

# Security Case Competition

Improving Security at Green Star Bank



Remington Steele  
Dylan Eastman  
Jason Smith  
Drake Loud  
Mat Rose

Green Star Bank  
ATTN: Board of Directors  
100 Green Star Way,  
Lansing, MI 48937

1 March, 2017

To the Board of Directors:

As a result of the recent security breach and subsequent \$1.2M loss, I have directed Green Star Bank's cybersecurity team to assemble a report identifying information security threats throughout the company. The report describes recommendations designed to mitigate these threats.

The changes to the new system will yield a return on investment of \$1,565,000 in the first year alone and will build goodwill for Green Star Bank within the Michigan community.

Green Star Bank is currently overcoming systematic attacks that target both the bank's network and employees. Social engineering attacks are the greatest threat to the bank. These social engineering attacks target employees directly and involve using schematic fraud to steal money. Other threats include weak passwords and phishing attacks on remote employees' computers.

The necessary change to Green Star Bank's system is to adopt COBIT 5, a system-wide framework, that will accomplish the goals of mitigating threats from social engineering attacks, remote employees' susceptibility to phishing, and weak passwords. Consistent with Green Star Bank's mission, the new system will provide Green Star Bank's customers with peace of mind.

Respectfully,

Green Star Bank CISO

<b>Executive Summary</b>	<b>3</b>
<b>Introduction</b>	<b>4</b>
Problem	4
Recommendations	4
<b>Preventive Controls</b>	<b>5</b>
People: Creating a “Security-Conscious” Culture	5
Implementing the Culture & Change Management	6
Employee Security Training	7
Hardware	9
Software	10
<b>Detective Controls</b>	<b>13</b>
Audit Accounts	13
Penetration Testing	14
<b>Corrective Controls</b>	<b>14</b>
Computer Incident Response Team (CIRT)	15
<b>Implementation</b>	<b>15</b>
Conclusion	16
<b>Appendix</b>	<b>17</b>
Meet the Team	17
Threat Model	17
Cost Benefit Analysis	19
<b>Works Cited</b>	<b>20</b>

# Executive Summary

---

**Overview** A recent security breach at Green Star Bank has brought light to areas of cybersecurity that need additional security coverage within the bank's systems. Implementation of a new system framework will cost just over \$40,000 the first year, but will provide a total benefit over \$1.5M the same year.

Cost-benefit Analysis	
Implementation Costs	(42,626.50)
Benefits of Implementation	1,565,000.00
<b>Net Benefit (year 1)</b>	<b>\$1,518,738</b>

**Problem** Most important, illegitimate users are still inside Green Star Bank's system. Furthermore, social engineering and phishing attacks similar to the recent attack will pose a significant threat to the bank's system until the new framework is in effect. While Green Star Bank has excellent security controls, this recent breach teaches that Green Star Bank has inadequate controls to prevent, detect, and correct these attacks.

**Solution** In short, the solution that will prevent, detect, and correct cyberattacks is COBIT 5. COBIT 5 is one of three industry-leading information system security frameworks.

First, COBIT 5 will detect and eliminate all current illegitimate users. Second, it will reduce the number of potent attacks on the system drastically. This cohesive framework implements defense-in-depth, securing multiple layers of the system. Finally, at Green Star Bank, COBIT 5 will correct current system flaws and inefficiencies, *reducing IT costs by \$200,000 annually.*

# Introduction

---

## Problem

Recently an employee who works remotely from home fell for a spear phishing email that installed malware on her bank-supplied laptop. As a result, the attacker was able to remotely observe the employee initiating bank transactions, and soon used the employee's bank employee credentials to login and initiate transfers to an offshore bank account. The bank officer who provided secondary approval for the transfers failed to detect or question the fraudulent transfers and the bank suffered a \$1.2M loss. Before detection, the attacker scanned the bank's systems and created alternative logins in order to maintain access in the future.

As a result of this breach, Green Star Bank contracted with an outside company to perform a thorough penetration test of Green Star Bank's operations. The pen testing company recommended a significant change in password security for all employee accounts.

The pen testers described the security problem as representative of a larger problem that is difficult to stop with the existing company information security policy. The pen testing unveiled a few major security issues, including:

- Weak passwords
- Remote employees' susceptibility to phishing
- Employee susceptibility to social engineering attacks

## Recommendations

It is recommended that Green Star Bank management review the current internal controls using the COBIT 5 internal control framework. COBIT 5 is a comprehensive framework of best practices relating to all aspects of the governance and management of IT. However, the portions of COBIT 5 focused on in this report are those that most directly pertain to the reliability of an information system and compliance with regulatory standards. Additionally, the elements of the COBIT 5 framework focused on have been organized around the principle in the Trust Services Framework (developed jointly by the AICPA and the CICA). Recommendations are categorized by the three areas of the time-based model<sup>[1]</sup> of security:

1. Preventive Controls
2. Detective Controls
3. Corrective Controls

The majority of the recommendations are preventive, dealing mostly with people training and device/software hardening controls. The concerns of the pen testing company have also been addressed by revisiting Green Star Bank's password policies.

The following report was created by Green Star Bank's cyber security team at the direction of the CISO.

## Preventive Controls

---

While there are currently controls in place to prevent fraud or malicious attacks from being successful, additional controls are necessary to provide a more robust defense-in-depth.<sup>[1]</sup> The majority of cyber attacks are stopped before they happen. Therefore, the majority of recommended controls focus on preventing cyber attacks. The recommendations in this section seek to mitigate threats in the following areas:

- People
- Hardware
- Software

### People: Creating a “Security-Conscious” Culture

Security is a management issue, not just a technology issue. While every preventive control is necessary and important, people management will always be the most critical. No matter how many controls, software, hardware, or other checks are put on a system, ultimately, the biggest weakness are the people. According to a study by Proofpoint, Social Engineering is the most effective attack against organizations; which makes people the number one target at a company.<sup>[2]</sup> In order to protect Green Star Bank from these attacks, creating a company-wide culture of security that is supported and reinforced by top management is critical.

