Investing in Information Security: A Case Study in Community Banking

Wes Earnest

Investing in Information Security: A Case Study in Community Banking

GIAC (GSEC) Gold Certification

Author: Wesley Earnest, wes.earnest@gmail.com
Advisor: Chris Walker
Accepted: August 6, 2016

Abstract

Small businesses, such as community banks, often do not have resources dedicated to information technology, much less resources dedicated to information security. Despite larger financial institutions having more resources to invest in information security, they are also attempting to secure much larger, more complex environments. Community banks, with a smaller footprint of computer systems and networks, have the opportunity to produce even greater results with a comparatively smaller investment. This case study shows how one small community bank enjoyed the successes of transitioning from an environment of constant reactionary troubleshooting to implementing an information security strategy that focused not only on improving the information technology environment but also business operations and regulatory compliance for the bank.

1. Introduction

Financial institutions are an obvious target for cyber criminals. At the end of 2015, the sum of assets held by all commercial banks in the US totaled $15.5 trillion dollars (Federal Reserve, 2015). The too-big-to-fail megabanks account for the biggest percentage of these dollars, but there is another segment of the market that often gets less attention, community banks. Community banks in the US hold $3.8 trillion in assets, $3.1 trillion in deposits, and $2.6 trillion in loans to consumers, small businesses and the agricultural community (ICBA, 2015). In contrast to the megabanks that tend to place a priority on serving large corporations, community banks focus primarily on the needs of local families, businesses, and farmers.

While community banks share a strong connection with the communities they serve, small banks are often the underdog when it comes to competing with large financial institutions. In recent years, the number of small banks in the US has declined 27 percent, while the market segment for large banks has increased 32 percent during this period (Pierce, 2015). Community bankers are constantly looking for ways to build brand loyalty and stay relevant in an increasingly more competitive and challenging marketplace. One of the key challenges facing all financial institutions is the struggle to keep up with the threat of cyber-attacks.

"Cyber security is critical to any business enterprise, no matter how small. However, leaders of small businesses often do not know where to begin, given the scope and complexity of the issue in the face of a small staff and limited resources" (US-CERT, *n.d.*). Community banks are no different. Many community banks do not have a full-time employee (FTE) dedicated to information technology (IT), much less an FTE dedicated to information security (InfoSec). Many community banks believe they do not have enough computer infrastructure to justify the expense of an extra person for so few systems. However, sixty percent of consumers surveyed believe small businesses are not as cyber secure as bigger organizations (KPMG, 2016). This public perception creates a disadvantage for community banks and an even greater urgency for community banks to

find a solution that will allow them to stay competitive in the ever-changing cyber landscape.

Conventional wisdom would favor the ability of larger organizations to build a team of security specialists, keep up to date with the latest innovations in information security and implement complex mouse traps to detect and stop cyber attackers. According to retired General Keith Alexander, "Your small and medium-sized companies cannot afford a world-class cyber threat team" (Koppel, 2016). A recent news story also stated, "[It] is definitely the case that these smaller banks are weaker links in the global financial system. Part of the problem is small banks don't have response teams and fancy detection software like the big banks do." (Shahani, 2016). While it is true that many small banks fall into this mold, it is not necessarily the case that small banks are destined to this fate.

For community banks to remain competitive with larger rivals and provide the level of information security necessary, they must question this conventional wisdom. Securing a smaller environment should be an advantage over securing a larger environment because there are fewer systems to protect. The total resources required to secure the smaller environment should also cost less than achieving the same level of security in a larger, more complex environment. The problem is not that community banks cannot afford the talent and systems to achieve world class results. The problem for many organizations is that they simply do not possess the experience and expertise needed to make informed decisions about the risks they face and how best to protect their data. All too often the most convenient uninformed decision made is the passive decision to maintain the status quo.

2. A Case Study in Community Banking

Smalltown Community Bank was established in the late 1800s. At the end of 2015, it had grown to just over $150 million in assets. Its main office and drive-through locations are staffed by a total of 30 employees. Both locations are situated in a rural community with a population of about 2,800 residents. Defined by a 25-mile radius, the bank's service market includes 20 small communities totaling 37,000, and a single

metropolitan of approximately 45,000. Over 90% of the bank's customers reside within this service market. The board of directors is comprised of four members of the bank's management team and three outside directors. The average age of the directors is 59 years, and historically, the average tenure has been about 24 years. The bank has enjoyed the success of continued growth and consistent profits for 21 of the past 22 years. This environment is typical for many community banks, and one that often produces a conservative and risk-averse culture, set on doing things "the way we've always done it".

