization (Dunn, 2004).

Web Application Firewall

A Web application Firewall is a shield between an application and the internet which filters out harmful attacks to protect the application (Anderson, 2020). Web applications need to be secured with firewalls (WAS, WAF) within the application layer (Boberski, M., 2010). WAS is an algorithm which uses a blacklist to detect vulnerabilities in web

applications. This is a negative logic filtering built on signatures of known attacks (Kazanavicius, E., Kazanavicius, V., Venckauskas, A., & Paskevicius, R., 2012). A web application firewall (WAF) operates in the application layer of a web application server. It is an intrusion detection system, but it is not operating on the network level (Kapodistria, H., Mitropoulos, S., & Douligeris, C., 2011).

Intrusion detection

Intrusion detection systems (IDS) can detect malicious attacks by using boxes which sit on the network and look for signs of an attack in progress or a compromised machine to prevent or minimize the impact (Anderson, 2020). IDS defines which (intruder) machines need to be followed to understand the malicious logs or to find out what else they will attack. Besides the normal simple intrusion detection as: failed logons, credit card expenditure or extreme long phone calls, more sophisticated systems fall into two categories: Misuse detection and Anomaly detection (Kim, G., Lee, S., & Kim, S., 2014). Misuses detection systems detect likely behavior of an intruder, by looking for a signature (characteristics) of a specific attack. Anomaly detection systems search for anomalous behavior without using a clear model of the attackers operations to detect attacks who are not previously recognized and catalogued (Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y., 2013).

Encryption

Encryption is a mathematical process of transforming information using an algorithm, so the plain text will be unreadable by changing it into a cipher text which is only readable for those who have special knowledge about the encryption of the cipher text (Diffie, W., & Hellman, M., 1976). According to Anderson (2020) ‘it is the key technology for protecting distributed systems’. The symmetric key only uses one secret key for encrypting and decrypting and an asymmetric key uses a public and private key (Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y., 2017). Using symmetric keys the preferred worldwide standard algorithm is Advanced Encryption Standard (AES). The commonly used algorithm which is used for public encryption or digital signatures is RSA in combination with the technique of optimal asymmetric encryption padding (OAEP) (Diffie, W., & Hellman, M., 1976). OAEP is used as a padding scheme and encrypts the message and adds randomness to the process.

Access control

According to Anderson (2020) Access Control is the gravity of Computer Security. It functions by controlling which principles (persons, processes machines etc.) have access to which resources, what they can read, which programs they could execute and how data could be shared. Within access control measurement four principles are important: identification, Authentication, Authorization and Nonrepudiation to define the access. The access will be executed on four different levels (Anderson, 2020):

- Hardware: Operating systems relies on hardware protection for the processor and memory of the system.
- Operating system: How could resources form lower components like files and communication ports be used in the applications. For example using different apps on the same phone without sharing data
- Middleware: The applications are written on middleware, so the access to browsers, systems or databases need to be managed.
- Application: Which principles (people) have which responsibilities to read, execute or share data from the applications.

Decide

In this chapter is decided which countermeasures need to be taken to mitigate each risk. In figure 8 is shown where in the online environment of the application the risks are mitigated by which countermeasures. Below the figure is described.

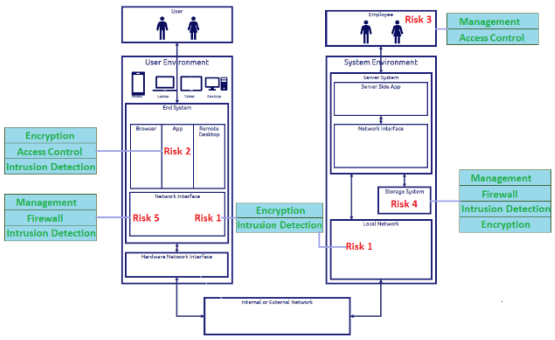

Figure 8. Countermeasures in online environment (Slot, R., 2019)

See appendix for readable image

Risk 1 - Payment fraud: The management needs to maintain all the required updates of the payment systems so it reduces the risk of being attacked by malicious users (Anderson, 2020). The process of paying in the app of RXR realty need to be encrypted with AES symmetric key, since this is the most commonly used cryptography by banks due its standard definition, high security and efficient

processing (Selvaraju, N., & Sekar, G., 2010). Nevertheless, when the encryption is being hacked, intrusion detection systems reduce the impact. Misuse detection systems recognize attacks using big data to compare online malicious behavior with normal customer behavior like exceptional high transactions (Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J., 2013).