The culture should support the raised awareness of each employee to the dangers of social engineering and other security attacks. It should also be easy for employees to be able to report potential security risks and receive prompt, effective support. Employees should feel the importance of the new culture and be able to engage in activities that make being security-conscious employees second nature. The elements of the proposed culture can be easily summarized by the acronym, **A.R.I.S.E.**, for this purpose. Taken from the five points of the culture, A.R.I.S.E stands for:

- Awareness
- Reporting
- Importance
- Support
- Engagement

**Culture of Awareness** Just as important as reporting the problem, employees at Green Star bank should be able to detect when they are being targeted through Social Engineering. As employees understand the threats and how they might be susceptible, they will be better prepared

when they are being attacked. A culture of understanding and awareness is paramount for the success of Green Star bank. Employees should be encouraged for their own personal learning as well.

**Culture of Reporting** Green Star bank should have an open door policy when it comes to reporting any threats or problems that may come up. Security teams should be responsive and allow members of the organization to easily and openly be able to talk about their concerns.

**Culture of Importance** During a training, it may be easy for an employee to feel the importance of being security minded, but it is imperative that the security culture resonate through the company. Employees of Green Star Bank need to be reminded and remember the importance that their actions have on the company.

**Culture of Support** Security efforts need to come from every level of the company. Leaders in the company need to be exemplars of the culture. New and junior employees need to see the leaders of the company exemplifying the culture of the company. If C-Level employees aren't supporting the culture, then the culture will struggle to persist. Senior employees should encourage junior employees to understand the importance of security. Senior employees and leaders should show support to junior employees in all aspects to foster the new culture.

**Culture of Engagement** Lastly, Green Star employees should be engaged in being secure in all that they do. A chain is only as strong as it's weakest link, and Green Star's security is only as strong as the weakest employee. Green Star bank should focus on having every employee engage in the initiative to be security conscious and to engage in doing their part in keeping data secure.

## Implementing the Culture & Change Management

Simply creating the idea of a secure culture does not guarantee that it will be implemented. We recommend that the following steps be implemented. These steps will ensure that the new security focused culture will stay.<sup>[3]</sup>

**Initial Kickoff** A firm kickoff, which may include the initial trainings to introduce the new focus of Green Star Bank. Top management should present to help show the importance as well as the buy in from top management.

**Improve Hiring Practices** Security awareness should be part of the hiring process. Through interviews and other initial contact with potential new employees, the importance of a secure culture should be emphasized.

**Change Onboarding to Reflect Culture** When employees are hired and begin onboarding, new employees should receive trainings about the new security culture, in addition to trainings about how to detect social engineering and what to do when they do detect it.

**Reinforce the Culture** To maintain the culture that is being created in the long term, we recommend that appropriate reinforcement be prevalent moving forward. Employees should receive posters, cards, and other branded office supplies that they can keep in their cubicles as reminders of the new A.R.I.S.E initiative. These physical objects serve as artifacts of the new secure culture. In addition, it is important that the culture in being reinforced is not only from the top down, but employees are able to share their experiences openly with others. Managers should take the responsibility over their employees as well.

## Employee Security Training

Regular security training will help to distribute the new culture and will remind employees of the importance of being “security-minded.”

**Anti-Phishing Training** Phishing training for all employees should happen on regular basis (e.g. quarterly, semi-annual, etc.). In addition, all new-hires should receive a personalized phishing training within the first month of their hire-date. The training should include:

- Proper procedures regarding email
- Increase privacy or removal of personal information from social media sites
- Notification of penalties due from not following security protocols
- Recent examples of successful phishing schemes
- How to report suspicious emails or potential security breaches

With these trainings in place, employees will be less susceptible to phishing attacks. Employees can be a great security risk, but when they are trained effectively, they are the first line of security in any company.

**Password Policy** One of the major findings from the pen testing company was password weakness. They noted themed passwords that centered around sports or seasons. The current password guidelines are pretty strict, and that may be causing some bad password behavior. The strict policy requiring 8-12 characters, with upper and lower case, numbers and symbols make it difficult for users to create and remember their passwords without adding much security. Requiring that passwords be changed every 90 days, and not allowing password reuse can cause users to create password schemes for altering a password by changing a single character, like incrementing a number. We recommend the following 6 password guidelines for all employees with general access accounts:

1. Length 12 Characters or greater, with no enforced maximum
2. Passwords should be stored in the company password management software
3. Employees should be trained to use diceware to create master passwords for their password manager account.
4. Passwords should not contain any part of the employee’s username



5. New passwords must not be more than 50% the same as the last 5 passwords
6. Passwords may not be transmitted to another person

According to Gartner “Password aging is widely advocated, but rarely worthwhile. It is essentially a stopgap for other missing controls. However, long-period aging may [improve] residual risks.”<sup>[4]</sup> We recommend removing the requirement to change passwords every 90 days, but suggest password changes in the following situations:

- If a known breach occurs costing over \$1m all employees must change their password.
- If a system that they maintain or use is found to be compromised.
- If two or more people in their immediate team is hacked, or is found to have a virus or malware.
- If one or more of their work or personal accounts is compromised or becomes infected by a virus or malware.

