TwoHands Corporation Security Consultation

Dennis Czaplicki……......…………………………..dmc5645@psu.edu
Michael McCarren…….……………………...…mpm5375@psu.edu
Tim Flynn……………..………………………………tjf5285@psu.edu

Table of Contents

INTRODUCTION:

TwoHands is a company which develops, produces, and markets specialized gloves used in waste disposal and other safety-related applications. The company is divided into three main sections; Human Resources and Payroll, Research Lab, Accounting, Inventory Management, Purchasing.   While all of these areas need to be secure, we feel that the areas that need the most attention are Human Resources and Payroll and the Research Lab.

The Human Resources and Payroll department is in charge of dealing with internal personnel issues. Their responsibilities include hiring employees, keeping employee records, operating payroll and employee relations. Within the Human Resources department, computers store employee's personal information such as paychecks, taxes, hours worked, vacation days and many other pieces of personal employee data. It is important that the department is kept secure because if a hacker gained unauthorized access to the department, it would be very bad for TwoHands. Human Resources and Payroll stores sensitive information (listed above) about the company's employees with only a select group of people allowed to access it. This information can be exploited by the attacker in a few different ways most notably through a web based attack of some sort. If in the hands of a competitor, this information could be used to lure employees away from TwoHands. They could do this by offering them more financial incentive and even more vacation days to come work for their company since they know exactly what TwoHands is paying them and how much time they are given for vacation.

The main purpose of the research lab is to research new glove designs and coatings to be used for new products. The researchers in this department must do research, perform scientific calculations, share ideas with each other and write reports. Their overall goal is to improve products to make them more marketable and appealing to customers. They also hope to keep ahead of competitors and lead the way with new technology. The researchers also need to use the internet for both research and communication. It is extremely important that this connection is secure to ensure that no trade secrets and other intellectual property is stolen. Also, their research data must be kept secure within their local network to prevent against any data leakage if their network security ever is compromised. With their current setup, they are vulnerable to various web-based attacks that could compromise their data and help their competitors. To prevent against these attacks various types of authentication, firewalls and confidentiality measures could be put in place.

Section 1: writing assignment

Introduction:	All members
Authentication and Digital Identity Facility Deployment (HR and Payroll):	Michael McCarren
Authentication and Digital Identity Facility Deployment (Research Lab):	Dennis Czaplicki
Firewall Deployment:	Tim Flynn
Data Confidentiality Deployment (HR and Payroll):	Michael McCarren
Data Confidentiality Deployment (Research Lab):	Dennis Czaplicki
Cost Analysis:	All members

Section 2: Authentication and Digital Identity facility deployment

When implementing a new type of security mechanism, TwoHands needs to ensure that it is feasible, that the employees will embrace the new technology, and appreciate its benefits. For these reasons, token-based security is the best option for the Human Resources and Payroll department and biometrics is the best form of security for the Research Lab.

Human Resources and Payroll: Token-based Security

In the Human Resources and Payroll department there are about 30 employees. Because of this, it is important that each employee has a unique password that cannot be regenerated by an attacker. Token-based security is a form of security in which every employee has their own token on them at all times. The token is synced with a database and generates a new password every minute. When users want to login they use this password and as long as it matches the one on the database, they will be given access to the system. This ensures that the same password if never used twice, thus increasing security.

One company that offers a token-based security service at a reasonable price is RSA SecurID. This company is one of the leaders in its field and offers a quality product that could be implemented immediately. TokenGuard.com is a website that sells these devices in bulk which we will use to minimize costs. The option that we are suggesting is 50 units for $2,125, which comes out to $42.50 each. This is a decent price to spend on each employee in order to ensure security. We believe that the benefits of having this system in place greatly outweighs the cost.

This security implementation will protect against various vulnerabilities. Specifically it protects against attacks where the intruder steals or decrypts a user's passwords. Since the password never lasts longer than a minute, by the time the attacker obtains the password and decrypts it, it will most likely be too late to use it any more. In addition this can protect against the vulnerability of shoulder surfing. In this case an attacker would obtain a user's password by watching the user type it in and then memorizing it. Even if this is accomplished, it is once again extremely unlikely that the attacker will be in position to use the password until it has already been changed to the next new password. This means that the information within the Human Resources and Payroll department will be much more secure than when one password was used all of the time.

