Planning Phase……….2

Project Identity………2

Methodology………….3

Business Requirements……….4

Prototyping………….4

Work Breakdown…….5

Analysis Phase……….5

Project Value…………6

Key Players………….8

Requirements……….16

Implementation…….16

UML Diagrams……….17

References……………18

The goal of this system design for Richard’s Building Supply is to meet the needs of customers and to be maintainable, efficient, and reliable. In addition, our system shall be produced in a way that meets project budgets and schedules and will be done in an economical fashion. This will not be an easy task because the system contains complex, large applications. To make this system successful our team will need to avoid issues we have faced in the past that caused previous project to fail such as over budgeting, the system being too difficult for users to use, performance not meeting our expectations, missing market windows and/or schedule delays, low quality, and not meeting customer requirements, inadequate test coverage, unrealistic project goals, and inaccurate estimates of needed resources. This system will require the coordination of our stakeholders who will be organized into teams. Their primary objective will be to build a system that will meet our defined requirements.

Here at Richard’s, we currently have 16 branches in six states on the east coast. We are a building supply company that caters to contractors and customers in the construction industry. We sell high end products that consist of asphalt roofing shingles, siding, windows, doors, decking, costagra, and many other building materials. We want to extend our services through custom installation of all these products. We will need a system where contractors and customers can order, buy, schedule appointments, and receive quality prompt service to supply their needs. Our qualified and certified professionals will deliver and install these products. Our mission statement is strategically and successfully deliver and install building materials to customers in a way that will positively impact and improve their quality of life. Our short-term goal is to slowly roll out this system in as little as six months and have this system completely active throughout our entire organization between one year to one year a half, to increase online orders by thirty percent within one year. Our critical success factors include involving our users, receiving support from our executives, clear business objectives, optimization, Agile processing, skilled resources, emotional maturity, and strong project management.

We will use is agile software development life cycle which is a structured series of stages that our system will cycle through as it moves from beginning to end. We will use an agile project management methodology which places value on individuals and interactions over processes and tools, response to change over following plans, customer collaboration over contract negotiation, and working software over comprehensive documentation. Our scrum teams will have clearly defined roles and work in sprints similar to iterations. During the concept phase the scope of our system will be defined and once that is underlined, it is time to build our software development team during the inception phase. In the construction phase our developers will combine system requirements and customer feedback and turn our system design into code. After testing our system will be ready for release. It will then be deployed and made available to our customers This system will require the coordination of our stakeholders who will be organized into teams. Their primary objective will be to build a system that will meet our defined requirements.

Here at Richard’s, we currently have 16 branches in six states on the east coast. We are a building supply company that caters to contractors and customers in the construction industry. We sell high end products that consist of asphalt roofing shingles, siding, windows, doors, decking, costagra, and many other building materials. We want to extend our services through custom installation of all these products. We will need a system where contractors and customers can order, buy, schedule appointments, and receive quality prompt service to supply their needs. Our qualified and certified professionals will deliver and install these products. Our mission statement is strategically and successfully deliver and install building materials to customers in a way that will positively impact and improve their quality of life. I think prototyping this system is a good idea as well. This will allow the users to “test-drive” the system and give feedback. Their feedback can then be used to validate user requirements or to help formulate the final product. Agile development methods may be used as well, which will entail the developers building a series of prototypes and constantly making revisions according to user requirements and feedback received from users. Benefits include a reduced risk that the finished system will fail to support our organizational needs. Managers can evaluate the model and gain a better understanding with a working model. And prototyping will aid in avoiding misunderstandings. However, prototyping and developing the system at a rapid pace may reduce quality. A prototype may become difficult to manage if the system is complex. Note that reliability and maintainability cannot be tested accurately while prototyping.

Our business requirements consist of:

* The need to identify slow- or fast-moving building supplies so our inventory department can manage our building supply inventory more efficiently.
* We need accurate recordkeeping and timely order processing so management can better equip staff so they can provide effective crane operators and installers scheduling, up-to-date inventory, and efficient appointment scheduling.
* We need prompt notification of any security issues so IT can mitigate any security threats that may arise in a timely, cost-effective manner.
* We need effective training provided to all internal users of the new system to provide effective and efficient service to customers.
* We need a simple yet adequate interface for the cashier system for ease-of-use for our cashiers.

For work breakdown refer to chart in appendices.

* Our store managers need accurate and up-to-date reports from system developers to accurately assess the TCO of the new RBS system.
* Our owners need concise strategic objectives in place to make the new system run smoothly.