2.1. A Catalyst for Change

In 2012 *Smalltown Community Bank* hired its first employee with professional experience in information technology and information security. Up until this point, the bank had no true strategy for IT or InfoSec. Technology, both software and hardware, had been pieced together over many years through an ad-hoc acquisition process. This created an environment of disjointed technologies and poorly integrated processes. Information necessary to run the bank required manual input into multiple systems, via processes prone to errors and inconsistencies. The bank relied mainly on its software vendors and outside contractors to implement and maintain this technology which the bank relied on for day to day operations. Resolving issues often meant contacting multiple vendors and allowing remote access which usually led to ad-hoc system changes or manual manipulation of data, only to alleviate the current symptoms.

First impressions of this environment revealed a very reactionary mindset focused on getting the day's work completed before quitting time. The main problem with this approach was that no one was truly responsible for evaluating the risks imposed on the bank as a whole. The software vendors understood the functionality of their own systems, but they were certainly not experts in cyber security. In most cases, these vendors lacked even a basic understanding of vulnerability assessments or secure coding principles. The contractors hired to implement and maintain the servers and network equipment understood those technologies well, but were not experts in bank operations, regulatory requirements or the latest cyber threats affecting the bank's overall security.

In situations like this, there is a tendency for someone new to the environment to rush in and start making changes in hopes of fixing evident problems. While this is a

noble effort, it often causes more problems than it fixes because there is an inherent lack of knowledge of how and why things were implemented in the first place, and along with that, an inherent shortsightedness of the potential impact of these changes. To avoid this pitfall, IT and InfoSec practitioners should focus on understanding the needs of the business and adopt a systematic approach to change management. In this case, the bank chose the Visible Ops framework to stabilize the patient, find fragile artifacts, establish a repeatable build library, and enable continuous improvement (Kim, 2004). Over the course of the four years from 2012 through 2015, *Smalltown Community Bank* enjoyed the successes of transitioning from an environment of constant reactionary troubleshooting to implementing an information security strategy that focused not only on improving the information technology environment but also business operations and regulatory compliance for the bank.

2.2. Defining Who You Are

A very strong self-identity existed at *Smalltown Community Bank*. With over 100 years of success and a rich history supporting the local community, the bank had built a relationship and culture of trust with its customers. Unfortunately, this success and trust also created a culture of complacency with little thought to the impact of emerging risks brought on by changes in technology and technology vendors. Decisions about which technologies to implement and which vendors to trust were made based on references from other community banks, or often the recommendations of the vendors themselves. Because so many community banks operate this same way, this status quo paradigm became a self-reinforcing mantra based on past success.

For an information security strategy to be successful, controls must be implemented to protect the confidentiality, integrity and availability of critical data. But before these controls can be implemented, an informed decision should first be made about what controls are necessary. The bank's senior management and board of directors must become more engaged in this decision-making process and actively consider what information is needed to perform this task. "FinTech, cyber-security, IT resilience and technology implications of regulatory changes have all become critical board-level issues but many bank boards simply don't have adequate expertise to assess these issues and

make decisions about strategy, investment and how best to allocate technology resources" (Accenture, 2015). It can be easy for seemingly risk-averse banks, lacking this technology expertise, to unconsciously accept undue risk simply by not having the capability to identify the risk in the first place. This is no excuse. "The board and senior management are responsible for understanding the risks associated with existing and planned IT operations, determining the risk tolerance of the institution, and establishing and monitoring policies for risk management" (FFIEC, 2004). Though this may seem like a daunting challenge for community banks, developing a culture of continuous improvement, challenging the status quo, and seeking out training opportunities are the foundation necessary for building the expertise on which good decisions can be based.

2.2.1. Investing in Information Security Expertise

In order for *Smalltown Community Bank*'s decision-making process to benefit from "adequate expertise", the bank first had to invest in obtaining that expertise. The two most common ways to approach this are either contracting with a consultant or hiring an in-house employee with the necessary skill set in IT and InfoSec. Regardless of where this expertise comes from, the crucial factor is that the bank appoints a qualified candidate to the role responsible for understanding the end to end risks of the existing and planned IT operations, and can communicate the risks to senior management and board of directors, who are ultimately accountable. In smaller organizations without a team of security experts, this role requires a unique ability to engage both strategically from a high level, but also technically at the network and systems level.

For *Smalltown Community Bank*, the first step was hiring someone with a professional background in technology. The second step was investing in training and technical certifications to stay informed about the ever-changing cyber threat landscape. While this will represent an increased expense for most small community banks, the question should not be simply 'how can we justify this expense?' but rather 'how can this new role be leveraged as a capability to generate value for the organization?' Answering this question requires examining the bank's culture to see whether it is ready to transition from the past mindset of "this is the way we have always done it," to a new model of continuous improvement. Training and certifications are a way to prove not how much

an individual knows, but how much he or she is willing to learn. Investing in training and certifications not only develops the technical expertise the organization relies on for informed decision making, it also provides an unbiased recognition of credibility with senior management, external auditors, and bank examiners.