Since we plan on ordering the bulk order of 50, this will leave us with about 20 extras; assuming TwoHands is a medium sized company with about 30 employees working in the Human Resources and Payroll department. We will set each Human Resources and Payroll employee with a device and explain to them how it works. It is a very simple concept so we do not see there being any issue when it comes to user acceptance and integration. With the extras, we can test them in other departments and see how they are accepted, as well as have backups incase come devices malfunction. These devices will last for 2 years so we will have the option to upgrade or switch security again soon if we are unsatisfied or feel the need to upgrade. The devices that we plan on ordering show a combination of 6 numbers every minute. However, if we feel that more security is necessary, we can upgrade so that a new password is generated every 30 seconds instead, as well as increase the password to 8 digits in length. There is no set price to upgrade so we would need to negotiate, however since we will already have the physical devices and it is supported by RSA, it should not be too expensive. Both of these methods would increase security even more without too much difficulty of implementation.

Research Lab: Biometrics

The Research Lab is a very important aspect of TwoHands that contains future glove designs or coatings that the company utilizes for profits. It is important this information does not fall into the wrong hands or that could mean major losses for TwoHands. That being said, the level of security to gain access into the research lab must be very high while simultaneously keeping the number of people with access low. We have devised a scheme that will utilize different authentication methods for getting into the actual Research Lab and to view sensitive files on computers in the Lab.

To make this possible, we will be using Privaris, a company that specializes in biometric security products. After researching some of the different products that the company offers, we have decided to use a Privaris plusID75, the world's first personal biometric device. It is a physical and logical access device according to the company website. Basically, it is a small biometric token to protect a room or building that the user wants. The Privaris instruction manual also states that the plusID75 is used for passwords for computer logins, secure email, and internet access. For TwoHands, it is vital that we make sure the Research Lab is as secure as possible. To implement this, we would start by downloading the software that comes with it to the computers both inside the actual Research Lab as well as the computers that grant access into the lab. This software will allow certain employees to enroll in the security program so that it can link a specific user to a specific device. Throughout the enrollment process, the employee of the Research Lab will scan their fingerprint so that the software will recognize the user when they want to gain access. They will also assign credentials such as a PIN number to the buttons of the device according to the instruction manual or a one-time password which will help grant them access to the Research Lab using an existing card reader outside of the door.

The actual process of getting into the Research Lab using the device is quite simple. The employee walks up to the Research Lab door, and holds their plusID75 device up to the receiver device next to the door. They then swipe their fingerprint on the sensor on their plusID token. If the fingerprint swiped matches the fingerprint that was enrolled with that specific device, then the door will unlock. A low and high frequency RFID is used to communicate with the receiver located next to the door. Once inside the Research Lab, the employee will then use the same exact process to logon to the computer located in the lab. The user plugs the device into the computer via the USB port or Bluetooth. If a successful biometric scan takes place, then the device will generate the one time password or allow the user to enter their PIN to login. This method will ensure the utmost security for TwoHands.

With the Research Lab being arguably the most important part of TwoHands and the key to future successes, it is important that we deploy top of the line security procedures to keep the information in there safe. That being said, higher security means more expensive products. The Privaris plusID75 costs $150 per device. Assuming TwoHands is a medium sized company with about 30 employees working in the Research Lab that comes out to $4500 total to buy and implement this system right away. This is very cost effective because it is extremely affordable and also provides a high level of security making it worth the cost. It also saves TwoHands a lot of money since they do not have to keep buying new tokens every few years and they do not have to spend money continually updating password and PIN systems.

Utilizing the plusID75 as the security protocol for the research means very little maintenance and management for the device. The device can get about 1000 uses on each charge. This can be solved by having employees charging it while the device is not in use. Managing the devices is not hard either considering each employee needs to only be enrolled once to use. The administrator can also manage the access each employee can have by simply plugging their device into the administrative computer and switching on or off which doors their device can gain access to. The same goes for adding new employees or removing employees who no longer work for TwoHands. The administrator can plug the device in and add or remove their access privileges. Credentials that are assigned to the device only have to be updated at the discretion of the employee and the authentication does not need to be updated because it is very strong and will always remain strong through the use of biometrics.

