UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE

Red Clay Renovations

A case study for CSIA 413

Valorie J. King, PhD

3/30/2016

Table of Contents

Tables

Figures

Company Overview

Red Clay Renovations is an internationally recognized, awarding winning firm that specializes in the renovation and rehabilitation of residential buildings and dwellings. The company specializes in updating homes using “smart home” and “Internet of Things” technologies while maintaining period correct architectural characteristics. The company’s primary line of business *is Home Remodeling Services* (NAICS 236118).

Corporate Governance & Management

Red Clay Renovations was incorporated in the State of Delaware in 1991 and is privately held. (Its stock is not publicly traded on a stock exchange.)The company maintains a legal presence (“Corporate Headquarters”) in Delaware to satisfy laws relating to its status as a Delaware corporation. The company has a five member Board of Directors (BoD). The Chief Executive Officer (CEO) and Chief Financial Officer (CFO) each own 25% of the corporation’s stock; both serve on the BoD. The CEO is the chair person for the BoD. The three additional members of the BoD are elected from the remaining stock holders and each serve for a three year term. The BoD provides oversight for the company’s operations as required by state and federal laws. Its primary purpose is to protect the interests of stockholders. Under state and federal law, the BoD has a fiduciary duty to ensure that the corporation is managed for the benefit of the stockholders (see http://www.nolo.com/legal-encyclopedia/fiduciary-responsibility-corporations.html). The BoD has adopted a centrally managed “Governance, Risk, and Compliance” (GRC) methodology to ensure that the corporation meets the expectations of stakeholders while complying with legal and regulatory requirements.

The company’s senior management includes the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Operating Officer (COO), Director of Architecture & Construction Services (A&C), Director of Customer Relations (CR), Director of Human Resources (HR), the Director of Information Technology Services (ITS), and the Director of Marketing and Media (M&M). The Director of ITS is dual-hatted as the company’s Chief Information Security Officer (CISO). These individuals constitute the Executive Board for the company and are responsible for implementing the business strategies, policies, and plans approved by the BoD. A separately constituted IT Governance Board is chaired by the Chief Operating Officer. The five directors (A&C, CR, HR, ITS, and M&M) serve as members of the IT Governance board. This board considers all matters related to the acquisition, management, and operation of the company’s information technology resources.

The CEO, CFO, and COO have been with the company since it started in 1991. The Directors for A&C, CR, and HR have over 20 years each with the company. The Director for M&M has ten years of service. The Director of ITS / CISO has been with the company less than two years and is still trying to bring a semblance of order to the IT management program – especially in the area of IT security services. This is a difficult task due to the company’s failure to promptly hire a replacement for the previous director who retired two years ago.