2.2.2. Communicating with the Executive Team

It is essential for IT and InfoSec practitioners to establish and maintain communication channels with senior management to equip the decision makers of the organization with the information they need to make good decisions. For many community bankers, engaging in a dialog about IT strategy or the risks of cyber security may seem intimidating and outside the comfort zone of normal bank operations. Only 6% of board members and 3% of CEOs at the world's largest banks have professional technology experience (Accenture, 2015). A unique opportunity exists to surpass these larger rivals by developing the capability to integrate technical expertise into the bank's risk assessment and decision-making processes. However, IT and InfoSec practitioners must recognize that failing to implement the proper communication strategy with senior management will likely result in failure to obtain approval for projects needed to manage risk and improve information security.

Bridging this communication gap is a critical step in steering the organization's culture away from passively maintaining the status quo toward actively recognizing and managing these risks. The more involved that IT and InfoSec departments become in this process, the more influence they can have on priming the decision-making environment. "Our thoughts and our behavior are influenced, much more than we know or want, by the environment of the moment" (Kahneman, 2011). Just as securing the bank's confidential data requires designing and implementing a defensible infrastructure, designing and implementing an effective communication strategy positively influences the culture of the organization, and ultimately the decision-making environment.

For *Smalltown Community Bank*, this communication process began by raising awareness of the weaknesses and risks posed by the current IT environment. Following the Visible Ops principles, recurring issues and root cause analysis were discussed with the IT committee. These discussions were then documented in the IT risk assessments

and committee meeting minutes which were submitted to the monthly board meetings. This provided an opportunity to contrast the current state of the environment with the perceived level of security the bank had trusted in for so many years. It was also effective to share additional information with senior management, such as news articles on recent breaches or regulatory changes related to information security, along with an analysis of how these risks could impact the bank. Further efforts were made through one on one conversations with senior management about how unmanaged risks could be leveraged by attackers, and how these risks seemed to contradict the conservative self-image of the bank.

Many of the conversations with senior management relied on the use of analogy to draw comparisons from the physical world into the world of technology. One simple example relates the bank's core banking system (i.e. the mainframe where all of the customer account data is stored), to the physical vault which stores the cash. In most cases, the board of directors is aware of the cost of the things such as the physical vault, the building itself, and maybe even the alarm system for monitoring attempts to break into the vault. In comparison, the board may not have considered the security of this core system, what technical vulnerabilities exist, what vendors have physical access to the server, or even remote electronic access to the data. This analogy can also be used to point out that the physical vault only stores a small percentage of the bank's total assets, while the core system represents access to every dollar of every customer.

From the perspective of the IT or InfoSec practitioner, the ability to influence the decision-making process at the board level may seem beyond the scope of one's daily responsibilities. However, if there is a requirement for the board of directors to understand the risks involved in IT operations, then there is an equal responsibility for IT and InfoSec personnel to present information and ideas to senior management and the board of directors in a way that is easily understood. Unfortunately, only 1 in 10 security leaders have successfully made this transition from technology expert to business risk manager and can effectively communicate IT risks to business peers (Symantec 2012). This again speaks to the importance of establishing a solid communication strategy with senior management and building credibility.

2.2.3. Competitive Advantage

While the Symantec report paints a dim outlook with only 10% of technology experts transitioning to the role of business risk manager, the transition is not complicated. It primarily involves taking the time to understand the needs of the organization and its users. Because this is not a technical skill, many IT and InfoSec practitioners fail to see the importance of developing soft skills, such as communicating with senior management. However, it is precisely this intersection of both technical expertise and soft skills that creates the ability to identify the risks and potential solutions which will create the most value for the organization. "The fastest way to master any area of life, is to become good at two or more areas, intersect them in a unique way, and now you are the best in the world at the intersection" (Altucher, 2015).

All too often, decisions points are framed in such a way that senior management must weigh the opportunity costs of information security with competing priorities such as investment in new business opportunities. Instead of looking at these business decisions as either-or propositions, this idea of intersection provides a way to integrate the advantages of multiple solutions into something new (Martin, 2009). *Smalltown Community Bank* applied this same concept in its approach to risk assessment by identifying not only risks to information security but also searching for solutions where improvements in information technology intersect with a business opportunity and regulatory compliance.

The goal of a successful information security strategy involves more than just implementing a checklist of technical controls to reduce risk. Instead, it means understanding the risk tolerance of the organization and which activities generate value for the organization. Constantly searching for opportunities to question the status quo, or ask whether there is a better way to accomplish the bank's mission leads to a better understanding of business operations, and develops a culture of continuous improvement. Combining these technical and non-technical factors into the risk assessment process provides the information necessary for making informed decisions. When choices are presented as business opportunity or regulatory compliance questions, informed decisions become much easier for senior management to make.