In the first report, we identified multiple potential vulnerabilities that could target the Research Lab. The problem of unauthorized personnel getting into the lab is eliminated because the system uses biometrics to get into the Research Lab and logon to the computers. If the fingerprint that is swiped does not match the fingerprint that was enrolled with the device, then access will not be granted. The same goes if the PIN number assigned does not match to the PIN enrolled. It also eliminates the chance of hacking into a database and getting a hold of the biometric data because that information is stored on the device itself and not a network database.

Section 3: Firewall Deployment

To further ensure the security of the TwoHands Corporation, a robust firewall system should be established. The firewalls employed will help to monitor traffic going in and out of both the Human Resources and Research department, and prevent malicious actors from accessing these networks and the sensitive data they contain. By placing firewalls in the correct places and establishing rules specific to each department, we aim to meet the very different needs of both departments in the most secure way.

Human Resources and Payroll: Software Firewall

The Human Resources and Payroll department differs greatly from the Research Lab and other departments of the corporation and therefore requires its own unique firewall implementation. Due to the increased amount of employees and various roles played by the department, a software firewall is a great choice. Comodo Firewall, a software firewall, will be applied to each individual workstation in order to ensure that they are kept safe and secure. Software firewalls are highly customizable and will fit the needs of the department perfectly.

Comodo firewall features several unique features that make it a perfect fit for people in the Human Resources and Payroll department, who may not be as technically oriented as other members of the organization. Comodo contains a feature they call DDP or Default Deny Protection, which consults a database of known attacks and alerts the user if any suspicious activity is detected. This feature will likely come in handy because unlike the Research Lab, the Human Resources department may need to access many different software applications other than basic information gathering, like financial transactions and other things.

This firewall also features application control, sandboxing, and a training mode that lets the firewall learn which applications are trusted and minimize alerts to the user. These features, from a safety and convenience standpoint allow Comodo firewall to protect the users dynamically, and avoid distracting them with intrusive dialog boxes. Application control in particular is a major feature of any modern firewall and helps to ensure that rules are developed and maintained on an application level basis. This makes sure that anytime a new or foreign application tries to create traffic, it does not go unnoticed, ensuring that the TwoHands Corporation will stay one step ahead of attackers.

While the security of the Human Resources and Payroll department is extremely important, it makes sense financially to only have one layer of protection. Also, because each individual system will have its own firewall, a breach of one machine does not put the entire network at risk. Also, the Human Resources and Payroll department is less likely to be attacked than the Research Lab, so one layer of firewall protection, along with various other methods of network security is enough to keep the department secure in a costly manner.

The specific firewall rules for the Human Resources and Payroll department will be slightly different than the other departments and initial assessments will likely block some features used, but an aggressive policy will be put in place to protect the department as best as possible. Below are the settings recommended for the Comodo firewall to be used.

Comodo Firewall Rules

Firewall Rule	Packet Destination	Source Address	Destination Address	Packet Type	Source Port	ACK	Action
A	Outgoing	Internal	External	TCP	80	*	ALLOW
B	Outgoing	Internal	External	TCP	22	*	ALLOW
C	Outgoing	Internal	External	TCP	443	*	ALLOW
D	Outgoing	Internal	External	TCP	465	*	ALLOW
E	Outgoing	Internal	External	TCP	995	*	ALLOW
F	Outgoing	Internal	External	TCP	25	*	ALLOW
G	Outgoing	Internal	External	*	53	*	ALLOW
H	Outgoing	Internal	External	*	*	*	DENY
I	Incoming	External	Internal	*	*	*	DENY

These rules are fairly intensive and allow through many common protocols that would be used by employees of the Human Resources and Payroll Department. All outgoing HTTP and HTTPS traffic is allowed (Rules A and B) as well at FTP (Rule C) for some applications. Also, SMTP and POP3, protocols used for email are allowed (Rules D, E and F). DNS is also allowed to ensure that web traffic flows smoothly. These basic rules, along with the advanced features of Comodo firewall and other security measures put in place will help to keep the Human Resources and Payroll department secure.

Research Lab: Hardware and Software Firewalls

Due to the importance of the research lab to the corporation's success, network security is an extremely important issue that should be handled quite thoroughly. To ensure that all connections to and from the Research Lab are legitimate, two layers of firewalls will be used. While deploying two firewalls does present additional costs, it also helps to protect one of the most crucial departments in the entire corporation.

The first of the two firewalls will be a Cisco ASA 5500-X hardware firewall, installed at the perimeter of the network. This particular firewall is a type of next-generation firewall that features many advanced features including: granular control of applications, stateful packet inspection, an intrusion protection system, secure remote access and protection from botnets. These features, along with general firewall functions will help to make sure that the Research Lab stays as secure as possible.