Risk 2: Private agenda: To identify, authenticate and authorize each user RSA asymmetric key encryption is applied. RXR realty shares a public key as the 'log in' of the mobile application, then the tenant uses its private key to log in, next RXR realty uses its private key to encrypt the code of the tenant and certifies the log in (Boneh, D., 1999). The RSA encryption is a secure cryptography broadly used in android apps, since it is a strong code and it enables efficient communication with multiple actors (Rabefaritra, K. M., & Rabevohitra, F. H., 2019). Next, Access control matrices are used to administrate which roles each group, list or person has. This means for example that each tenant can adjust their own agenda, but the employees do not have the right to adjust anything in the tenant's agenda (Sandhu, R. S., & Samarati, P., 1994). Lastly, the misuse intrusion detection is applied, to monitor if there is unusual behavior like wrong password enters or remarkable adjustments of personal information (Kim et al., 2014).

Risk 3: Insider risk: For RXR realty it is important to reduce the probability of the insider risks. Access control reduces the risk of violating security policies and unauthorized access (Bishop, M., & Gates, C., 2008). RXR realty needs to inform the employees about the consequences of certain actions by creating awareness by sharing additional information and giving workshops (Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M., 2019).

Risk 4: hacking database: RXR realty needs to secure their database, because it stores sensitive data of all their tenants. According to Anderson (2020), databases can be protected by the use of the following four layers: Management, Firewall, Intrusion detection and encryption. The management layer is responsible for keeping the applications up to date. Secondly a firewall needs to be used to protect the database for intruders. Thirdly an intrusion detection system needs to be put in place, because if the systems get breached intruders will be detected. Lastly the data in the databases need to be encrypted.

Risk 5: system overload: It is important to secure the RXR application against network attacks. System overload is harming the availability of the systems and applications. It is important to keep the systems up to date to prevent these attacks. (Anderson, 2020). According to McDowell (2009) denial of service attacks can be avoided by installing a firewall and restricting traffic coming into and leaving the environment. Lastly, intrusion detection systems can be used to monitor the traffic on the network.

Act

In the 'act phase' a new risk assessment for the digital transformation of RXR realty is created, by analyzing the result of the countermeasures to mitigate the identified risks. The risk analysis is done using the impact and likelihood of each risk shown in Table 6.

The OODA loop is a continuous model, so when 'the act phase' is ended all the used countermeasures and risks will be analyzed and reflected on. To do this a new term of the CIA model is applied 'auditability', which ensures that all the crucial information is stored for control measurements. As stated by Kupec (2017) 'The internal audit activity should monitor and evaluate the effectiveness of the enterprise's risk management system'. The auditability in this risk assessment will be executed by logging all the activities and processes of the digital transformation (Kupec, V., 2017). Also, all the exceptional events like for example detecting hackers or payments fraud need to be logged so they can later be analyzed to improve the current counter measurements.

Risk 1 - Payment fraud: The likelihood of payment fraud is strongly decreased, since all the payment communication is encrypted using AES encryption. Also, consequently updating all the systems contributes to reduce the impact, which eventually results in a likelihood of 2. The impact is reduced by using misuse detection systems which will immediately detect malicious attack and therefore minimizes the impact to 3. This will mainly have an impact on confidentiality.

Risk 2: Private agenda: Using RSA encryption users can safely log in, which reduces the likelihood of hacking or that other strangers have access to personal data. Additionally, access control defines which people have which responsibilities so only the rightful authenticated people have access to read or adapt the private agenda, which results in a likelihood of 2. The impact again is reduced by using the misuse detection system and therefore has an impact of 3.

Risk 3: Insider risk: The likelihood of insider risks is reduced by using access control, so only certified employees of RXR realty who signed a contract for these responsibilities have access to sensitive data. RXR realty also strongly informs all their employees about the consequences of misusing their responsibilities and therefore the likelihood is

reduced to 1. Currently, the impact is not reduced, as when the employees violate their contract terms they know exactly what the vulnerabilities of the company are, which results in an impact of 5.

Risk 4: hacking database: Hacking the database was the biggest risk of RXR realty. The probability of a hack will drastically decrease, by implementing a firewall, encrypting the files and keeping the programs within the system's update. The impact of the hack will decrease by the intrusion detection system, because the system can notice a hack. Therefore the impact has been decreased to 4 and the likelihood to 3.

Risk 5: system overload: RXR realty can strongly decrease the likelihood of a system overload, by keeping the apps up to date and implementing a firewall. The firewall will protect the online environment against intruders. In addition the intrusion detection system is decreasing the impact, because the attack can be identified in an earlier stage. For that reason the impact is decreased to 3 and the likelihood has been decreased to 2.

Impact						
Very high to certain	5					Risk 3
High to very high	4			Risk 4		
Middle to high	3				Risk 1 & 5	
Low to middle	2				Risk 2	
Zero to Low	1					
		5	4	3	2	1
				Likelihood		

Table 6. Risk assessment RXR Realty Post-Measures

See appendix for readable image

Conclusion

The report aims to mitigate the identified risks from the main report 'the road to adaptability in real estate' by applying countermeasures to reduce the likelihood and impact of each risk. Comparing the first risk assessment with the risk assessment including the countermeasures, the impact and likelihood of each risk decreases to the green zone in the model. Only risk 4 hacking the database still hits the yellow part of the model and therefore needs extra research for improvement. Overall, it can be concluded that the current countermeasures improve the confidentiality, integrity and availability of the digital transformation in RXR realty. In contrast, these theoretical results could differ from the real world, therefore applying auditability is important to log and monitor the processes, and so the countermeasures could be improved or extended if needed.