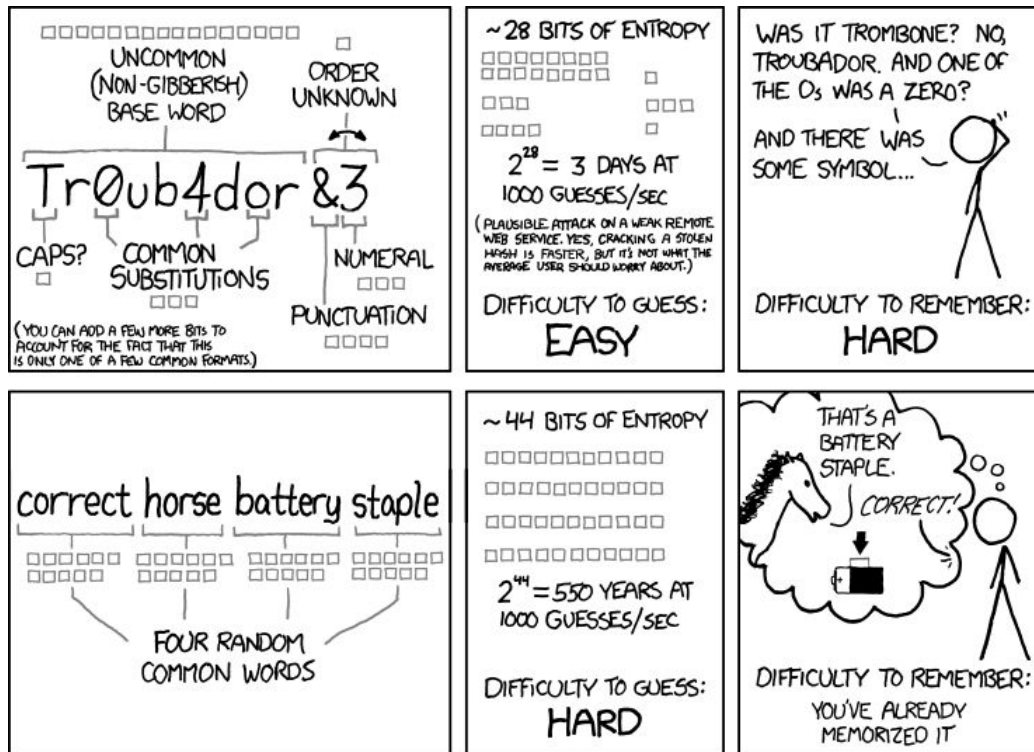
We think that only requiring a password change in these circumstances would remove some of the pressure to constantly create difficult passwords, and help enforce a secure culture where employees have a stake in encouraging secure behavior. The introduction of the IDS and account auditing will eliminate the need to change employee passwords as it eliminates the access that an attacker may have gained by stealing an employee's password.

Some employees who have higher levels of access, such as system admins, or those with the highest levels of public visibility, like executives, should be required to adhere to higher more secure guidelines.

1. A Diceware passphrase must be used
2. Length must be greater than 15 characters
3. Passwords should expire after 6 months, but longer passwords are valid longer
4. Fingerprint readers will be provided and should be used to access computer systems and password managers

We recommend the use of passphrases, and using Diceware is a technique of generating random phrases. Phrases generated by the user are susceptible to very similar weaknesses as passwords they generate, mainly that they are common phrases that are easy to guess. In a research study done at Cambridge they found that “users aren’t able to choose phrases made of completely random words, but are influenced by the probability of a phrase occurring in natural language.”<sup>[5]</sup>

Using dice to generate passwords adds entropy. In an article published on The Intercept, Micah Lee explains how unlikely it is that an attacker will be able to guess your Diceware Passphrase. He says “if an attacker knows that you are using a seven-word Diceware passphrase, and they pick seven random words from the Diceware word list to guess, there is a one in 1,719,070,799,748,422,591,028,658,176 chance that they’ll pick your passphrase each try. At one trillion guesses per second — per Edward Snowden’s January 2013 warning — it would take an average of 27 million years to guess this passphrase.”<sup>[6]</sup> The XKCD comic shown below ([Figure 1](#)) gives another explanation of how entropy improves password security.



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

**Figure 1-** How password entropy increases security

## Hardware

The first step to ensuring network security within Green Star Bank is to locate and eliminate unwanted network activity. While intruders have clearly entered Green Star Bank's system, we must detect their movement and eliminate their presence within the system.

The first step to removing illegitimate users is to detect their presence within the system. The Cisco ASA 5525-X IPS is a network security tool in Cisco's leading-edge security module lineup. This Cisco ASA will both detect and prevent unwanted network traffic, including malware, worms, keyloggers, and many other threats. In addition, the 5500 line of Cisco ASA products offers automated cleanup of malware and spyware infections.<sup>[7]</sup>

The Cisco ASA 5525-X IPS costs \$5020.00 new. It has eight ports and features support for VPNs. The IPS portion scans network activity and performs behavior analysis. This particular feature is especially pertinent to Green Star Bank's current information security threats because this device will scan network activity and can automatically eliminate network threats.



**Figure 2 -** Cisco ASA 5525-X IPS

The Verifi P5100 Premium Metal Fingerprint Reader will be utilized in conjunction with the multi-factor authentication. It connects to computers via USB ports, accurately reads fingerprint inputs, and sends the input to be compared with fingerprints in the database. If the input matches, authentication is proven, and the system will allow the user to access the system.



**Figure 3 - Verifi P5100 Premium Metal Fingerprint Reader**

## Software

After reviewing the losses of the bank, the reasons behind those losses, as well as current industry security standards, it has been decided to implement and upgrade various security measures through software. The following ideas are recommended in order to increase remote employees' security.