As previously mentioned the Cisco ASA 5500-X firewall uses stateful packet inspection, which is a type of packet inspection that keep track of connections and allows packet in only if they are part of an existing connection, or are in the process of completing a three-way handshake. This helps to prevent spoofing attacks and provide context to packets attempting to enter the network. This provided context may help to prevent attacks that would circumvent the formally described rules defined by the firewall.

Another feature of this hardware firewall is application level controls. These controls provide an added layer of security by checking which applications packets are going to and from and allowing or denying them based on predefined rules. This application based approach allows for a finer tuned firewall that will be more effective in preventing attacks and malicious content from entering the network.

The Cisco ASA 5500-X also features an Intrusion Prevention System, which acts as another layer of security by detecting malicious activity using different, context based detection methods. Examples of methods employed by Intrusion Protection Systems include signature based, anomaly based and protocol analysis detection. These methods work by keeping track of patterns in network activity and rejecting any traffic that seems out of place. They also refer to predefined attack signatures and compare network traffic to them to see if any known attacks are possibly being carried out. The Intrusion Prevention System features of this firewall will definitely help to protect the Research Lab and ensure attackers are kept out.

With all of these advanced features, the Cisco ASA 5500-X will help to provide a variety of security features that will keep the Research Lab's network secure. To ensure that all necessary traffic is allowed and nothing else, a set of rules must be determined and will be provided below, along with a network topology diagram to show how the firewall will be implemented physically.