REFERENCES

Amadeo, K. (2020). Why Buying a Home Helps Build the Nation. *The Balance*. Retrieved 12 October 2020, from https://www.thebalance.com/how-does-real-estate-affect-the-u-s-economy-3306018.

Anderson, R. (2020). *Security Engineering* (3rd ed.). John Wiley & Sons., Hoboken, New Jersey

Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2018). Insider threat: The human element of cyberrisk. *McKinsey Quarterly*, 1-8. Retrieved 29 September from: https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

Barbanel, J., (2020). Market Value of New York Real Estate Shows Signs of Weakening. *The Wall Street Journal*. Retrieved 2 October 2020, from: https://www.wsj.com/articles/market-value-of-new-york-real-estate-shows-signs-of-weakening-11579442400

Barchard, K. A., & Pace, L. A. (2011). Preventing human error: The impact of data entry methods on data accuracy and statistical results. *Computers in Human Behavior*, 27(5), 1834-1839. doi: 10.1016/j.chb.2011.04.004

Barribal, E., George, K., Marcos, I., Radtke, P., (2020). Jump-starting resilient and reimagined operations. *McKinsey & Company*. Retrieved 2 October 2020, from: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/Jump%20starting%20resilient%20and%20reimagined%20operations/Jump-starting-resilient-and-reimagined-operations.pdf

Bertino, E., & Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and secure computing*, 2(1), 2-19. doi: 10.1109/TDSC.2005.9

Bishop, M., & Gates, C. (2008, May). Defining the insider threat. In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (pp. 1-3). *Association for Computing Machinery*, New York. Retrieved 3 October 2020 from: https://dl.acm.org/doi/10.1145/1413140.1413158

Boberski, M. (2010). The ten most critical Web application security risks. *Tech. rep., OWASP*. Retrieved 1 October 2020, from: https://owasp.org/www-project-top-ten/

Boneh, D. (1999). Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2),

203-213. Retrieved from: https://crypto.stanford.edu/~dabo/pubs/papers/RSA-survey.pdf

Boyd, J. (1987). A discourse on winning and losing [PowerPoint slides]. Retrieved from: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0151_Boyd_Discourse_Winning_Losing.PDF

Brehmer, B. (2005, June). The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control. In Proceedings of the 10th international command and control research technology symposium (pp. 365-368). Retrieved from: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf

Clarke, K. (2020). Covid-19 Pounds New York Real Estate Worse Than 9/11, Financial Crash. *WSJ*. Retrieved 2 October 2020, from: https://www.wsj.com/articles/covid-19-new-york-real-estate-11597939146.

Dunn, K. (2004). Automatic update risks: can patching let a hacker in? *Network Security Archive*, (7), 5-8. Retrieved from: https://www.semanticscholar.org/paper/Automatic-Updates%3A-Automatic-update-risks%3A-can-let-Dunn/d4064cbae100bf6de7bf226289a3fca3a1bd0d04

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644-654. Retrieved from: https://ee.stanford.edu/~hellman/publications/24.pdf

Gujral, V., Palter, R., Sanghvi, A., & Vickery, B. (2020). Commercial real estate must do more than merely adapt to coronavirus. *McKinsey & Company*. Retrieved 2 October 2020, from: https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/commercial-real-estate-must-do-more-than-merely-adapt-to-coronavirus.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys* (CSUR), 52(2), 1-40. doi: https://doi.org/10.1145/3303771

Kapodistria, H., Mitropoulos, S., & Douligeris, C. (2011). An advanced web attack detection and prevention tool. *Information Management & Computer Security*. Retrieved from: https://pdfs.semanticscholar.org/b778/443a7eacb66ae1d3d7fe928b9f38edb9e410.pdf

Kaspersky. (2019). Cybercriminals use smartphone calendars to distribute scam offers. Retrieved 1 October 2020, from: https://usa.kaspersky.com/about/press-releases/2019_cybercriminals-use-smartphone-calendars-to-distribute-scam-offers

Kazanavicius, E., Kazanavicius, V., Venckauskas, A., & Paskevicius, R. (2012). Securing web application by embedded firewall. *Elektronika ir Elektrotechnika*, 119(3), 65-68. doi: https://doi.org/10.5755/j01.eee.119.3.1366

Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690-1700. doi: 10.1016/j.eswa.2013.08.066

Krebsonsecurity. (2019). Sale of 4 Million Stolen Cards Tied to Breaches at 4 Restaurant Chains. Retrieved 1 October 2020, from: https://krebsonsecurity.com/2019/11/sale-of-4-million-stolen-cards-tied-to-breaches-at-4-restaurant-chains/

Kupec, V. (2017). Digital possibilities of internal audit. *Acta VŠFS-ekonomické studie a analýzy*, 11(1), 28-44.