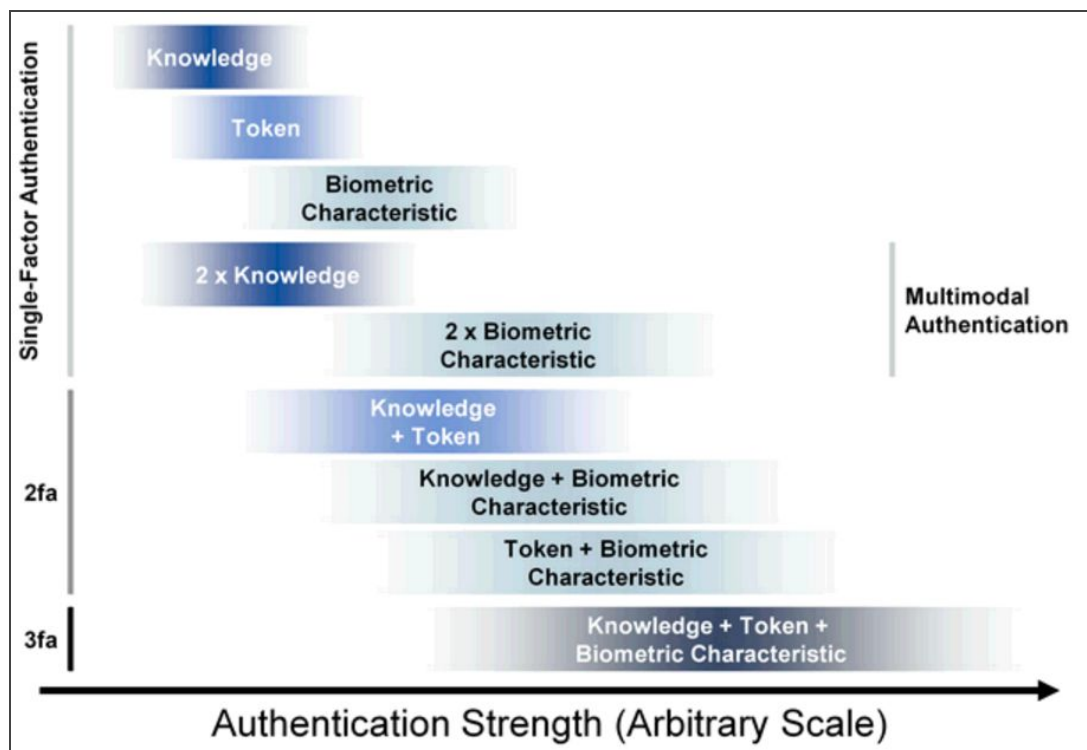
**Password Managers** Password managers are a software solution that creates an encrypted database to store users credentials for different sites and softwares. According to Gartner "Personal password managers offer a means of alleviating this cognitive burden by recording these passwords in a secure, yet easily accessible, manner. In essence, these tools encrypt an organized collection of data with a "master password" and, for convenience, offer form-filling functions to provide reduced sign-on by automatically entering user IDs and passwords when appropriate."<sup>[8]</sup> Many password managers are able to generate strong passwords and store them so that users don't ever have to memorize them. We recommend using an enterprise password manager so that it can be integrated with other authentication systems already used in the environment like Microsoft's Active Directory. LastPass is a highly rated password manager that offers an enterprise level service. We also recommend LastPass because it can be used along with other security services like Multi-factor and Biometric authentication that will be discussed in the next few sections. The service would cost \$30/yr/user or just over \$15,000/yr.<sup>[9]</sup>

**Multi-factor Authentication** Authentication may be undermined by an attacker obtaining access to a user's digital identity and then being able to log in as a legitimate user. Authentication strength is measured by how difficult it is for an attacker to masquerade as a legitimate user.<sup>[10]</sup>

Multi-factor authentication is a method of computer access control that requires users to present different types of authentication in order to gain access to the protected system. Figure 4 depicts the relative strength of various forms of multi-factor authentication to single-factor authentication. Adding multi-factor authentication better secures against common authentication attacks.

It is suggested that Duo Security, a leading multi-factor authentication service provider, be used to provide employees with a simple means of multi-factor authentication. When an employee attempts to log in to the system, Duo Security sends a message to the employee's mobile phone to confirm a

legitimate log in. After the employee confirms they made the attempt, Duo provides an access token to the system. The combination of the password (knowledge) and Duo's confirmation (token) decrease the likelihood of an attacker gaining system access if an attacker does obtain an employee's login credentials.





**Figure 4 - Multi-Factor Authentication**

Critical user roles (accounts that, if compromised, pose significant threats to the system) are recommended to use additional forms of authentication to secure the system. Multi-modal forms of authentication, such as a fingerprint (biometric characteristic) combined with a password (knowledge) and/or a Duo confirmation (token) would provide greater levels of security to such accounts. Specific recommendations for affordable fingerprint scanners can be found in the “Hardware” section of this report.

**Malware Protection** Preventing malware incidents is more cost-effective than detecting, remediating and removing malware, and this was taken into consideration while researching the optimal malware protection software. During the research, priorities focused on prevention, detection, cost, scalability, and ease of use. Other factors taken into consideration included expert reviews, user reviews, additional software features, processor load, and support.

McAfee AntiVirus Plus emerged as the recommended software to implement. **Figure 5** is a visual representation of the attributes considered, as well as relative costs. Although the figure pricing is geared towards individual use, McAfee has also proven to be effective on the enterprise level.