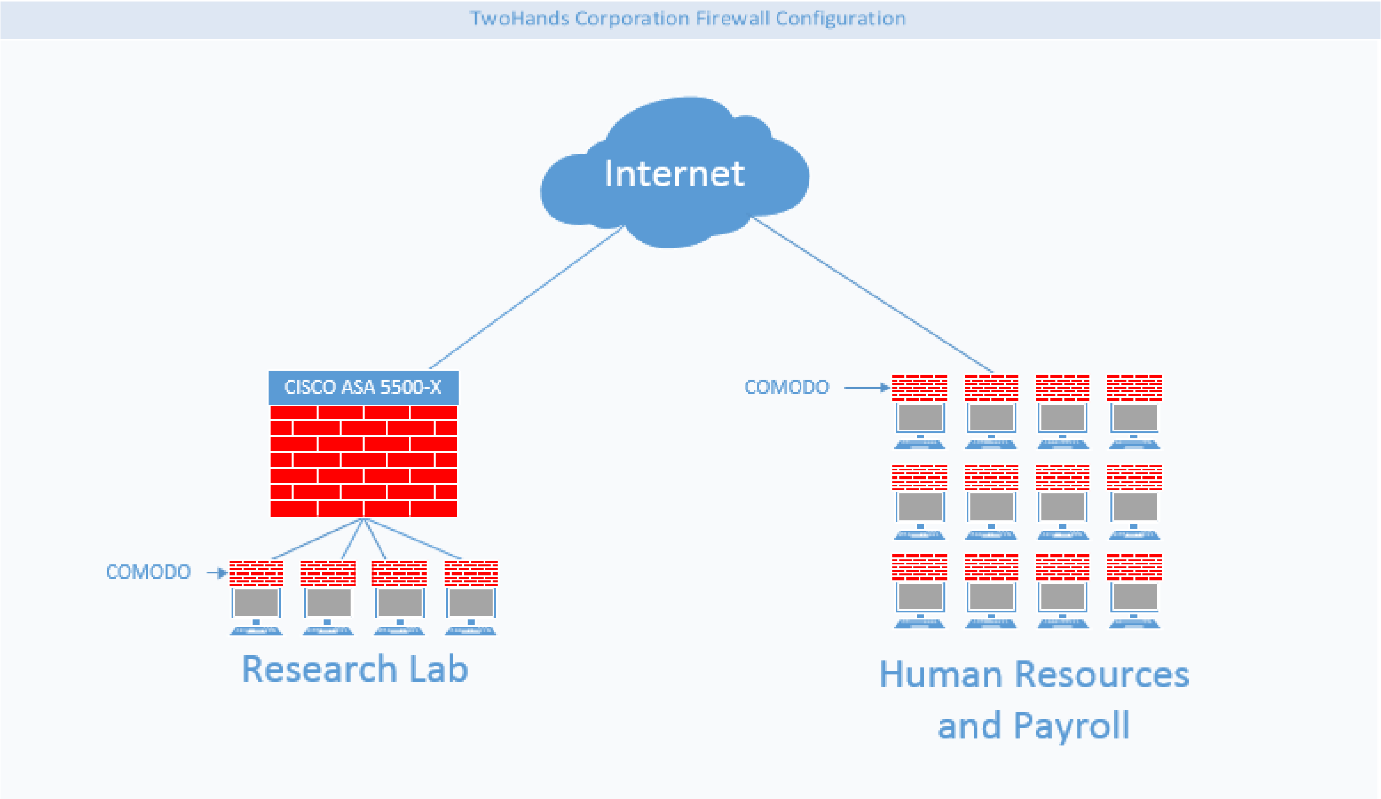
Cisco ASA 5500-X Firewall Rules

Firewall Rule	Packet Destination	Source Address	Destination Address	Packet Type	Source Port	ACK	Action
A	Outgoing	Internal	External	TCP	80	*	ALLOW
B	Outgoing	Internal	External	TCP	22	*	ALLOW
C	Outgoing	Internal	External	TCP	443	*	ALLOW
D	Outgoing	Internal	External	*	*	*	DENY
E	Incoming	External	Internal	*	*	*	DENY

These rules are put in place to ensure that only required protocols are allowed and everything that is unneeded is denied. All incoming traffic, regardless of protocol or packet type, is denied. Due to the fact that the research lab is a secure facility and workers will have to enter the facility to access the network, all outside connections are denied. The goal of this is to ensure that no intruders can connect to the network and only authenticated users within the physical building have access to the network. The outgoing rules are a bit more detailed and allow traffic to pass through port 80 (HTTP), 22 (SFTP) and 443 (HTTPS). These services are required by the researchers so that they can access outside information through HTTP and HTTPS as well as SFTP. These rules ensure that only outbound connections are allowed and that intruders cannot connect to the network.

Due to the high importance of the Research Lab's computing, Comodo firewall will also be installed on their machines to ensure additional security in case a hardware failure, or attack. By adding redundancy to the system, it can be ensured that the Research Lab will stay protected from intruders. The Comodo firewall software (as previously mentioned) is highly customizable and will be set up in a fashion very similar to the Cisco ASA 5500-X hardware firewall, to stop any potential intruders in case they manage to circumvent the perimeter security.

Network Topology:


TwoHands Corporation Firewall Configuration

As seen in the network diagram above, the Research Lab features two layers of firewall protection, protecting the entire network, and each individual machine. Human Resources and Payroll is protected by a firewall on every individual machine. These strategies previously discussed will help to keep TwoHands Corporation secure.

SECTION 4: DATA CONFIDENTIALITY DEPLOYMENT

Now that we have multiple security mechanisms, it is essential that they do their jobs and protect valuable data within TwoHands. Ensuring the protection of data is the goal of our security consultation and we firmly believe that the products, software and protocols that we want to instill are effective and will perform to the highest level of security.

In using the RSA SecurID, employees will be increasing their security because instead of using a password that they set and use for an extended amount of time, they will be using a device to give them a new password every minute. This refers to the security aspect of "what you have" which greatly enhances security by not allowing anyone access without possession of the device.

This additional security does not only protect against attacks on customers private data but also protects against attacks on supplier and vendor's data. The reason that this is possible is because every employee is required to login to the system using the RSA SecurID no matter what information they are trying to access. Every time a new transaction takes place, information is updated, employees are hired, etc., it is required that the user first authenticates themselves by signing in securely. Additionally, this information is encrypted on our servers. Employee or customer information cannot be received/sent without properly encrypting/decrypting it first. It is extremely important to us to keep this information as confidential as possible. This ensures that not only the customers data is secure but also that the supplier and vendor's data is secure as well.

In order to further ensure that the information on our servers is secure we will schedule backups to occur monthly using Acronis. Acronis is a company that provides software which backs up data from a business onto its own servers. This will save all the information in the Human Resources and Payroll department so that if for some reason the data was lost, we would be able to get it back.