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16-24. doi: http://dx.doi.org/10.1016/j.jnca.2012.09.004

McDowell, M. (2009). Cyber security tip st04-015-understanding denial-of-service attacks. *United States Computer Emergency Readings Team*. Retrieved from: https://us-cert.cisa.gov/ncas/tips/ST04-015

Nadella, S. (2020). 2 years of digital transformation in 2 months. *Microsoft*. Retrieved from: https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

Our Company | RXR Realty. (2020). Retrieved 2 October 2020, from https://rxrrealty.com/company

Pleyers, G., & Poncin, I. (2020). Non-immersive virtual reality technologies in real estate: How customer experience drives attitudes toward properties and the service provider. *Journal of Retailing and Consumer Services*, 57, 102175. doi: https://doi.org/10.1016/j.jretconser.2020.102175

Rabefaritra, K. M., & Rabevohitra, F. H. (2019, June). RemoteEncrypter: An Android Database Asymmetric Encryption Module. *In The ACM MobiSys 2019 on Rising Stars Forum* (pp. 13-18). Retrieved 4 October 2020 from: https://dl.acm.org/doi/10.1145/3325425.3329937

McKinsey & Company. (2020) Reimagining the real estate industry for the next normal. Retrieved 2 October 2020, from: https://www.mckinsey.com/about-us/new-at-mckinsey-blog/how-will-real-estate-be-different-in-the-next-normal.

RXR Lab | RXR Realty. (2020). Retrieved 2 October 2020, from: https://rxrrealty.com/lab

Safire, W. (2020). Location, Location, Location. *The New York Times magazine.* Retrieved 2 October 2020, from: https://www.nytimes.com/2009/06/28/magazine/28FOB-onlanguage-t.html

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. doi: https://doi.org/10.3390/fi11040089

Samonas, S., & Coss, D. (2014). THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. JISSec *Journal of Information System Security*, Volume 10, Issue 3. Retrieved from: http://www.proso.com/dl/Samonas.pdf

Santarelli, M., (2020). NYC Real Estate Market 2020 Overview. Norada. Retrieved 2 October, 2020 from: https://www.noradarealestate.com/blog/new-york-real-estate-market/

Securion pay. (2020). Everything you know about payment security. Retrieved 2 October 2020, from: https://securionpay.com/payment-security/#a1

Selvaraju, N., & Sekar, G. (2010). A method to improve the security level of ATM banking systems using AES algorithm. *International Journal of Computer Applications*, 3(6), 5-9.

Slot, R. (2019). Information Security Architecture Tilburg University [PowerPoint Slides]. Retrieved from https://tilburguniversity.instructure.com/courses/5141/pages/week-5-security-engineering?module_item_id=132511

Strawbridge G. (2019). 10 Biggest DDoS Attacks and how your organisation can learn from them. *Metacompliance.* Retrieved 1 October 2020, from: https://www.metacompliance.com/blog/10-biggest-ddos-attacks-and-how-your-organisation-can-learn-from-them/

Swinhoe, D. (2020). The 15 biggest data breaches of the 21st century. *CSO*. Retrieved 2 October 2020, from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web*, 16(4), 449-475. doi: https://doi.org/10.1007/s11280-012-0178-0

Weill, P., & Woodham, R. (2002). Don't Just Lead, Govern: Implementing Effective IT Governance. *SSRN Electronic Journal*. doi: https://doi.org/10.2139/ssrn.317319

Weill, P. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. *Harvard Business School Press*. Retrieved from: https://www.researchgate.net/publication/236973378_IT_Governance_How_Top_Performers_Manage_IT_Decision_Rights_for_Superior_Results

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017, August). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In 2017 international conference on engineering and technology (ICET) (pp. 1-7). *IEEE*. Retrieved 2 October 2020 from: https://ieeexplore.ieee.org/abstract/document/8308215