3. Building Momentum

Although the transition from technology expert to business risk manager is not complicated, it can be a very slow process. Implementing change is not an easy task in any organization. It requires a patient and persistent effort to become involved in understanding business operations. Building consensus and support for what may seem like obvious decisions to improve security can be frustrating at times. Understanding the benefit of planning, testing and implementing small changes with clear rollback strategies is important for IT and InfoSec practitioners to continue down the path of credibility and partnership with business operations. This is why developing a culture of continuous improvement is so critical. Implementing small changes over time will result in a successful overall defense-in-depth information security strategy. The following three examples are just a sampling of the many changes that *Smalltown Community Bank* successfully implemented between 2012 and 2015.

3.1. Implementing 15 Character Passwords

During the first half of 2012, the most common help desk request was resetting user passwords. Even in a small office of only 30 users, it was common to receive multiple password reset requests per day for various applications. Each of these requests represented a loss of productivity for both the end user and IT based on the time spent waiting for the user account to be unlocked, a new temporary password to be assigned, and the user creating a new password. It was also common during this time to find user passwords on sticky notes taped to the underneath side of keyboards or mouse pads which presented a security risk. Since the bank could not reduce or eliminate the eight character password requirements mandated by the FFIEC banking regulations, it would be easy to accept the status quo as inevitable.

The IT committee recognized that business productivity, regulatory requirements, and password security improvements all needed to be addressed in any potential solution. Based on the hypothesis that longer passphrases would be easier for users to remember and type, senior management agreed to test the feasibility of enforcing fifteen character passwords for Active Directory user accounts. The goal was to manage the risk of lost productivity caused by account lockout and forgotten passwords as well as increase

security by using passwords with higher entropy (Strand, 2012). This change also represented an opportunity to build credibility with bank regulators during audits and examinations of the bank's security policies, further reducing compliance risk by going beyond just the minimum requirements.

Another factor considered when implementing this change was the culture of the organization. Given the environment of repeated requests for password resets, there was a strong possibility that increasing the minimum length to fifteen characters would only exacerbate the issue. However, *Smalltown Community Bank*'s results were vastly different than those in a study later published by NIST, which concluded that increasing the minimum length would lead to password fatigue and further loss of productivity (NIST, 2014). In the year following this change, password reset requests dropped by 97% for Active Directory accounts, indicating that users spend less time struggling to remember and type eight character complex passwords. During this same time, some legacy applications with a six or eight character password limit still produced continual reset requests.

Even though the solution may seem counter-intuitive, this represented a very low-cost experiment with minimal downside risk, and a worthwhile benefit to the organization if successful. If productivity loss increased, it would have been very simple to roll back to the old password settings. Changing from eight character passwords to fifteen character passwords may only be a minor improvement in overall security. However, this small technical change provided an opportunity to engage the entire organization in security awareness training, and its successful implementation paved the way for larger, more substantial future changes.

3.2. Implementing Virtual Desktops

In 2012, *Smalltown Community Bank* began to focus on the Windows XP end of support date scheduled for April 2014. At the time, the bank had a diverse mixture of workstations consisting of various makes and models, most of which the hardware maintenance had expired. Many of these systems were pieced together from spare parts as hardware failures became more frequent. The easiest solution may have been to purchase new workstation hardware and Windows 7 operating system (OS) licenses.

Instead, the IT committee began searching for solutions that would provide additional value beyond the basic life cycle management of workstations.

The first step was to identify and communicate the risk of managing the workstations in the current environment. The challenges included managing asset inventory, OS and application security patches, configuration drift, users with local administrator access, shared accounts and passwords, licenses for the OS and installed applications, hardware failures and incident response. Next, a baseline cost estimate was compiled for the new hardware and OS licenses. Several systems management tools were also investigated to see if a solution existed to solve these challenges. During this research, the idea of implementing virtual desktop infrastructure (VDI) began to emerge as a possible solution.

In 2011, the bank had started the process of virtualization by converting a few aging physical servers to virtual machines. The VMWare environment had been designed with spare capacity for future virtualization. This created an opportunity to utilize the existing environment for VDI as well. VDI provided a solution for most of the risks that had been identified. Managing asset inventory would be simplified by replacing the diverse workstation hardware with standardized zero client terminals. Patching the OS and applications would be managed through VMWare's linked clone technology where changes are implemented on a single base image and then propagated to user desktops. Using the linked clones also provided an effortless way to revert back to the base image on a regular interval, eliminating configuration drift. The negative impact of hardware failures would be minimized by running the user desktops in a fully redundant VMWare cluster.