This Acronis software can be implemented immediately and is very easy to use. Once it is set up we can schedule how often we want our information to be updated. In order to ensure that the backed up information is as secure as possible, Acronis backs it up using AES encryption. This is a standard encryption service that encrypts in either 128, 192, or 256 bits. This is extremely important because if an attacker could hack into our backup with no problems then there would be no point in all the changes we had made in implementing the SecurID.

The initial price to purchase the software will be $1000. This is a small price to pay for this valuable service. This software will help protect against the vulnerability of our servers crashing and us losing all of our customer, supplier, and vendor information. If this event did occur and we did not have a backup, TwoHands would be set back extremely far and could even go out of business. This information is extremely valuable to the company and the risk is too high to not have a second copy of all of this information. The benefits absolutely outweigh the costs and every time an upgrade comes out for the software it is free to install. This allows for a good maintenance plan because we are able to continue to use the services of one company even as security changes. We will be able to keep our information as up to date as possible knowing that we always have another way of obtaining it.

Research Lab

By using the Privaris plusID75 device, you are incorporating multiple security methods such as credentials and biometrics. After explaining how it is used, concerns about the device's security may begin to arise and how it could be potentially exploited. According to the Privaris website, all of the biometric processing, including the enrollment and template matching is performed on the user's personal device that they carry around. This means the data is never stored on an external server or database which would certainly be vulnerable to a cyber-attack. For the computer logon aspect of the device, two ways can be utilized. The user can either manually assign a PIN number to their device that will be entered when logging onto a computer. The user can also utilize the one time password feature that the plusID75 model comes with. Using this method, a SecurID one time password is generated by the device only when a verified biometric scan occurs. They then plug the device into the USB port or use bluetooth for this password to be used or they are allowed to enter their own PIN to login.

This entire process works with RSA SecurID systems and uses three-factor authentication to protect the data. It also uses an extra layer of encryption for Bluetooth to make sure the data is secure when transmitted between sender and receiver via Bluetooth. Two way encryption is also utilized to ensure that there is no point throughout the process that the data is vulnerable. The token itself also uses a secure ASIC processor and the fact that the device is only active for a few seconds (after a finger swipe) means it cannot be sniffed or cloned by a potential hacker. This means that when you are scanning your fingerprint and the device is sending the authenticated scan data to the receiver, the data is encrypted the whole way to ensure it cannot be compromised at all. The security software, HID idBank, is bought with the device and is used for data encryption and we have decided to buy 50 of them because they only come in certain quantities and this number will cover the number of employees in our Research Lab department. This software is priced at $100 per unit while buying a quantity of 50 that will come out to $5000 total. The software will contain card formats (access control IDs) that will enable the device to be used in the place of a card, which in this case will be used to open the door to the Research Lab. By using this, Privaris stresses that the company will dramatically reduce password and pin maintenance costs which can pile up. You are also saving costs on having to buy new security tokens that have to be replaced every few years or so.

The biggest thing TwoHands is considering is how using this device will make their Research Lab more secure. The biggest concern is that an unauthorized user breaking into the lab either physically or remotely via a computer and stealing data. This important data is the future of TwoHands and could potentially make them a lot of money meaning the data is very valuable. Using the Privaris plusID75, an unauthorized user cannot physically break into the Research Lab because the device uses biometrics. Without the authorized fingerprint, there is simply no way to physically get in. Even if one of the tokens were stolen or lost, it would be absolutely useless in the hands of another user because of the biometrics. The security is so good that another user could not even use a fake fingerprint to get into the device because the device itself looks deeper into the skin than just the fingerprint rendering a "gummy attack" useless. Addressing the problem of acquiring access information to get into the lab or lab computers, this vulnerability is also protected. The enrolled data is all stored on the tamper resistant device and not on any external servers or databases. This eliminates the chance of a hacker remotely breaking in to steal login information in some way and use it to gain access. Finally, the information is encrypted at all points when it is being transmitted back and forth between the device and the receiver along the door. They even added an additional layer of encryption to the Bluetooth aspect so that the TwoHands can be assured their data is safe at all times. All in all, the device is excellent in protecting the data as well as being an easy yet secure means of access control for the Research Lab.