APPENDIX

Figure 1

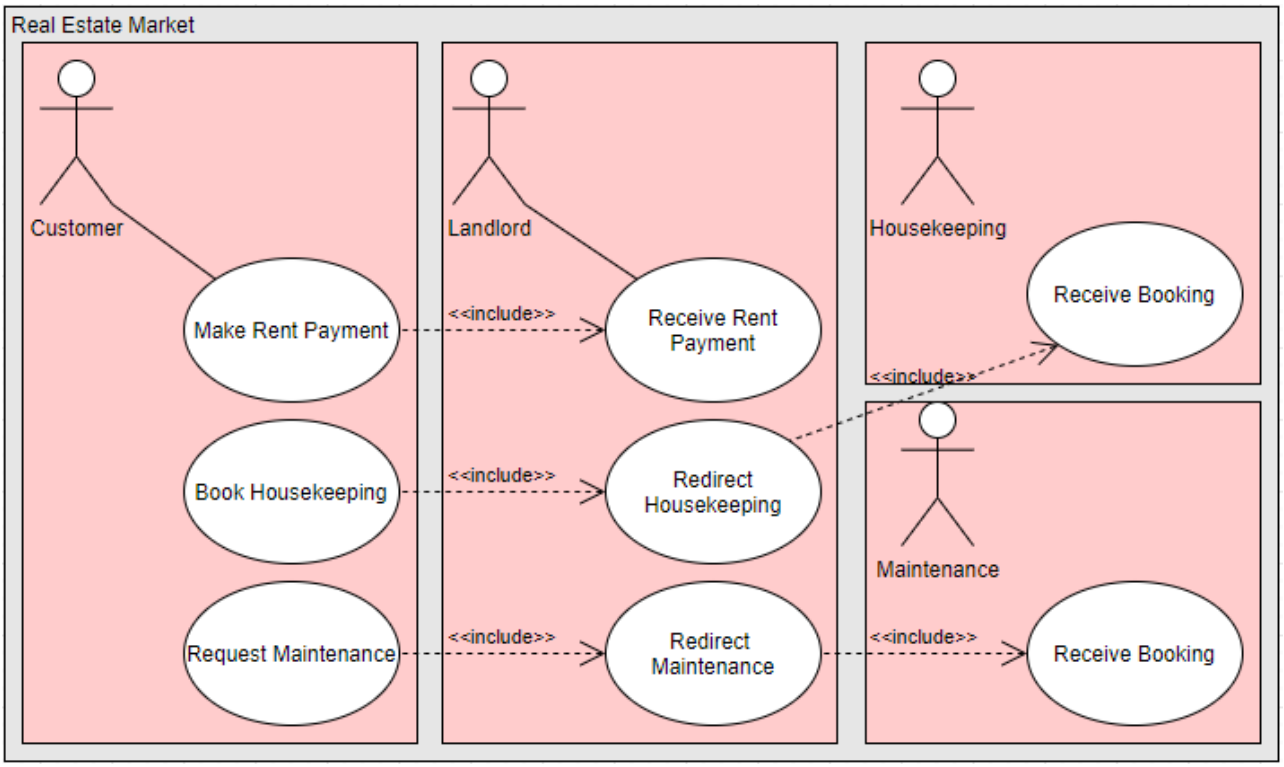

Figure 2

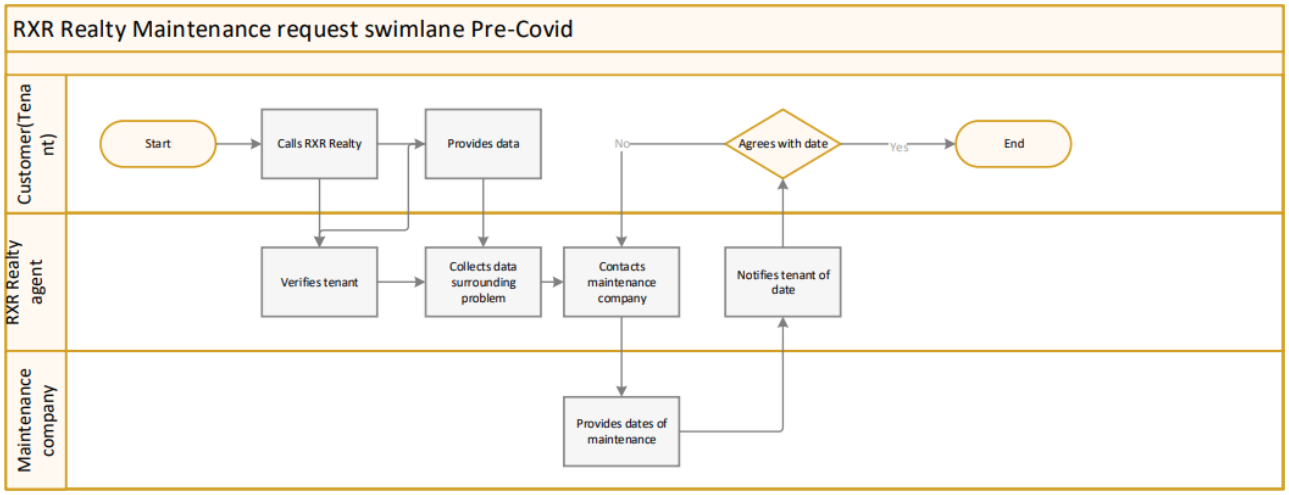

Table 1

Impact							
	Very high to certain	5					
	High to very high	4	Risk 2		Risk 3		
	Middle to high	3		Risk 1			
	Low to middle	2					
	Zero to Low	1					
			5	4	3	2	1
			Likelihood				

Table 2

	IT principles	IT architecture	IT infrastructure	Business application needs	IT investment and prioritization
Business monarchy					
IT monarchy		x	x		
Feudal					
Federal				x	
Duopoly	x				x
Anarchy					