Name	McAfee AntiVirus Plus (2017)	Webroot SecureAnywhere eAntiVirus	Bitdefender Antivirus Plus 2017	Symantec Norton AntiVirus Basic	Kaspersky Anti- Virus (2017)	Avast Pro Antivirus 2016	Emsisoft Anti- Malware 11.0	ESET NOD32 Antivirus 10	F-Secure Anti- Virus (2017)	Trend Micro Antivirus+ Security (2017)
										
Lowest Price	\$24.99 <a href="#">SEE IT</a>	\$19.99 <a href="#">SEE IT</a>	\$25.99 <a href="#">SEE IT</a>	\$19.99 <a href="#">SEE IT</a>	\$39.99 <a href="#">SEE IT</a>	\$39.99 <a href="#">SEE IT</a>	\$39.95 <a href="#">SEE IT</a>	\$39.99 <a href="#">SEE IT</a>	\$39.99 <a href="#">SEE IT</a>	\$34.95 <a href="#">SEE IT</a>
Editor Rating	●●●●●○ <small>RG</small>	●●●●●○ <small>RG</small>	●●●●●○ <small>RG</small>	●●●●●○ <small>RG</small>	●●●●●○ <small>RG</small>	●●●●●○ <small>RG</small>	●●●●●○	●●●●●○	●●●●●○	●●●●●○
On-Demand Malware Scan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
On-Access Malware Scan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Website Rating	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓
Malicious URL Blocking	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
Phishing Protection	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
Behavior- Based Detection	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Bonus: Vulnerability Scan	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗
Read Review	<a href="#">McAfee AntiVirus Plus (2017) Review</a>	<a href="#">Webroot SecureAnywhere eAntiVirus Review</a>	<a href="#">Bitdefender Antivirus Plus 2017 Review</a>	<a href="#">Symantec Norton AntiVirus Basic Review</a>	<a href="#">Kaspersky Anti- Virus (2017) Review</a>	<a href="#">Avast Pro Antivirus 2016 Review</a>	<a href="#">Emsisoft Anti- Malware 11.0 Review</a>	<a href="#">ESET NOD32 Antivirus 10 Review</a>	<a href="#">F-Secure Anti- Virus (2017) Review</a>	<a href="#">Trend Micro Antivirus+ Security (2017) Review</a>

**Figure 5 - Various malware/antivirus softwares**

Using McAfee AntiVirus Plus will reduce remote employees' susceptibility to malware, both by adding extra prevention to known malware, as well as constantly scanning to detect malware that has been put on the system.

**Email Filter** The attacker's point of entry into the system was a phishing email with hidden malware attached. We recommend putting in place an email filter to scan email and prevent spam, malware, viruses, trojan horses, Cryptolocker from getting into the enterprise, and many can prevent sensitive information or company secrets from being leaked via email. The SpamStopsHere Enterprise cloud service effectively mitigates the threat of malicious emails because it provides the essential functions of attachment filtering, TLS encryption, quarantine, and outbound filtering. This service costs \$7962.50/year. <sup>[11]</sup>

**Enterprise Software Management System** Anti-virus software is a way to detect and remove a virus or malware that is downloaded or installed, but Enterprise Software Management Systems prevent anything but allowed programs to be run. One of the ways that this is done is by using the Software Manager to distribute the allowed programs. This is typically done through the use of a software agent that is installed on the system during provisioning of the employee's computer, and the agent listens for instructions about what software should be installed. Only software that the organization has approved are made available to be installed via some sort of application portal. The agent is configured to block any application from running if it's not approved.



Having this agent also allows IT administrators to remove local administrative rights from the users, and prevent them from installing other applications that have not been approved. Removing this right further prevents malicious files that the user may download from installing because the user's account no longer has rights to install anything.

**Telecommunications** To better protect data and communications transmitting between the network and remote employees, a Virtual Private Network (VPN) should be installed.

A VPN creates a virtual circuit, or tunnel, from the remote client to the private network and appears as a dedicated connection between two endpoints. Green Star Bank should select a VPN provider that uses IPsec secure protocols to ensure data protection and completeness as packets are transferred between endpoints. Using a VPN with secure protocols guarantees that data in packets are encrypted by the hashing algorithms: Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). Since IPsec requires security protocols Internet Key Exchange (IKE) and Internet Security Association and Key Management Protocol (ISAKMP) to authenticate both network nodes, this will ensure that only authorized devices can access the private network. In the event that an attacker does attempt "packet sniffing" all data will be encrypted.<sup>[12]</sup>

VPNs and firewalls on machines can be configured to require a VPN connection for specific applications on a machine to gain access to any network. By configuring remote clients in this way, it would remove the likelihood of a remote user forgetting to establish a VPN or losing VPN connections during sessions without noticing.

## Detective Controls

---

While the majority of the recommendations for Green Star have been preventive, these controls are never 100% effective in blocking every attack (as evident by the recent breach). COBIT 5 describes activities that Green Star Bank needs to be able to detect intrusions and problems in a timely manner. These activities have been reviewed to determine appropriate ways that Green Star Bank can review the effectiveness of its system and detect possible incidents.

### Audit Accounts

Before being detected, the attacker was able to create alternative logins (employee accounts) to allow future access to the system. To purge unauthorized accounts from the system, it is recommended that an audit of all accounts should be conducted. This audit will consist of three processes: 1.) Reviewing account creation process, 2.) Verifying current employee accounts, and 3.) Establishing regular account audits.

**Reviewing account creation process** Since the attacker was able to create additional accounts to maintain system access, the account creation process should be reviewed. The access

control matrix should be reviewed to ensure only authorized admins can create employee accounts. It may also be beneficial for an additional account creation admin to review proposed accounts. This will help to mitigate one individual (attacker or employee) from creating fictitious or incomplete employee accounts.

**Verifying current employee accounts** Since it may be difficult to determine which accounts were created by the attacker, it is recommended that each account in the system be reviewed. Automated processes may be used to ensure that each account has been created by a validated, active employee. It may be beneficial to have each branch/department manager confirm the existence of employees to ensure the attacker did not falsify an employee record. Any flagged accounts should be reviewed in-depth. It is suggested that flagged accounts be frozen and employees verified to prevent further malicious use.

**Establishing regular account audits** To better prevent or detect fictitious accounts in the future, it is recommended that a regular account audit process be established. This could be an automated process that reviews employee accounts as regularly as desired (e.g. weekly, quarterly, semi-annual, etc.) and flags suspicious accounts for further investigation.