SECTION 5: COST ANALYSIS

For the Research Lab, TwoHands would be required to purchase two different products. The first of these things would be the biometric token, the Privaris plusID75. This token costs $150 each. With 30 employees in this department, the total cost for the biometric tokens is $4500. TwoHands also has to buy supporting software which costs around $100 per unit. Since the software is only sold in certain quantities, the company would have to buy the package of 50 units. This cost comes out to $5000. Adding up both costs, it would cost TwoHands $9500 to protect the Research Lab department at the highest level of security. This is a feasible cost because it will protect the department for a long time while continuously being secure. They will also save on costs of bringing in another person to manage the security of the device because it can be simply added into the current security plan without adding any extra employees. A few minutes of training is all it takes for one to know how to properly use the device.

For the Human Resources and Payroll Department, TwoHands would need to purchase two different products as well. The first product that would be purchased is the RSA SecurID SD200 devices. These devices will be purchased in a bulk of 50 devices costing $2,125 or $42.50 each. In addition, the Human Resources and Payroll department will also be purchasing the Acronis software in order to securely back up the information on its servers. This will cost the department $1,000. Therefore, in total the Human Resources and Payroll department will be paying $3,125 in order to increase its security. These purchases are feasible because it is greatly reducing the risk of attacks which could lead to tremendous setbacks. It will be much harder to attackers to get into the department's servers and the servers will always be backed up if anything happened to them. In addition, this is feasible because the employees will be accepting of it and will understand how to use their new devices after a quick training session so no experts will need to be paid to manage the devices.

In order to implement the proposed firewall solutions, two main purchases must be made. The most expensive item that needed to be purchased is the Cisco ASA 5500-X hardware firewall. This firewall costs $3,200, a price that is definitely justifiable consider the importance of its' job. Also, it will not need any costly updates on a regular basis, so the running costs should be relatively low. The other piece of firewall equipment that needs purchased is the Comodo Firewall software. This software costs $40 per computer per year. This means that assuming the Research has 30 computers, and the Research Lab approximately 20, the approximately yearly cost will be (50*40/year) about $2000. Combining this with the $3,200 price tag of the hardware firewall, around $5,200 will be needed to fund the firewall implementation. This is a relatively low cost for protecting sensitive data from intruders, and is definitely an investment worth making.

Item	Amount	Cost
Privaris plusID75	30	$4500
Privaris Software	50	$5000
RSA SecurID SD200	50	$2125
Acronis Software	1	$1000
Cisco ASA 5500-X	1	$3200
Comodo Firewall	50	$2000
Total Cost: **$17,825**		

WORKS CITED

"Best Backup Software for Data Protection and Disaster Recovery." *Best Backup Software for Data Protection and Disaster Recovery*. N.p., n.d. Web. 25 Apr. 2014. <http://www.acronis.com/en-us/>.

"Campus Technology." *CT Solutions* --. N.p., n.d. Web. 25 Apr. 2014. <http://campustechnology.com/Articles/2008/05/CT-Solutions.aspx>.

"Cisco ASA 5500-X Series Next-Generation Firewalls - Products & Services." *Cisco*. N.p., n.d. Web. 25 Apr. 2014. <http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html>.

"Deploying Firewalls Throughout Your Organization." *Cisco*. N.p., n.d. Web. 24 Apr. 2014. <http://www.cisco.com/c/en/us/products/collateral/security/ios-firewall/prod_white_paper0900aecd8057f042.html>.

"Firewall Protection." *Firewall*. N.p., n.d. Web. 25 Apr. 2014. <http://www.comodo.com/home/internet-security/firewall.php>.

"Privaris - Biometric Security - PlusID." *Privaris - Biometric Security - PlusID*. N.p., n.d. Web. 25 Apr. 2014. <http://www.privaris.com/products/index.html>.

Privaris. N.p., n.d. Web. 25 Apr. 2014. <http://www.privaris.com/pdf/plusID%20Manager%20Quick%20Start%20Guide.pdf>.

Privaris. N.p., n.d. Web. 25 Apr. 2014. <www.privaris.com/privarisplusidlow.wmv>.

"RSA SecurID 200 AuthenticatorThe Gold Standard in Two-factor Authentication." *RSA SecurID 200 Authenticator*. N.p., n.d. Web. 25 Apr. 2014. <http://www.tokenguard.com/RSA-SecurID-SD200.asp>.

"RSA SecurID Hardware Authenticators Convenient Two-factor Authentication Security Tokens." *RSA SecurID Hardware Authenticators*. N.p., n.d. Web. 25 Apr. 2014. <http://www.emc.com/security/rsa-securid/rsa-securid-hardware-authenticators.htm#!compare>.