Figure 4

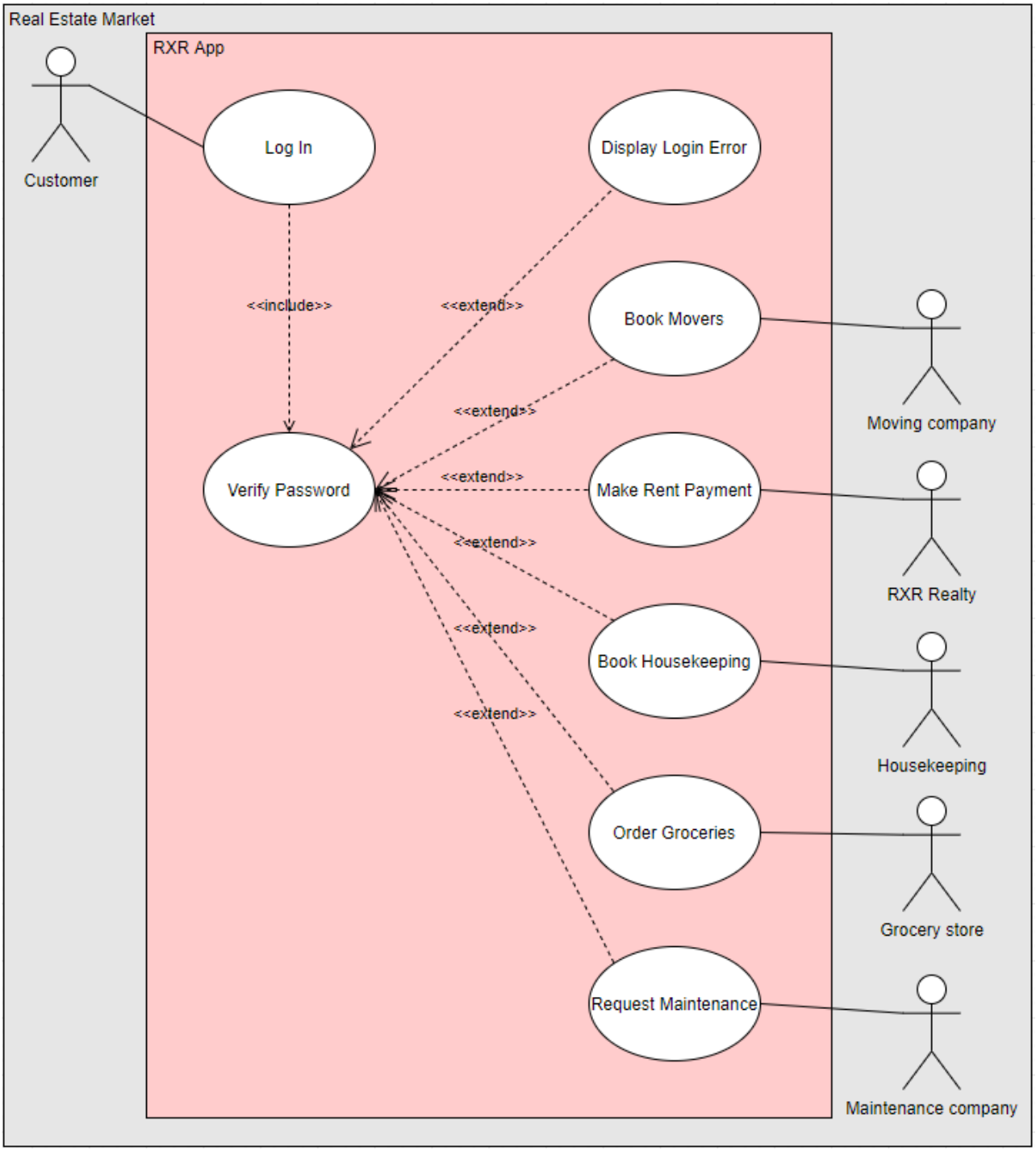
Real Estate Market
RXR App
Customer
Log In
Display Login Error
<<include>>
<<extend>>
Book Movers
Moving company
<<extend>>
Verify Password
<<extend>>
Make Rent Payment
RXR Realty
<<extend>>
<<extend>>
Book Housekeeping
Housekeeping
<<extend>>
Order Groceries
Grocery store
Request Maintenance
Maintenance company

Figure 5

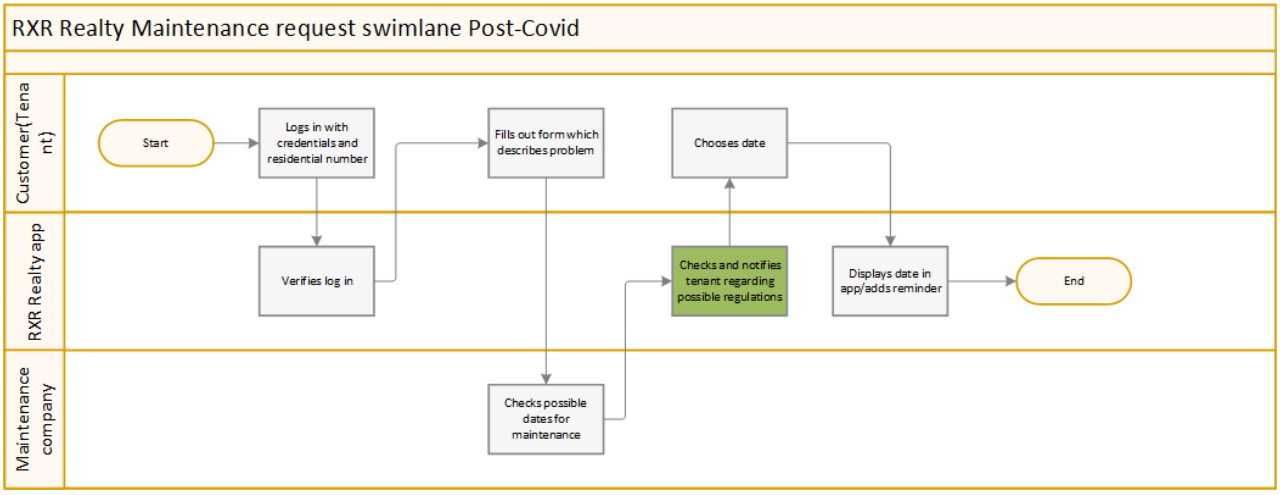

Table 3

Impact						
Very high to certain	5	Risk 4	Risk 3	Risk 1 & 2		
High to very high	4	Risk 5				
Middle to high	3					
Low to middle	2					
Zero to Low	1					
		5	4	3	2	1
		Likelihood				

Table 5

	IT principles	IT architecture	IT infrastructure	Business application needs	IT investment and prioritization
Business monarchy				x	x
IT monarchy		x	x		
Feudal					
Federal					
Duopoly	x				
Anarchy					

Figure 7

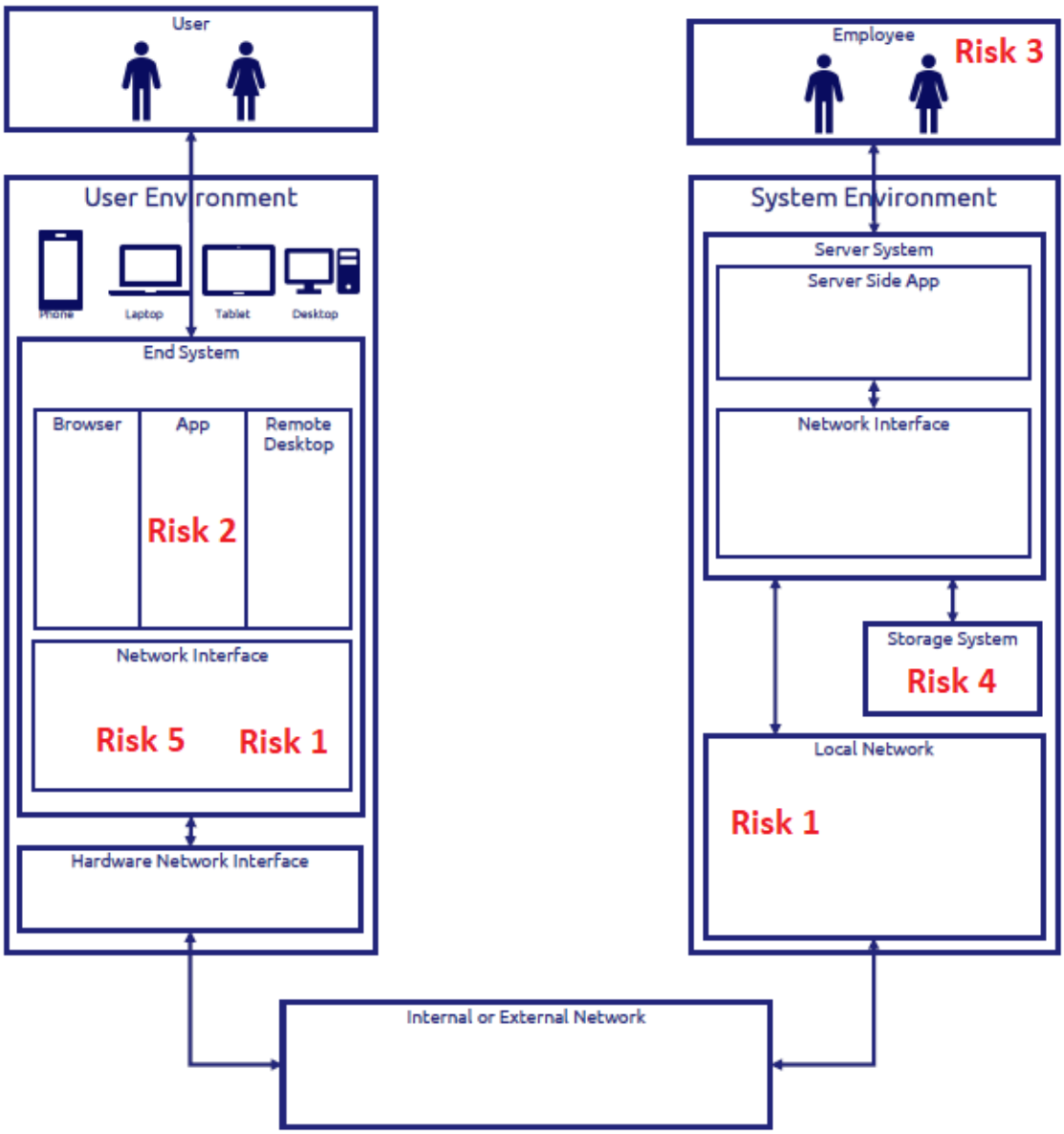
User
User Environment
Phone
Laptop
Tablet
Desktop
End System
Browser
App
Remote Desktop
Risk 2
Network Interface
Risk 5
Risk 1
Hardware Network Interface
Employee
Risk 3
System Environment
Server System
Server Side App
Network Interface
Storage System
Risk 4
Local Network
Risk 1
Internal or External Network