## Penetration Testing

**Spear Phishing Resistance** To test the effectiveness of employee anti-phishing training, the CSIO (or assigned party) could conduct spear phishing campaigns on employees. The results of these campaigns would reveal the effectiveness of employee training (e.g. individually, by branch or department) and give insights for future trainings. Results could also be used by management to reinforce the company culture of being “security minded.”

**Continued Brute Force Password Attacks** By conducting regular brute force attacks on employee accounts, management would gain insight into how effective password policies are upheld. If employee passwords fail brute force attacks based on Green Star Bank’s policies, it will allow for more targeted training and further implementation of the company culture.

## Corrective Controls

---

While it is important to detect problems quickly, it is not enough. COBIT 5 recommends procedures for management to be able to respond to incidents by correcting the problem in a timely manner. The effectiveness of these procedures depends greatly on the appropriate planning and preparation. One of the most important controls highlighted in COBIT 5 is the creation of a computer incident response team (CIRT).

## Computer Incident Response Team (CIRT)

To be able to respond to security incidents quickly and effectively is the creation of a computer incident response team (CIRT). The CIRT should be comprised of technical professionals and senior operations management. Management must be a part of the CIRT because only operations management understand the costs and benefits or economic consequences of particular actions.

Together, the CIRT should review current processes and determine responses to security incidents by planning how to proceed in the following four ways:

1. Recognition - recognizing that a problem exists
2. Containment - after detection, how to proceed to contain the breach
3. Recovery - how to repair any damages caused by the attack (e.g. restoring backups or reinstalling corrupted programs)
4. Follow-up - after the incident, analyzing how/why the incident occurred and how to prevent future attacks

Communication is vital throughout all four steps. The CIRT should determine appropriate communication and processes to take to ensure a smooth and defined approach to reacting to incidents. After a plan has been created, Green Star Bank should occasionally test the incident response plan to determine its effectiveness and identify and needed changes.

## Implementation

---

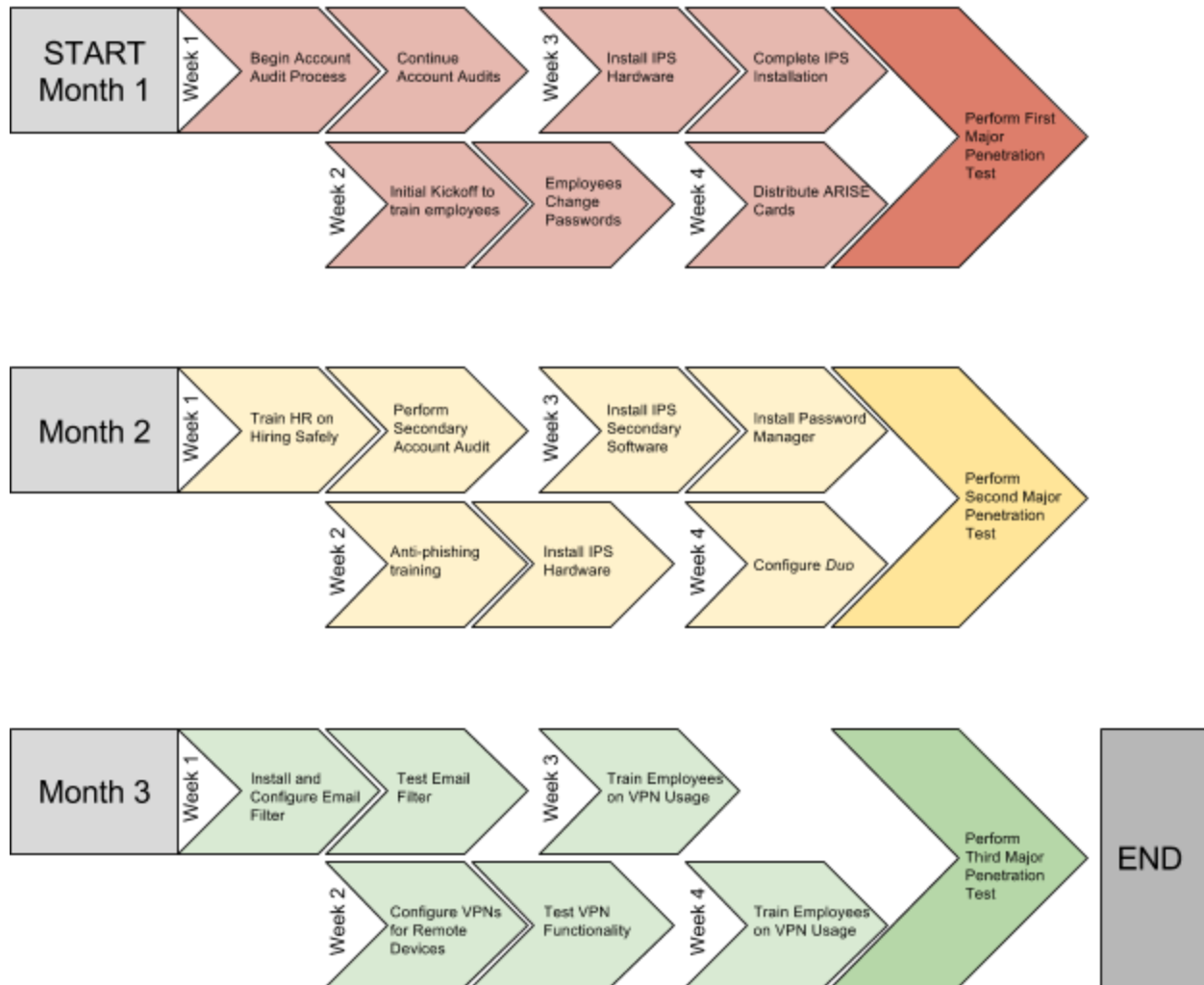
The implementation of these recommendations has been carefully considered to ensure the success of this plan. The implementation will take 3 months in total, and is broken down into major milestones to take place each month.