Migrating from physical to virtual desktops also presented the perfect opportunity to test and implement several security changes by removing local administrator access for all users and locking down the workstations using a principle of least privilege. In a small environment of only 30 employees, performing multiple roles is necessary for business operations. In the past, this meant setting up shared accounts for users to access workstations configured for specific job functions. Shared accounts and passwords were also eliminated by allowing users the ability to log into their assigned desktop from any

location throughout the bank. Incident response procedures were updated from the previous method of attempting to clean suspect workstations and minimizing user impact, to a more thorough method of deleting a suspect virtual desktop and provisioning a brand new virtual desktop from a known clean base image within a matter minutes.

The cost differences between the VDI implementation and the physical workstations were negligible, but the flexibility of the VDI solution created much more value for the organization. The downside risk was whether all of the legacy applications and peripheral devices would function correctly in an entirely virtual environment. To manage this risk, extensive testing was conducted before the final solution was purchased. Testing consisted of installing each application, deploying a test image to end users of each department, allowing them to test the changes, then installing the next application and repeating the process. These steps were conducted in a very controlled manner, involving end users at each step to test every change to generate buy-in from end users and ensure that performance would meet the users' needs. Although the process of researching and testing every user application was time-consuming, it was also an opportunity for the IT staff to develop a deeper understanding of business operations and each employee's role within the bank. Once the testing was completed, the options were presented to senior management for the decision on which solution to choose. This effort resulted in an environment where 100% of the bank's employees utilize a VDI desktop as their primary workstation.

3.3. Implementing Network Segmentation

When a system is compromised, one of the first things an attacker will do is check to see what other systems are connected to the same network by scanning all of the IP addresses in that subnet and then attacking those systems. Detecting this type of malicious activity can be difficult, so it is critical for organizations to understand and define what "normal" traffic looks like on its network. To accomplish this level of visibility, networks must be designed in such a way to collect and analyze the traffic. Network segmentation is not an easy concept for most bankers to understand. Discussions with senior management included physical analogies to explain the risks

inherent in the single monolithic internal network that contained all of the bank's systems.

The first analogy compared a blueprint of the bank's physical office building to a drawing of the bank's network topology. The problem becomes clear when the internal walls are removed from the drawing of the office. When the office walls are removed, confidentiality is at risk from eavesdropping. Taking away the restroom walls also takes away privacy. Removing the walls of the vault also removes the security of the assets inside the vault. In a situation without interior walls, all of the bank's cash is metaphorically sitting in a large public lobby. The same problem exists when segmentation is not properly implemented in the bank's internal networks.

The second analogy compared the bank's security camera system to the monitoring capabilities of the bank's managed intrusion prevention system (IPS). Having only one IPS monitoring the external internet connection would be the same as having only one video camera at the main entrance to the bank. There would be no way to see what each person did after they entered the bank, only the fact that someone entered or exited the building. A recent study shows that it typically takes organizations 146 days to detect that their network has been breached (Mandiant, 2016). Implementing better network segmentation creates a business opportunity for the bank to reduce that 146 days as much as possible. The security camera analogy allowed senior management to recognize that they would not hire a vendor to work on equipment in the bank's vault and leave that person unattended without video surveillance of the cash. However, there were multiple vendors with remote access to the bank's computers without the ability to monitor this network traffic. Implementing network segmentation would provide a way to track and record vendor connections.

While there are no regulations that stipulate how internal networks should be segmented, there are regulatory requirements for banks to understand the flow of traffic within its network. "Management should also develop data flow diagrams to supplement its understanding of information flow within and between network segments as well as across the institution's perimeter to external parties" (FFIEC, 2004). Once these data flows are documented, it is easy to question the status quo by asking why unrelated

systems, such as the digital signage in the lobby, have the ability to communicate directly with the core banking system or automated teller machine.

Implementing network segmentation represented another low-cost change as existing equipment could be reconfigured to meet the requirements. The decision to create additional subnets and VLANs and split systems up into corresponding segments was largely transparent to the end users, yet it involved a much higher risk to bank operations. In order to minimize the potential impact to end users, extensive research and monitoring had to be conducted. There were three major steps to implementing this change, monitoring existing traffic, implementing host-based firewalls, migrating systems to new VLANs and subnets. Monitoring and analyzing the traffic was accomplished utilizing a combination of BroIDS, Enterprise Log Search and Archive (ELSA), and host-based firewall logs to document all known good traffic. All workstations, including the new VDI desktops, were placed in their own VLAN, and the host-based firewalls were configured to prevent all desktop to desktop traffic. Additional VLANs, DMZs, and firewall ACLs were created for vendor VPN connections, Internet-facing systems, infrastructure, and internal application servers. Communicating the phases of this plan, testing procedures and rollback plan with senior management helped ensure a smooth transition.

The benefits of implementing network segmentation significantly improved security by limiting lateral movement of an attacker within the network. Additional benefits included better visibility into network traffic which would allow more detailed troubleshooting and quicker resolution of network issues. The most noticeable impact these changes had ended up being with third party vendors. There was somewhat of a culture shock in training vendors that these systems were the property of the bank, and as such required permission and accountability when connecting or making changes.