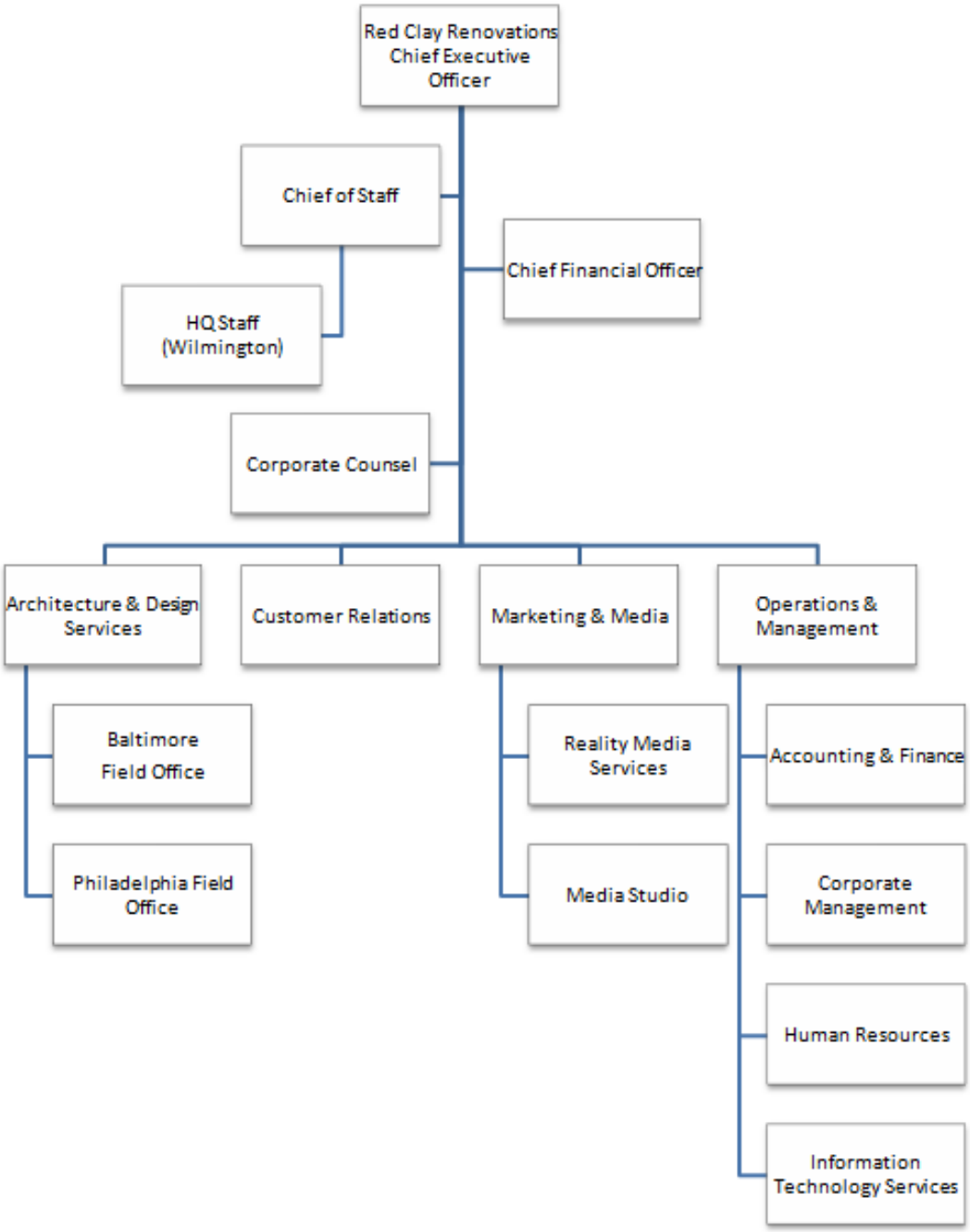

Figure 1. Red Clay Renovations Organization Chart

Table 1. Key Personnel Roster

Name & Title	Office Location	Office Phone No.	email
James Randell CEO	Wilmington	910-555-2158	jr@redclayrenovations.com
Irma Bromley Executive Assistant to Mr. Randell	Wilmington	910-555-2150	Irma_Bromley@ redclayrennovations.com
Nancy Randell Chief of Staff	Wilmington	910-555-2152	nr@redclayrenovations.com
Marcus Randell CFO	Wilmington	910-555-2159	marcus@redclayrenovations.com
Julia Randell COO	Owings Mills	667-555-5000	julia@redclayrenovations.com
Edward Randell, Esq Corporate Counsel	Wilmington	910-555-1000	ed@redclayrenovations.com
Erwin Carrington CIO & Director IT Services	Owings Mills	667-555-6260	Erwin_Carrington@hq.redclayrenovations.com
Eric Carpenter CISO / Deputy CIO	Owings Mills	667-555-6370	Eric_Carpenter@hq.redclayrenovations.com
Amanda Nosinger Director, Customer Relations	Owings Mills	667-555-6400	an@redclayrenovations.com
Rebecca Nosinger Director, Marketing & Media	Ownings Mills	667-555-6900	rn@redclayrenovations.com
Eugene Nosinger Director, Architecture & Services	Owings Mills	667-555-8000	en@redclayrenovations.com
Charles Kniesel Manager & Architect in Charge, Baltimore Field Office	Baltimore	443-555-2900	Charles@balt.redclayrenovations.com
Erica Kniesel Office Manager & ISSO, Baltimore Field Office	Baltimore	443-555-2900	Erica@balt.redclayrenovations.com
William Kniesel Manager & Architect in Charge, Philadelphia Field Office	Philadelphia	267-555-1200	William@philly.redclayrenovations.com
Alison Kniesel-Smith Office Manager & ISSO, Philadelphia Field Office	Philadelphia	267-555-1200	Alison@philly.redclayrenovations.com

Operations

Red Clay Renovations has offices in Baltimore, MD, Philadelphia PA, and Wilmington, DE. The contact information for each location is provided in Table 2.