Figure 8

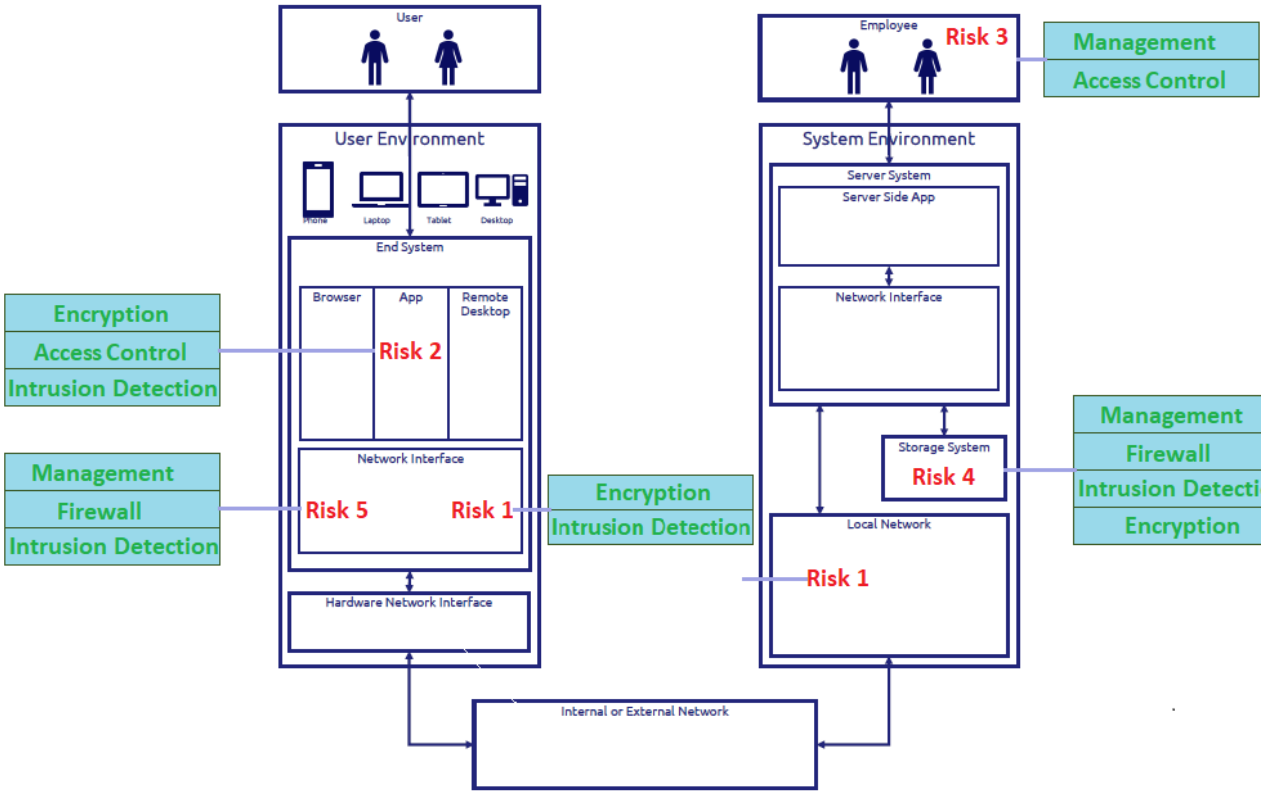

Table 6

Impact						
Very high to certain	5					Risk 3
High to very high	4			Risk 4		
Middle to high	3				Risk 1 & 5	
Low to middle	2				Risk 2	
Zero to Low	1					
		5	4	3	2	1
		Likelihood				