The first month the focus will be on making sure that any fake accounts that the attacker could be using to maintain access have been found and removed. We also want to begin training the employees right away so that we can begin the culture shift and prevent future breaches. The final piece of the first phase is to install the IDS to help detect if an intruder is in the network. The second month we will train the HR recruiters how to find new employees who are security aware, and will fit into the new culture. We also want to install the IPS to prevent an attacker from gaining access to the network. Finally we want to roll out the password management and multi-factor authentication software to improve employee identity verification.

In the final month of the implementation we want to implement the email filtering and VPN service, and provide training around these services. There is also some slack time built into the third month schedule in case the penetration tests during the previous two months have turned up anything that would cause serious delays.



## Implementation Plan



## Conclusion

In conclusion, by using the Preventive, Detective, and Corrective control elements of the COBIT 5 framework, data security at Greenstar Bank will be assured. Employees will be able to ARISE to the challenge of data security, and the systems will be aligned to support the employees in these challenges.

# Appendix

---

## Meet the Team

**Remington Steele** Prepared the cover letter and executive summary. Analyzed social engineering threats and researched solutions to major threats, including phishing attacks. Developed plans to train employees on recognizing and avoiding spear phishing. Contributed to penetration testing plans. Analyzed, researched, and wrote recommendations about IPS and other hardware.

**Dylan Eastman** Researched the COBIT 5 framework. Managed report flow, editing, voice, and formatting. Researched VPNs and associated protocols. Researched and wrote sections on account auditing, penetration testing, and CIRT. Co-authored and narrated video script. Managed report citations.

**Jason Smith** Analyzed, researched, and wrote recommendations about password policy, password management software, enterprise software management, and email filtering. Also did the cost benefit analysis to ensure that this proposal would be beneficial for organization.

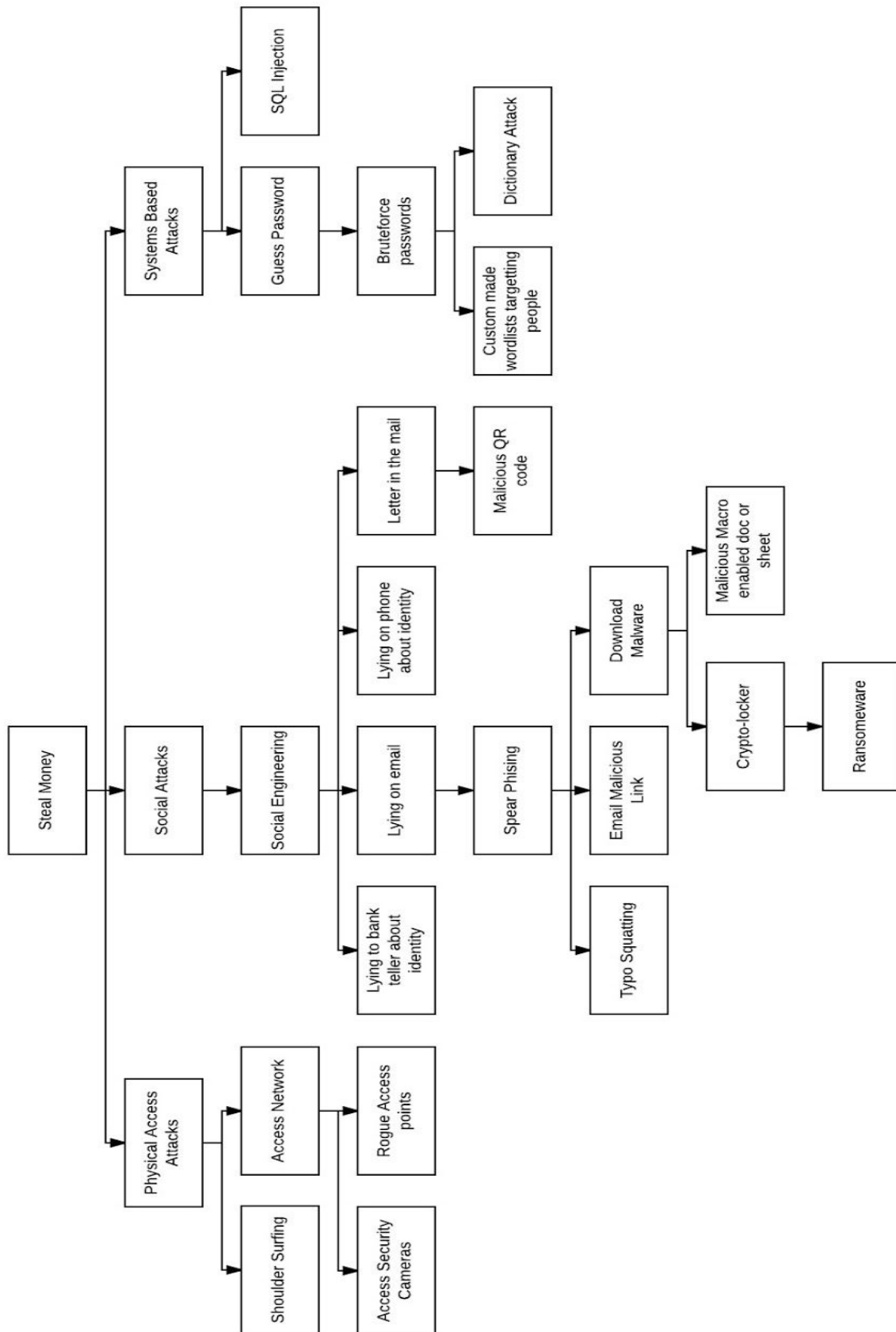
**Drake Loud** Team lead, coordinator, training specialist and videographer. Researched and analyzed employee training, and culture creation.

**Mat Rose** Analyzed, Researched, and wrote the sections about two-factor authentication and malware protection. Also devised and wrote up the training schedules and implementation for segregation of duties as well as phishing attacks. Co-authored the script for the presentation video.