3.4. Risky Moves

While topics such as password length, virtual desktops, and network segmentation are not new topics in information security, there are very few community banks that have attempted to implement these controls to this degree. In fact, many large organizations have struggled to implement as stringent of controls due to the complexity and

dependencies involved in larger networks. This methodical approach to continuous improvement through identifying and communicating risk has improved the overall security of *Smalltown Community Bank*. However, these technical controls were just the beginning of bigger changes yet to come.

4. The Core Banking System Project

A bank's core banking system is the system of record for all customer and account data within the bank. It is the system that stores the all of the deposits, withdraws, account balances, loan payments, and customer information. *Smalltown Community Bank* moved from paper ledgers to its first electronic core banking system in the 1970's. The system received a few updates over the years, moving from green screen terminals to a visual basic user interface, but the underlying system was essentially still the same outdated system full of security vulnerabilities.

4.1. Request for Proposal

As the culture of the bank began to change and the decision-making process began to include more factors in its risk assessments, the role of information security in the bank's legacy applications became more prominent. Although the bank recognized that the old core was outdated, there was a strong reluctance to find a new solution. One employee commented that she would just have to retire early because learning a new system would be too hard. A few employees who supported the idea of utilizing a newer system just didn't believe it would be possible to find a cost-effective alternative. The bank's CEO commented that there was a 99% likelihood his vote would be "no" when asked to purchase a new core banking system. Despite this resistance, senior management agreed to allow the IT committee to compile a request for proposal (RFP) and send it out to vendors for bids on a new core banking system.

Until this point, the bank had never performed a cost analysis of the features and functionality of their core banking system. Creating an RFP with defined requirements would provide a quantitative measurement to score the cost and functionality of the proposals compared to the old system. This approach proved vital to the decision-making process by defining an objective process for the risk assessment, cost analysis and

selection of the final solution. Gaining consensus and approval for the RFP and selection criteria up front helped mitigate the bias of senior management and the board of directors towards preserving the status quo and staying with the existing vendor. Whatever the result of this process ended up being, the decision makers could have confidence in the final selection, because they approved the process.

The initial goal was to replace only the core banking system and leave all of the other ancillary systems in place as long as they were compatible with the new core banking system. The purpose being to reduce the scope of the change and reduce the amount of training required for end users to work with the new system. Even with this limited scope, this change would still be a major project impacting all areas of bank operations. The requirements for the RFP were gathered from all areas of the bank, operations, tellers, lending, customer service and IT. Many of the requirements were based on observations of business operations during previous projects such as the VDI implementation. Everyone in the bank was encouraged to contribute suggestions, requirements, or concerns which helped to generate interest in the project and influence the culture towards being more receptive to change.

Based on the initial responses, it was evident that this change would not be an easy sell. The old core system really was the low-cost choice, but other factors still needed consideration. Each response to the RFP included additional functionality beyond what was requested. Providing the right information to senior management and enabling them to make an informed decision would require some additional work. The IT committee put together a matrix for each of the responses showing what functionality was included along with the price. Then the matrix was updated to include the functionality of the old system. Some of the proposals even included functionality that was covered by the existing ancillary products. At this point, the IT committee realized that in order to prepare a true "apples to apples" comparison, the bank would need to inventory all of its ancillary products and associated contracts. Once this was complete, an updated RFP was sent out to the vendors requesting updated proposals to include options for all ancillary system functionality. In places where the proposals included new functionality that the bank did not currently have, the existing core vendor was also asked

to provide proposals for similar functionality. See Appendix A for a sample functionality matrix.

Other risk factors included not only the cost of the existing core banking system, but also the cost and complexity of managing separate contracts for each of the ancillary products required to operate the bank. Finding a solution that could perform all of the same functionality would mean consolidating nine separate vendors into one. Given the regulator's increased scrutiny of third party vendor management, this was an attractive benefit. Another factor to consider with all of these contracts was the termination and data deconversion fees. Even after all of these factors were included in the functionality matrix, the project began to seem more viable. Consolidating almost all of the bank's legacy systems and applications into an integrated solution from a single vendor also contained the promise of improved operational efficiencies. The old systems required data to be input in some cases as many as three or four times into various applications because there were no automated integrations.

Many of the information technology risk factors dealt with how outdated the old system was; flat file data structures, Cobol backend, visual basic user interface and communication protocols such as telnet and FTP just to name a few. There were also many security concerns including the software vendor's remote access to the system, hard coded usernames and passwords embedded in the client application, and the lack of user authentication for many data retrieval functions. The flip side of this risk evaluation was the unknown of whether a new vendor would perform any better. There were also numerous risks to consider concerning the conversion of the data from multiple legacy systems to the new system.