Table 2. Red Clay Renovations Office Locations & Contact Information

Location	Mailing Address	Phone Number
Baltimore Field Office	200 Commerce Street, Suite 450 Baltimore, MD 21201	443-555-2900
Philadelphia Field Office	1515 Chester Street Philadelphia, PA 19102	267-555-1200
Operations Center (Owings Mills)	12209 Red Clay Place Owings Mills, MD 21117	667-555-6000
Wilmington Office	12 High Street Wilmington, DE 19801	910-555-2150

The Operations Center is the company's main campus and is located in suburban Baltimore, MD (Owings Mills). The Owings Mills facility houses the company's data center as well as general offices for the company's operations. These operations include: accounting & finance, customer relations, human resources, information technology services, marketing, and corporate management. There are approximately 100 employees at the Operations Center. Day to day management of the Owings Mills facility is provided by the company's Chief Operating Officer (COO).

The company's Chief Executive Officer, corporate counsel, and support staff maintain a presence in the company's Wilmington, DE offices but spend most of their time at the Owings Mills operations center.

Field Offices are located in downtown Baltimore and suburban Philadelphia. Each office has a managing director, a team of 2-3 architects, a senior project manager, a business manager, and an office manager. Support personnel (receptionist, clerks, etc.) are contractors provided by a local staffing services firm. Each office operates and maintains its own IT infrastructure.

The company's architects, project managers, and other support personnel frequently work from renovation sites using cellular or WiFi connections to access the Internet. Many field office employees are also authorized to work from home or an alternate work location ("telework site") one or more days per week.

Acquisitions

Red Clay acquired "Reality Media Services," a five person digital media & video production firm in 2015 (NAICS Codes 512110, 519130, and 541430). RMS creates a video history for each residential

construction project undertaken by Red Clay Renovations. RMS also provides Web design and social media services for Red Clay Renovations to promote its services. RMS employees work primarily out of their own home offices using company provided equipment (computers, video / audio production equipment). Each employee also uses personally owned cell phones, laptops, digital cameras, and camcorders. While RMS is now wholly owned by Red Clay, it continues to operate as an independent entity. Red Clay senior management is working to change this, however, starting with bringing all IT and IT related resources under the company's central management. As part of this change, Red Clay has set up a media production facility ("Media Studio") in its headquarters location which includes office space for RMS personnel. The production facility and RMS operations are under the management control of the Director, Marketing & Media Services.

Legal and Regulatory Environment

The firm is licensed to do business as a *general contractor* for residential buildings in three states (DE, MD, PA). The company's architects maintain professional licensure in their state of residence. The company's general counsel is licensed to practice law in Delaware and Maryland. The Chief Financial Officer is a Certified Public Accountant (CPA) and licensed to practice in all three states.

The company collects, maintains, and stores personal information from and about customers over the normal course of doing business. This includes credit checks, building plans and drawings for homes, and information about a customer's family members which needs to be taken into consideration during the design and construction phases of a project (e.g. medical issues / disabilities, hobbies, etc.).

When renovations are required due to a medical condition or disability, the company works with health insurance companies, Medicare/Medicaid, and medical doctors to plan appropriate modifications to the home and to obtain reimbursement from insurers. This sometimes requires that the company receive, process, store, and transmit Protected Health Information (PHI) generated by medical practitioners or as provided by the customer. The company's legal counsel has advised it to be prepared to show compliance with the HIPAA Security Rule for PHI for information stored on computer systems in its field offices and in the operations center.

Red Clay began offering "Smart Home" renovation services in 2005 (NAICS Codes 541310 and 236118). These services are primarily offered out of the Baltimore and Philadelphia field offices. A large percentage of the company's "smart home" remodeling work is financed by customers through the Federal Housing Administration's 203K Rehab Mortgage Insurance program. Red Clay provides assistance in filling out the required paperwork with local FHA approved lenders but does not actually process mortgages itself. Red Clay does, however, conduct credit checks on prospective customers and accepts credit card payments for services.

As a privately held stock corporation, Red Clay Renovations is exempt from many provisions of the *Sarbanes-Oxley Act of 2002*. But, in certain circumstances, i.e. a government investigation or bankruptcy

filing, there are substantial criminal penalties for failure to protect business records from destruction or spoliation.

Policy System

The company's Chief of Staff is responsible for the overall organization and management of the company's collection of formal policies and procedures ("policy system"). The company's policies provide guidance to employees and officers of the company (CEO, CFO, and the members of the Board of Directors) with respect to their responsibilities to the company. Policies may be both prescriptive (what "must" be done) and proscriptive (what "must not" be done). Responsibility for writing and maintaining individual policies is assigned to a designated manager or executive within the company. Each policy identifies the responsible individual by title, e.g. Director of Human Resources.

The major policy groupings are:

- Human Resources
- Financial Management
- Information Technology
- Employee Handbook
- Manager Deskbook

Selected policies are published as an Employee Handbook and a Manager's Deskbook to communicate them to individual employees and managers and to ensure that these individuals are aware of the content of key policies which affect how they perform their duties.

Risk Management & Reporting

The company engages in a formal risk management process which includes identification of risks, assessment of the potential impact of each risk, determination of appropriate risk treatments (mitigation, acceptance, transfer), and implementation of the risk management strategy which is based upon the selected risk treatments. For information technology related risks, the CISO working in conjunction with the IT Governance Board is responsible for identifying and assessing risks.

Corporate-wide, high level risks which could impact the company's financial performance are disclosed to shareholders during the annual meeting and in the *Annual Report to Investors*. For the current year, the following high level cybersecurity related risks will be disclosed.

1. Cyber-attacks could affect our business.
2. Disruptions in our computer systems could adversely affect our business.
3. We could be liable if third party equipment, recommended and installed by us (e.g. smart home controllers), fails to provide adequate security for our residential clients.

The company's risk treatments for cybersecurity related risks include purchasing cyber liability insurance, implementing an asset management and protection program, implementing configuration baselines, implementing configuration management for IT systems and software and auditing compliance with IT security related policies, plans, and procedures.

The corporate board was recently briefed by the Chief Information Officer concerning the company's IT Security Program and how this program contributes to the company's risk management strategy. During the briefing, the CIO presented assessment reports and audit findings from IT security audits. These audits focused upon the technical infrastructure and the effectiveness and efficiency of the company's implementation of security controls. During the discussion period, members of the corporate board asked about audits of policy compliance and assessments as to the degree that employees were (a) aware of IT security policies and (b) complying with these policies. The CIO was tasked with providing audit reports for these items before the next quarterly meeting of the corporate board.

The corporate board also asked the CIO about future plans for improvements to the IT Security program. The CIO reported that, in the coming year, the CISO will begin implementation of an IT vulnerability management program. The CIO also reported that the CISO is working with the IT Governance Board to restart the company's security education, training, and awareness (SETA) program. SETA activities had fallen into disuse due to a perceived lack of quality and lack of timeliness (out of date materials). The CISO has also determined that the System Security Plans for the field offices are out of date and lacking in important security controls. These plans have been scheduled for update in the near future to ensure that the company's risk management strategy for cybersecurity risks is fully implemented.