## Threat Model

Threat modeling is the process of brainstorming and coming up with possible threats or vulnerabilities that target a specific objective. Although many of the vulnerabilities that were found from creating our attack tree are out of scope for this project, we wanted to specifically mention them so that both upper management and individual users might be aware of some of the attack vectors that attackers may use to either steal information or money from the bank.

If additional action is desired for other attack vectors that were not mentioned inside of our proposal, we are open to discussion on those vectors on a future date. The attack tree is below with the attack vectors and vulnerabilities found from our brainstorm (*next page*):



## Cost Benefit Analysis

Because implementing the new policy has associated costs, an analysis of the costs and benefits associated with implementing the new policy is necessary. As detailed in the following discussion of costs and benefits, the cost of implementation is only a fraction of the monetary value created by the proposed policy. The new policy will add value by mitigating the risk of exposure caused by data loss and increased security, while the reducing the costs of technical support staff, and general business overhead.

Costs			
Description	Qty	Unit Cost	Per year cost
Malware McAfee AntiVirus Plus	500	\$24	\$12,000.00
Fingerprint Scanner	250	\$150	\$3,7500.00
Duo (Multi-Factor Auth)	500	\$5	\$2,500.00
SpamStopsHere (Email Filtering)	500	\$7962.50	\$7962.50
LastPass (Password Manager)	500	\$30	\$15,030.00
Cisco ASA 5525-X IPS	1	\$5,020	\$5,020.00
Total Yr 1 Cost			\$46,262.50

The majority of the expense comes from the implementation of Password Managers, and Antivirus software across the enterprise. These costs will be offset by the following expected benefits.

Benefits			
Description	Qty	Unit Cost	Per year Cost
Reduced IT Support staff	4	\$50,000.00	\$ 200,000.00
Reduction in Expected Loss			\$ 1,365,000.00
Total Benefits/Year			\$ 1,565,000.00

The initial expenses total to about \$46,263. However, in just the first year, the new security implementations are expected to reduce the impact of expected loss from \$1.5M to only \$140,000, a difference of \$1,365,000. These figures were calculated using the conservative estimation of \$3.5M

for the average industry loss due to security incidents multiplied by the 43% chance of an incident compared to the 4% chance of something happening with the new security measures<sup>14</sup>. The cost of implementation and the expected loss with the new systems yield a return on investment of \$1,565,000 in the first year alone.

A cost-benefit analysis reveals that even with an initial outlay of \$46,263, the proposed system still provides a 330% return on investment within the first year which translates to a \$1,518,738 benefit. Additionally, as Green Star Bank gains a reputation for being secure and safe, customers will feel more confident trusting their investments with Green Star Bank.

## Works Cited

---

1. Romney, Marshall B., and Paul John. Steinbart. Accounting information systems. 13th ed. (Boston: Pearson Education, 2015), 231.
2. Proofpoint Staff. "The Human Factor 2016: People are the key." Proofpoint. February 23, 2016. Accessed February 20, 2017.
3. <https://www.proofpoint.com/us/threat-insight/post/human-factor-2016-people-are-key>.
4. Solomon, Micah. "9 Leadership Steps For Corporate Culture Change." Forbes. January 29, 2015. Accessed February 19, 2017.  
<https://www.forbes.com/sites/micahsolomon/2014/09/27/a-leadership-checklist-for-culture-change-and-customer-experience-excellence/#77b55a3b4cd4>.
5. Alleen, Ant. " Best Practices for Managing Passwords: End-User Policies Must Balance Risk, Compliance and Usability Needs; Update." Www.gartner.com. November 03, 2015. Accessed February 21, 2017.  
<https://www.gartner.com/document/2785217?ref=TypeAheadSearch&qid=da9e1d27dffa b3febc904d0>.
6. Bonneau, Joseph and Ekaterina Shutova. 2012. "Linguistic Properties of Multi-Word Passphrases." In Financial Cryptography and Data Security. Vol. 7398, 1-12. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-34638-5\_1.
7. 2015, Micah LeeMicah Lee March 26, 10:29 am. "Passphrases that You can Memorize — but that Even the NSA Can't Guess." The Intercept., last modified March 26 2015, 10:29 a.m., accessed Feb 25, 2017,  
<https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/>.
8. "Cisco ASA 5500 Series Content Security and Control Security Services Module and the Children's Internet Protection Act." Cisco. Accessed February 21, 2017.  
[http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/overview\\_c11-483382.html](http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/overview_c11-483382.html).

9. Wynne, Neil, Ant Allan, and Felix Gaehtgens. "Four Kinds of Password Management." Technology Research | Gartner Inc. December 08, 2015. Accessed February 18, 2017. <https://www.gartner.com/document/3176324?ref=TypeAheadSearch&qid=4aa8d23beefd8adefceb>.
10. LastPass. "Pricing." LastPass. Accessed February 18, 2017. <https://lastpass.com/enterprise/enterprise-pricing/>.
11. Allen, Ant. "Defining Authentication Strength Is Not as Easy as 1, 2, 3; Update." Technology Research | Gartner Inc. September 19, 2011. Accessed February 18, 2017. <http://www.gartner.com/>.
12. SpamStopsHere. "Antispam Filter Pricing and Editions." SpamStopsHere. Accessed February 19, 2017. <https://www.spamstopshere.com/simple-pricing.html>.
13. Beasley, Jeffrey S., and Piyasat Nilkaew. Networking Essentials. 3rd ed. (Indianapolis, IN: Pearson Education, 2012), 494-497.
14. Ponemon Institute "2014 Cost of Data Breach: United States." Ponemon Institute. June 2, 2014. Accessed March 01, 2017. <http://www.ponemon.org/blog/2014-cost-of-data-breach-united-states>.