In early 2014, as the bank was evaluating the RFP responses, the bank received a notice from the existing core vendor's data center. A recent FFIEC regulatory examination reported that the vendor's information security program was unsatisfactory; citing that bank customer data was at risk of exposure or compromise due to the lack of security controls in place. This report confirmed the bank's suspicions that the existing vendor did not have a solid strategy for implementing changes necessary to meet new regulatory requirements, keeping pace with requests for new functionality or addressing

concerns with weak security practices. These factors were also included in the risk assessment and contributed to the decision to choose a new core banking system.

4.2. Negotiations

As the bank reviewed the RFP responses, three finalists were selected to provide an onsite demonstration of their proposed products. These demonstrations were the pivotal moment where senior management recognized the benefits that a new core banking system would provide. The culture shifted from total reluctance to one of optimism. After the initial round of demonstrations, two finalists were selected to compete for the final contract. Based on the recommendation of the IT committee, the bank hired an outside consultant that specialized in contract negotiations for core banking system conversions to audit the bank's due diligence process and work with the bank to negotiate the best possible contract with the selected vendor.

The last obstacle to overcome in the negotiations process was the lack of a contractual commitment from the selected vendor to resolve security vulnerabilities if any should be discovered in the future. Based on the lack of security that the bank found in the old core banking system, they did not want to end up in the same situation. One way to manage this risk was through requiring the vendor to include a clause in the contract defining the term security vulnerability and the vendor's responsibility to remediate security vulnerabilities. It took several months' worth of negotiations with the vendor's legal team to come to an agreement on the specific language that the bank required.

4.3. Implementation and Results

Smalltown Community Bank began production operations on the new core banking system and ancillary systems in late 2015. Overall, the implementation was a success. Employees adapted to the new systems much quicker than anticipated. The new core system reduced the number of steps needed to complete many routine tasks, such as end-of-day processing and statement generation. Because of the integrations between the core system and ancillary systems, such as new accounts, loan origination, and document archive, customer and account data no long had to be input multiple times improving operational efficiency and data accuracy. The relational database architecture provides

better reporting functionality and has improved the availability of information needed for management to make decisions. The bank has also been able to improve customer service operations because various pieces of data that used to be stored in multiple systems are consolidated into fewer user interfaces and now easier to find when answer questions for customers. Many of the new user interfaces provided integration into Active Directory as well, which further consolidated user accounts and passwords to reduce password fatigue for users. The conversion reduced the time required to comply with vendor management regulations by consolidating systems which reduced the overall number of vendors to manage. Information security was improved in many ways, increased auditing of user actions,

The core banking system project represented an enormous undertaking for an organization the size of *Smalltown Community Bank*. Changing the core banking system and all of the ancillary systems that the bank uses to serve its customers impacted every aspect of the bank's operations and the daily tasks of every employee. This project would not have been possible without first establishing a foundation with senior management based on credible technical expertise and honest communication. Fixing all of the security vulnerabilities in the old core banking system was not a realistic option. The only way to improve the security of the organization was to find a solution that not only improved information security, but also created value for business operations.

5. Conclusion

This case study represents a real world example of how investing in information security can provide improvements in many areas of an organization's operations. Organizations need technical expertise to make informed decisions about the information security risks they are facing. IT and InfoSec departments must gain an understanding of business operations to communicate effectively with the decision makers of the organization to manage these risks. The goal of a successful information security strategy should be finding solutions that manage risk and create value for the organization.

Wesley Earnest, wes.earnest@gmail.com

Achieving this goal is not dependent upon the size of the organization, as evidenced by *Smalltown Community Bank*. Even very small organizations can compete with the world class security teams and resources of larger organizations by taking a holistic approach to managing risk and implementing solutions that contribute the most value. Technical controls, such as fifteen character passwords, virtual desktops for all employees, and multiple layers of network segmentation, have been deemed not feasible by many larger organizations and have been avoided by many smaller organizations simply lacking the expertise to identify or implement. However, *Smalltown Community Bank* has not only implemented these controls successfully, it also completed a conversion of its entire core banking system and ancillary systems, based on an information security strategy designed to manage risk and create value. This success is the result of transitioning from a passive decision-making process of maintaining the status quo, to an active decision-making process focused on continuous improvement.