IT Security Management

The company's Chief Information Security Officer (CISO) is responsible for providing management oversight and technology leadership for the company's Information Technology security program. This program is designed around the ISO 27001/27002 requirements but is not fully compliant. For cost reasons, the Chief Information Officer (CIO) has decided not to pursue implementation of CobiT or ITIL standards for managing IT systems and services. A less costly alternative, using NIST guidance documents, was approved at the CISO's suggestion. The CISO's selected guidance documents include:

- NIST SP 800-12 "An Introduction to Computer Security: The NIST Handbook:
- NIST SP 800-18 "Guide for Developing Security Plans for Federal Information Systems"
- NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-100 "Information Security Handbook: A Guide for Managers"
- NISTIR 7621 "Small Business Information Security: The Fundamentals"

The CISO has determined that the closest fit for the level of security required by law for the company's IT systems is the "moderate level" as defined in the FIPS 199/200 standards and specified in NIST SP

800-53 Revision 4. The company has created its own minimum security controls baseline which is used for developing system security plans.

Under the company's existing *IT Security Management Plan*, the following individuals are responsible for the security of its IT systems.

1. Chief Information Officer: designated approving official for all IT systems certification and authorization.
2. Chief Information Security Officer: responsible for developing security plans and procedures.
3. Chief Financial Officer: responsible for negotiating and providing oversight for contracts and service level agreements for IT services.
4. Chief Operating Officer: responsible for approval of and compliance with security plans and procedures for the company's IT Operations Center. The COO is the *system owner* for all IT systems in the operations center.
5. Field Office Manager: responsible for approval of and compliance with security plans and procedures for his or her field office. The field office manager is the *system owner* for all IT systems in his or her field office.
6. Field Office Information Systems Security Officer (ISSO): responsible for day to day implementation of security plans, processes, and procedures.

Information Technology Infrastructure

Enterprise Architecture

The overview for the enterprise IT architecture for Red Clay Renovations is shown in Figure 2. This diagram shows the interconnections between the company's field offices and the operations center. Each facility-to-facility interconnection is made via a Virtual Private Network (VPN). The VPN connects the Local Area Networks (LANs) in the operations center and the field offices to the company's enterprise network. All IT systems are in the *operational* phase of the Systems Development Lifecycle. The company does not have plans at this time to upgrade ("major modification") or implement ("under development") any IT systems.

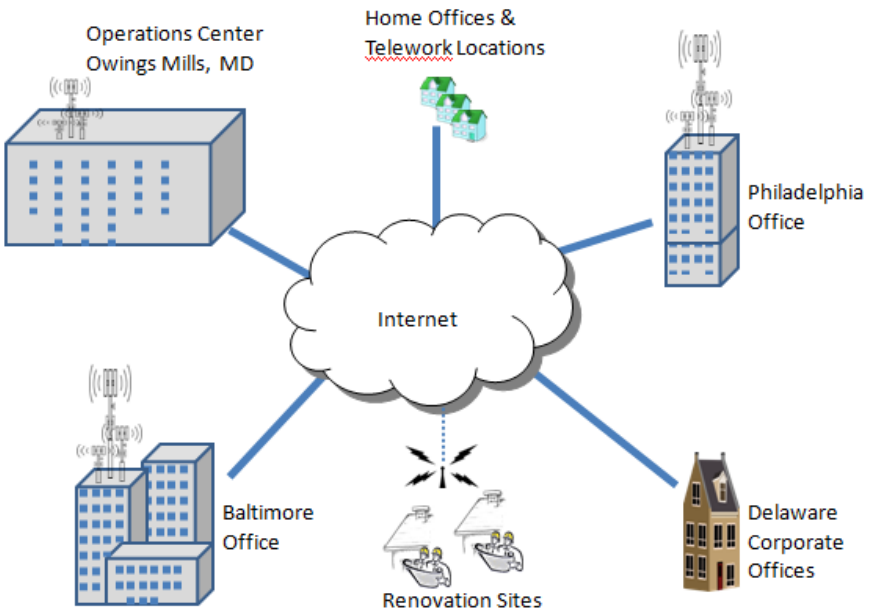

Figure 2. Overview for Enterprise IT Infrastructure

Operations Center IT Architecture

The Owings Mills facility (see Figure 3) contains the company's operations (data) center as well as general offices for the company's operations. These operations include: accounting & finance, customer relations, human resources, information technology services, marketing, and corporate management.

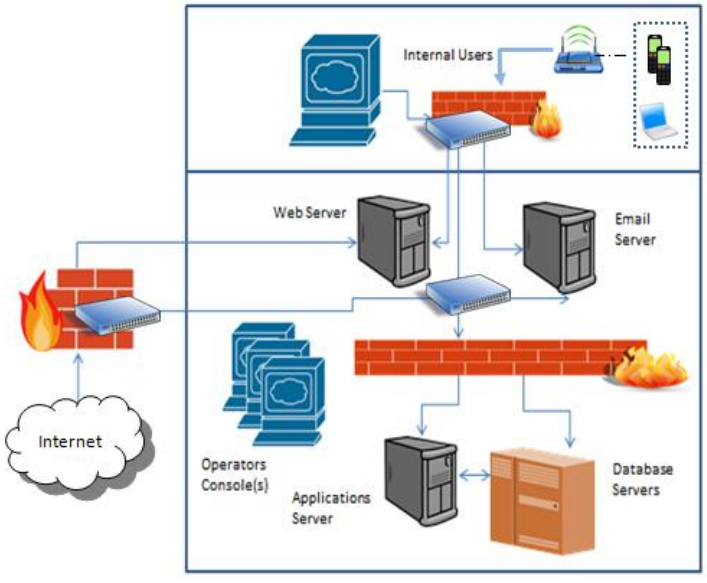

Figure 3. IT Architecture for Operations Center

Field Office IT Architecture

The company's corporate headquarters are located in Wilmington, DE. These offices have the same IT architecture as is used by the field offices in Baltimore and Philadelphia (see Figure 4). The company's Chief Executive Officer and support staff maintain a presence in Delaware but spend most of their time at the Owings Mills operations center. The company's architects, project managers, and other support personnel frequently work from renovation sites using cellular or WiFi connections to access the Internet. Many field office employees, including "Reality Media Services" staff, are also authorized to work from home or an alternate work location ("telework site") one or more days per week.

Red Clay's offices have been remodeled to use the "smart home" and "Internet of Things" technologies which it installs in the residential buildings that it rehabilitates. These devices have IP addresses and are connected to the in-office wireless network (WiFi). Each smart device has a controller which can be accessed via a Web-based interface that runs on the office's application server (username and password required). The brand and type of equipment varies. The majority of these devices have little to no security beyond a password protected Web-based logon. Every Red Clay location also has one or more conference rooms which provide "smart" podiums, projection and video conferencing technologies, and wireless network access to both the internal network and the Internet.

All locations use Dell computers for laptops, desktop computers, and servers. The laptops and desktops were recently upgraded to Windows 10 Enterprise for their operating systems. The servers are running Windows server 2012. All Windows systems have Symantec Endpoint Protection installed for host-based security (anti-malware, host-based firewall, host-based intrusion detection).

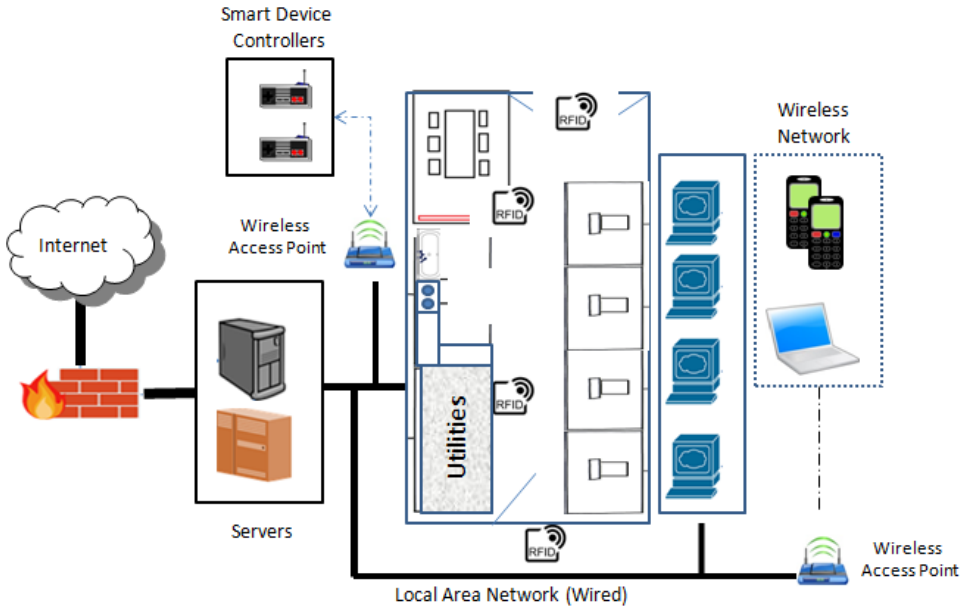

Figure 4. "Smart" Office IT Architecture (Baltimore, Philadelphia, Wilmington)

Each field office uses the same logical architecture. This infrastructure consists of a local area network with both wired and wireless segments. A wiring closet containing the premises router and switches is located in the office space (labeled "Utilities" in the diagram). The "smart office" and "IoT" devices are also located within the office suites and are connected via WiFi to the Wireless Access Points and from there to the office LAN. These devices are individually addressable via their IP addresses. Some have onboard programmable controllers with Web based interfaces. Others have limited onboard functionality and must be controlled via a central console (which has an IP address and Web based interface). The RFID system used to control access to doors has sensor plates affixed to the walls. These sensors are hard wired to a controller in the utilities closet. This controller connects to the local area network and can be accessed via a Web based interface using its IP address. Access control for the Web based interfaces (used for RFID system and "smart" device control) is limited to password protected logons.

System Interconnections

The Operations Center and the individual Field Offices connect to the Internet via a business grade Internet Services Provider with a standard Service Level Agreement (as established by the ISP). Systems interconnections between internal systems and between facilities are certified and approved by the Chief Information Officer. These interconnections include Virtual Private Network connections between the Operations Center and the Field Offices over ISP provided networks). The VPN is used to protect the confidentiality and integrity of information transmitted between IT systems located in the company's field offices, its headquarters, and the operations center. (See *Information Technology Infrastructure* later in this document for additional information about system interconnections.)

The operations center and field offices each have their own network infrastructure built on CISCO branded equipment (Virtual Private Network (VPN), wired and wireless local area networks, wireless access points, switches, a premise firewall, and intrusion detection system). Offices and server rooms have RJ-45 wall jacks for 100BaseT "wired" connections to the local area network. Network equipment serving individual LAN segments is located in locked equipment closets ("wiring closets") within the office areas.

The company's Wide Area Networking (WAN) and Internet services are provided by Verizon Business services. These services include static IP addresses for the company's network connections and domain name service for the company's primary domain name (RedClayRenovations.com) and multiple third level domain names (e.g. balt.redclayrenovations.com, philly.redclayrenovations.com, etc.). The company owns, operates, and manages its own Active Directory server, multiple Web servers, Email servers, file and print servers, and multiple application /database servers. These servers are accessed via local area network (LAN) and virtual private network (VPN) connections. The Email and public Web servers are located in a protected network segment (Demilitarized Zone AKA DMZ) and are accessible from both internal and external networks.

Verizon provides fiber optic cables to the building demarc. Internally, the company owns the cable infrastructure and has predominantly Cat 5 cabling inside the buildings. Company owned cabling also runs from the Verizon owned demarc to a company owned/maintained central wiring closet. This closet also contains routers and switches serving the internal LANs.

Telephone service is provided to each office building via fiber optic cables (as part of the FiOS business services). Internal to the buildings, telephone service routes through an Alcatel Private Brach Exchange (PBX) system over ANSI/TIA/EIA-568-B compliant wiring (predominantly Cat 3 cabling). The PBX system does not connect to the company's internal networks.

The company allows employees to bring and use their own personal digital devices (laptops, cell phones, cameras, etc.) provided that these devices are required to perform their duties. Contract employees are not allowed to "bring your own device" (BYOD) and will be terminated if they are found to be using cell phones or personal computers on the company's premises. Employees carry an RFID enabled "proximity access" card which they use to access offices and other restricted areas. BYOD devices are NOT allowed to connect directly to the company's VPN. These devices are restricted to WiFi access to the Internet using the company's wireless access points.