We will send our questionnaires to our staff for feedback and any concerns they may have about the new system. We will also conduct one-on-one interviews in a neutral setting because I believe our staff will be more honest with how they are feeling, requirements they may need and their concerns.

What are the benefits of the new system?

Text

Description automatically generated

Timeline

Description automatically generated

A picture containing table

Description automatically generated

Diagram

Description automatically generated with low confidence

Diagram

Description automatically generated

Key Players

At Richard’s we believe people are our most important resource on a systems project because through their efforts the project is successfully constructed and delivered. They are the lifeline of a successful project and as such competent staff must be recruited, motivated, trained, and provided will a path for potential growth.

Business management’s focus is profit, market competitiveness, customer satisfaction, and cost effectiveness. They are not typically involved in the technicalities of the new system. Business management includes development managers, marketing, and senior management.

Planning and tracking of the project are handled by project managers. They proactively implement improvements and changes throughout the project to make certain the project is within budget and on schedule.

Software development includes documentation, testing, configuration management, implementation, design, and architecture, and this is all handled by the development team. This team is responsible for maintaining and development of the system.

The customers are interested in a system that is cost-effective and meets their business needs but also is of high quality. They interact in specifying requirements.

The end users interact with the system after it is developed. They want a product that is easy to use and helps them perform their area of expertise efficiently.

Our IT department requires the most information and security is of the utmost importance. “Men do not attract that which they want, but that which they are. Their whims, fancies, and ambitions are thwarted at every step, but their inmost thoughts and desires are fed with their own food, be it foul or clean. Man is manacled only by himself; thought and action are the jailors of fate—they imprison, being base; they are also the angels of freedom—they liberate,” (Allen, 2003). The risk of cybersecurity incidents severely increases as companies around the world increase their analysis capabilities, storage, and data collection. Cyber criminals or hackers utilize a plethora of hacking styles to acquire access to data stores and infrastructure, taking advantage of network vulnerabilities, insufficient IT security frameworks, and human error.

A passive approach to risk management may leave companies open to being exploited and data theft, which can diminish their productivity and dissolve their reputation. We must constantly review our security standards and stay on top of new IT developments to neutralize the threat of data breaches and ransomware. “A 2019 report from Accenture found that the average cost of cybercrime for an organization increased $1.4 million from the previous year and now falls around $13 million in total. According to the National Institute of Standards and Technology, information security is defined as “the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability,” (Certitude Security, 2020). We achieve this objective by establishing strategies for managing security risks, IT policies, and internal processes.

” Confidentiality, integrity, and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The elements of the triad are considered the three most crucial components of security,” (Rouse, 2020). The overall goal of data confidentiality is to “protect data against unintentional, unlawful, or unauthorized access, disclosure, or theft. Confidentiality has to do with the privacy of information, including authorizations to view, share, and use it,” (Delaware, 2020). When managing confidentiality, we should consider who data will be disclosed to, will contracts, regulations, or laws require data to remain confidential, and will data only be in use under certain conditions. Also, we will consider the sensitivity of data, will there be a negative impact if disclosed, and will the data be invaluable to hackers or others who are not permitted to have it. Our guidelines for data confidentiality entail the encryption of sensitive data, data access management, data acquisition management, proper and secure disposal of paper records, devices, and data, physically securing paper documents and data, data utilization management, and device management. Data integrity is an essential component and entails maintaining the accuracy, consistency, and trustworthiness of data. It is designed to protect data from being altered by any unauthorized users. The final part of the triad refers to the availability of data and is best insured by maintaining the hardware, by performing hardware repairs, and managing the functionality of the operating system environment that does not contain software conflicts. Software or security equipment such as proxy servers and firewalls will be a defense against blocked data by DoS, unnecessary downtime, and intrusions. Our information infrastructure will be secured by using a Defense in Depth approach which is a series of security mechanisms and controls layered throughout the computer network that protects the CIA triad (confidentiality, Integrity, and Availability) of the network and data. To be effective the Defense in Depth may include tools, policies, and best practices such as patch management, strong passwords, the principle of least privilege, network segmentation, Endpoint Detection and Response (EDR), Intrusion Prevention or Detection Systems, (IDS/IPS), and Firewalls.

There is no magical solution to cybersecurity, but Defense in Depth and the CIA triad will help defend against network vulnerabilities, insufficient IT security frameworks, and human error. We must establish strategies to manage IT policies, internal processes, and security risks.

Our end users such as outside sales and appointment setters will work remotely.

In this ever-changing world, security threats are constantly changing. As these threats evolve compliance requirements become more and more complicated. These challenges force companies to implement extensive security programs, and without security policies in place trying to enforce a security program is unachievable. Remote access control is the ability to control and oversee access to networks or computers. Our employees will have the ability to work remotely away from the office or organization while retaining access to business networks or computers. “Deploying remote access control provides a secure connection. It minimizes the risk of data theft or loss and malicious activities since you are controlling the connection, therefore not allowing unknown entities to access private or corporate data” (Yfantis, 2018). People are finding increased productivity with the flexibility of “telecommuting.” It is imperative that our organization implements an information security policy to not only ensure employees and others follow security protocol, but to ensure the safety of our company’s data from new threats and security breaches. Our ISP or information security policy will be a guide that IT users in our organization will use to guide our company’s assets. Our information security policy will contain a broad overview of our organization’s network architecture. Our ISP outlines how our organization should react when encountering unauthorized use and includes instructions on acceptable and unacceptable use. The purpose of the information security policy is to ensure that employees and other affiliated users follow security protocol and procedures properly. Keeping an updated security policy ensures that only authorized users can access sensitive information. Creating, updating, and ensuring compliance of our security policy is a vital step in securing the prevention and mitigation of security breaches. Continuous updates to company changes means more effectiveness when new threats arise, and what better way to improve upon a security policy than to draw from previous breaches. To better understand how to increase productivity while maintaining organizational security with an effective remote access policy, we have to understand its role in an organization. According to Gallup’s State of the American Workplace report currently, at least 43% of workers in the U.S. work remotely at least part of the time (Hickman Ph.D., 2019). It has been reported that remote workers have higher job satisfaction and flexibility, have higher production rates, and experience less interruptions and distractions. In turn, organizations are experiencing less absenteeism, far greater employee retention, as well as less stress on office accommodations. Organizations are finding that remote workers are logging more hours away from the office and saving money on commuting expenses. Companies are saving on office space expenses also. The increase in usability and availability of remote accessibility services via mobile devices or personal computers allows access outside of firewall and physical wall protections of organizations draws a plethora of confidentiality, connectivity, and information security issues. These challenges jeopardize sensitive information by way of inappropriate or unauthorized use and may lead to compliance issues from statutes issued from Payment Card Industry Data Security Standards (PCIDSS) or Health Insurance Portability and Accountability Act (HIPAA). Damages incurred may also come in the form of theft, espionage, or accidental exposure of IP. “According to the U.S. Department of Commerce, intellectual property (IP) accounted for $5.06 trillion in value added, or 34.8 percent of U.S.

GDP in 2010. In May 2013, the Commission of the Theft of American Intellectual Property released a report that concluded that the scale of international theft of American intellectual property is roughly $300 billion per year and 2.1 million additional jobs in our economy” (Kahn, 2017). One instance of an information security breach is the massive hack of the federal government’s personnel office traced back to China, that compromised the data of more than 20 million Americans. Our remote access policy is a subsection of our network security policy, which presents the policies and rules for access to our organization’s network. Security controls for laptops are different for those of other devices so the policy must entail what is secure, compliant, and allowed.

Since I am discussing our information security policies with an emphasis on our remote access sub section, I will incorporate what should be included in our remote access policy with the elements of an information security policy.

The first element of the policy is the overview. The overview is basically an introduction and gives a broad view of what the policy will entail.

The purpose section of the policy is next and should give an understanding of why the policy is necessary. The objective of the policy should be defined clearly. Maintaining confidentiality, ensuring availability, and maintaining integrity should be a priority and stated in the purpose as an objective. The organization’s purpose may be to create and implement an overall approach to remote access control as it relates to information security policy. The purpose may be to uphold legal and ethical responsibilities, as well as maintain the reputation of the company. The purpose of a remote access policy as it pertains to information security policy is to detect information security breaches, how to respond to complaints concerning noncompliance, and respecting customers rights.

Our organization is enormous and will contain a lot of contracts, third party, and dependencies so, the scope of whom the policy pertains should be established and made clear early on. It should also contain what is in scope and what is out of scope.

“Cheng described the violation of information security policy in organizations. The results of the study revealed that employees with a stronger bond to their organization are less likely to deviate from policies and participate in delinquent behavior (Cheng et al., 2013). Policy compliance are goals that an organization sets to encourage employees/members to comply with the organization’s policies. Our remote access policies should include guidelines for access that may include the following:

* Password protocols
* Guidelines for connectivity
* Access privileges, hierarchy, and authentication
* Virtual and physical device security
* Encryption policies
* Confidentiality, information security, and email policies
* Software and hardware configuration standards for remote access
* Equipment ownership and access requirements
* Policy compliance, enforcement, and governance
* Third-party standards and protections

Controls are set in place and policy compliance is used to validate the controls that are set.

Related standards are standards that directly correlate to the remote access policy or information security policy. Some of which include:

* Personal and mobile devices
* Privacy regulations
* Data security policy
* Acceptable use policy
* IAM regulations
* SaaS and cloud policy
* Security incident response plan
* IT administration and operations

The definitions section is important because there are so many people within our organization with various roles. There will be a lot of language and lingo that will be foreign to employees/members in different departments, so it is imperative that the various terms are defined, because you want the policy to be as transparent as possible.

Making our information security policy effective requires a few key elements. It should be enforceable and practical, cover security from all angles across the organization, as well as focus of the business goals of the company. “Previous studies have revealed that employees’ information security awareness plays a vital role in mitigating the risk associated with their behavior in organizations” (Abawajy, 2014). Security is an essential part of remote access control and ensuring the safety and confidentiality of our organization’s data when connecting to an organization’s network from a users’ private server.

As I stated earlier, we should avoid certain obstacles if we want our system to be successful. These obstacles include over budgeting, the system being too difficult for users to use, performance not meeting our expectations, missing market windows and/or schedule delays, low quality, and not meeting customer requirements, inadequate test coverage, unrealistic project goals, and inaccurate estimates of needed resources. This system will require the coordination of our stakeholders who will be organized into teams. Their primary objective will be to build a system that will meet our defined requirements.

I think if we have the right technology like a workplace sign-in system we will benefit. We will be able to track visitors, staff, synchronize data, and have better visibility across our multiple locations. I think we need to invest in streamlining and automating processes by leveraging a workplace management solution to eliminate bottlenecks, and time-consuming processes. We must focus on immediate goals and marketing strategies. We must also focus on core strengths and embrace strategic planning.

I think a star topology is best because we can manage every node from one central switch and our central hub will be a server which will manage data transmissions across the entire network. The setup is simple, and we can add new computers without taking the network offline.

Although online processing will work well because it handles transactions in real time. It also requires lots of staff to maintain inventory, hardware problems create issues, and tons of requests become difficult to handle. I think batch processing is better because it handles large amounts of data that are processed on a routine schedule. Batch processing requires less training, hardware, and programming resources. Batch systems can work offline. However, it can be costly.

We will roll out our new system using the pilot operation changeover. We will implement the new SIM system in our Virginia Beach branch first while the old system will still be in use. After the system proves successful the direct cutoff method will be implemented. This changeover method is less costly than direct cutoff and parallel operation methods and we will avoid major errors.

Appendix A

ERD

Diagram

Description automatically generated

Work Breakdown

Graphical user interface, text, application, email

Description automatically generated

References

Allen, J. (2003). *As a Man Thinketh.* United Kingdom: Axiom Publishing.

*Certitude Security*. (2020). Retrieved from Certitude Security: https://www.certitudesecurity.com/blog/analysis-and-assessments/why-its-important-to-have-information-security-standards/

Delaware, U. o. (2020). *Managin Data Confidentiality*. Retrieved from https://www1.udel.edu/security/data/confidentiality.html

Rouse, M. (2020). *WhatIs.com*. Retrieved from TechTarget Network: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Yfantis, V. (2018). *What is Remote Access Control?* Retrieved from: <https://www.parallels.com/blogs/ras/remote-access-control/>

Hickman, A. (2019). *How to Manage Remote Employees*. Retrieved from: <https://www.gallup.com/workplace/263510/manage-remote-employees.aspx>

Kahn, R. (2017). *Economic Espionage in 2017 and Beyond: 10 Shocking Ways They are Stealing Your Intellectual Property and Corporate Mojo.* American Bar Association. Retrieved from: <https://www.americanbar.org/groups/business_law/publications/blt/2017/05/05_kahn/>

Abawajy J. (2014). *User Preference of Cyber Security Awareness Delivery Methods:* Behavior of Technology, pp. 236-237. Retrieved from: <https://doi.org/10.1080/0144929X.2012.708787>

Cheng L. (2013). *Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory.* Pp. 447. Retrieved from:<http://dx.doi.org.ezproxy.liberty.edu/10.1016/j.cose.2013.09.009>