References

Accenture (2015, October 28) *Bank Boardrooms Lack Technology Experience, Accenture Global Research Finds.* Retrieved from: https://newsroom.accenture.com/news/bank-boardrooms-lack-technology-experience-accenture-global-research-finds.htm

Altucher, J. (2015, January 2) *FAQ on How To Become An Idea Machine.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/faq-how-become-idea-machine-james-altucher

Federal Reserve (2015) *Total Assets, All Commercial Banks*. Retrieved from Federal Reserve Bank of St. Louis: https://research.stlouisfed.org/fred2/series/TLAACBW027SBOG

FFIEC (2004) IT Examination Handbook: Operations. Retrieved from http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Operations.pdf

ICBA (2015, December 31) *Community Banking Facts.* Retrieved from Independent Community Bankers of America: https://www.icba.org/files/ICBASites/PDFs/cbfacts.pdf

Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux. Retrieved from Google Books: https://books.google.com/books?isbn=1429969350

Kim G., Spafford G. (2004) *The Visible Ops Handbook: Starting ITIL in 4 Practical Steps*.

Koppel, T. (2016) *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath.* New York: Crown Publishers. Retrieved from Google Books: https://books.google.com/books?isbn=055341996X

KPMG (2016, February) *Small Business Reputation & The Cyber Risk.* Retrieved from: https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

Mandiant Consulting (2016, February) *M-Trends 2016*. Retrieved from FireEye: https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

Wesley Earnest, wes.earnest@gmail.com

Martin, R. (2009) *The Opposable Mind: Winning Through Integrative Thinking*. Boston, Massachusetts: Harvard Business Press. Retrieved from Google Books: https://books.google.com/books?isbn=1422139778

NIST (2014) *Report: Authentication Diary Study*. Retrieved from National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7983.pdf.

Peirce, H., Miller, S. M. (2015, March 17) *Small Banks by the Numbers, 2000–2014*. Retrieved from George Mason University, Mercatus Center: http://mercatus.org/publication/small-banks-numbers-2000-2014

Symantec (2012) *Banks likely to remain top cybercrime targets.* Retrieved from: https://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf

Shahani, A. (2016, May 27) *North Korea Linked To Cyber-attacks On Asian Banks.* Retrieved from Heard on All Things Considered: http://www.npr.org/2016/05/27/479764874/north-korea-linked-to-cyber-attacks-on-asian-banks

Strand, J. (2012, June) *Everything they told me about security was wrong*. SANS Rocky Mountain Conference 2012. Retrieved from: http://prezi.com/el3gwuqyja07/everything-i-know-is-wrong/

US-CERT (n.d.) *Resources for Small and Midsize Businesses (SMB).* Retrieved March, 2, 2016 from United States Computer Emergency Readiness Team: https://www.us-cert.gov/ccubedvp/smb

Wesley Earnest, wes.earnest@gmail.com

Appendix A

Core Conversion Functionality Matrix

	10 Year Cost Projection		10 Year Cost Projection Based on RFP / Quotes		
System Functionality	**Current Vendors**	**Deconversion Costs**	**Vendor A**	**Vendor B**	**Vendor C**
Core Banking System - Software					
Core Banking System - Hardware					
Offsite Backup / Disaster Recovery					
Teller Software					
New Accounts Platform					
New Loans Platform					
Secondary Market Loan Management					
Item Processing/Imaging - Software					
Item Processing/Imaging - Hardware					
Check Image Archive - Hardware					
Printing Temporary Checks / Loan Coupon Books					
Printing Cashier's Checks, Money Orders, and Drafts					
Statement Printing and Mailing					
Document Scanning / Archiving					
Report Archiving					
eStatements Archiving					
Internet Banking					
EFT / Debit Card Processing					
EFT / ATM Driving Network Interface					
BSA/AML Compliance / Fraud Monitoring					
Integrated Reporting / Dashboard					
Integrated Accounts Payable					
Totals					

Last Updated: September 17th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Dallas Fall 2019	Dallas, TXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS SEC504 Madrid October 2019 (in Spanish)	Madrid, ES	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS London October 2019	London, GB	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Cairo October 2019	Cairo, EG	Oct 19, 2019 - Oct 24, 2019	Live Event
SANS Santa Monica 2019	Santa Monica, CAUS	Oct 21, 2019 - Oct 26, 2019	Live Event
Purple Team Summit & Training 2019	Las Colinas, TXUS	Oct 21, 2019 - Oct 28, 2019	Live Event
SANS Training at Wild West Hackin Fest	Deadwood, SDUS	Oct 22, 2019 - Oct 23, 2019	Live Event
SANS Orlando 2019	Orlando, FLUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Houston 2019	Houston, TXUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Amsterdam October 2019	Amsterdam, NL	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS DFIRCON 2019	Coral Gables, FLUS	Nov 04, 2019 - Nov 09, 2019	Live Event
Cloud & DevOps Security Summit & Training 2019	Denver, COUS	Nov 04, 2019 - Nov 11, 2019	Live Event
SANS Paris November 2019	Paris, FR	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Sydney 2019	Sydney, AU	Nov 04, 2019 - Nov 23, 2019	Live Event
SANS Mumbai 2019	Mumbai, IN	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Bahrain September 2019	OnlineBH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced