Summer 2010

Layered Security Solutions Over Dependency Within Any Layer

Olga H. Brandt
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Abstract

Considering the advancement of computer systems and security solutions available in today's constantly changing world, there are various philosophies as to what is required (or adequate) in order to protect a system. This investigative study proposed to explore a possible problem with employing a layered security solution – over dependence or reliance on any layer. A risk analysis was performed to determine where over dependence or reliance could happen and what could be done to prevent this. Various reviews and other findings online were researched and the data compiled using a qualitative methodology. Lastly, a recommendation is made on what is needed to prevent this problem from happening and what can be learned from this.

Acknowledgements

Gene Brandt, Cyber Transport, 630 Electronic Systems Squadron, Hanscom Air Force Base, Massachusetts – Thank you for answering my questions regarding layered security, vertical stacks, and defense in depth and supporting me throughout this endeavor.

Helen and Olga Brandt, Lovely Daughters – Thank you for all your support and encouragement in understanding why I had to do this and telling me to hurry up.

Stella Duenas and Jo Bower, Best Sisters – Thank you for being proud of me. Ditto.

Table of Contents

Chapter 1 – Security Threats

Since computer systems have become a part of everyday life, protecting the computer system from various threats has been a critical aspect of security in Information Technology (IT). As IT has advanced so have the threats become more complex and frequent. Oppliger (1997) states, "In November 1988, Robert T. Morris, Jr. launched an Internet Worm flooding thousands of hosts". At that time, security incidents started growing exponentially (Oppliger, 1997). The seemingly endless hunt for a solid, complete security solution is perpetuated by the continuously growing onslaught of threats to computer systems. According to Perrin (December 2008), "there is no real possibility of achieving total, complete security against threats by implementing any collection of security solutions". Whether the threat is in the form of a hacker, spam-ware, virus, Trojan horse, etc., protecting computer systems from unwanted intrusions is likely to remain at the forefront of consumers' minds when implementing a security solution to protect their computer system.

Currently, other than keeping a computer system detached from the world or unplugged from the Internet in order to protect it from threats, there is no permanent solution to protect a computer system. According to IObit.com (September 2007), no security solution today offers 100 percent effectiveness at detecting viruses and malware. Businesses and people want and need to be connected to the world in order to perform their jobs, handle business and personal transactions, and communicate with the world in general. As of now, computer systems require various security measures to try to keep them safe from most known threats or attacks. These security measures include but are not limited to using firewalls, anti-virus and anti-spyware software programs, automatic updates, passwords, intrusion detection systems, malware scanners, integrity auditing procedures, and local storage encryption tools. Consumers need

more information in order to employ a well-rounded security solution that will work the best for their needs or they may rely on one aspect too much in trying to protect their system and still fail in the end.

Internal Threats

Under the category of internal threats are various factors easily over-looked. There are insider threats including malicious intent and negligence by employees. Spear phishing and theft of equipment fall within this category. Plus, administration of the system can inadvertently be an internal threat.

Insider threats may be some of the most difficult to protect against. Even though this threat is the most unlikable one, being concerned any of the employees could be harboring thoughts of malicious intent, whether in the form of espionage or discontent, is a difficult pill to swallow. There are also many cases where the system administrators are too busy and do not always have the time (or forget) to actively update the users' access and privileges. The internal threat may be something as benign as not protecting passwords (or allowing people over the shoulder to see the user id and password as they are typed in), so ill-will harboring people walking by may gain access to a system they are not authorized for. In these instances, employing stronger and more simplified solutions that automate policy enforcement and delegate administration for user provisioning is the optimal fix.

Another internal threat becoming increasingly more popular is the spear phishing attempts usually directed at organizations in an effort to gain unauthorized access to sensitive information. These email spoofing fraud attempts are almost always indistinguishable from the real thing in these current times. For those that are unaware or unlucky, they may have inadvertently opened the doors to criminals. Once this happens, the criminals now have access

to passwords, confidential or proprietary data, financial data, or unauthorized access in general for whatever purpose they choose. To help mitigate this threat, security strategies include implementing anti-phishing toolbars displaying a web site's real domain name and keeping track of popular phishing sites for employee reference.

Alarmingly, another threat is the disappearance or theft of people's laptops (or some form of media storage device). For companies this can be a devastating and costly happenstance, especially if there is proprietary or personal information involved. These tools or accessories may allow the thief or unscrupulous individual access to financial information, personal data, or proprietary data. This may be more alarming because there are still a good percentage of companies that do not have or enforce policies dealing with removable storage media. A recommended fix is to initially adopt and implement a policy regarding removable storage media, require employees to use start-up passwords on their laptops, frequently delete old emails, text messages, and any other unwanted files from the media, and make use of any encryption or other security features associated with the device.

In this age, new security software comes out frequently but does not always keep pace with the various holes found once released. This means companies and users are waiting a longer period of time for the latest and greatest patch to be released hoping current holes will be fixed. Another compounding factor may be security administrators not taking the time to ensure all updates and the latest security patches get installed. This dilemma can be resolved by using patch management software and services. These internal threats whether in the form of insiders, spear phishing, loss of equipment, or administrative in nature may be a cause in over dependence in a security layer just like external threats consisting of Trojan horses, hackers, viruses, spam mail, and natural forces.

External Threats

Some external threats are confused with others because they appear to attack the same way (i.e., Trojan horses and viruses). Trojan horse attacks are one of the most serious threats to computer security. A Trojan horse is an evil, security-breaking program in the disguise of something non-threatening. A user will download a file and by clicking on it they unwittingly release a dangerous program that begins causing havoc with the system, steals certain personal information, or allows the owner to get into their system. Trojan horse prevention entails never downloading something from another user or site not 100 percent recognizable, opening something if the person does not know what it is, being aware of hidden file extensions, turn off all automatic preview features, and do not become complacent because the anti-virus software is up-to-date.

Another external threat comes in the form of individuals that know how to modify computer hardware and software in order to accomplish some goal outside the original developer's intent. These individuals are known as hackers. Hackers hack computers for various reasons including just trying to prove themselves, educating themselves with the hardware and software, or wrongfully breaching someone's system in order to wreak havoc or gain access to information they are not authorized to have (also known as a cracker). A solution has been for companies to hire these hackers in order to find weaknesses in their systems so they can be fixed to prevent identity theft or other important computer crimes.

Viruses are another prevalent threat to information security. Continuously changing and growing in number, people will take advantage of the emergence of social networks (i.e. Facebook, Twitter, etc) to lure users to bad sites. Malware threats are taking greater advantages of users accessing online applications. Trojans evolve all the time and are predicted to easily

bypass the protections put in place by banks. For instance, one new technique involves a Trojan's ability to quietly break into a legitimate transaction, withdraw money, and get away with it because it is able to check the user's transaction limit to keep from alerting the bank (Perone, 2009). Along with Microsoft Office applications, Adobe Acrobat Reader and Flash are being exploited by cybercriminals. Plus, organizations and users need to beware of their computing power and bandwidth being siphoned away by others for their own use without obtaining it legally through the use of botnets. The best defense against viruses is to keep all anti-virus software up-to-date, make sure the entire system (desktop, file, and email server plus the internet gateway) is protected, employ centralized management, and some form of an auto update program.

Next, spam mail is when someone decides they want to bombard an email server with a lot of meaningless emails or junk mail. Usually the junk mail comes in the form of jokes, advertisements, solicitations, etc. Another form of email that is threatening to a server is known as chain mail, where an individual sends an email asking those who read it to forward it to as many people as they can and keep it going. Whether the intent behind it is positive or ill-meaning, the result can still be negative because it degrades the performance and response time of the server. At this point, the server is overwhelmed requiring administrators to take it offline, clean it up, and put it back online. An obvious prevention to spam mail is to create a security policy regarding its use, distribute to all employees, and emphasize the importance of adhering to the policy and the consequences to those that do not follow it. Also, implement anti-spam security measures and continuously keep it updated or install any necessary patches.

Even though forces of nature may not always be considered a threat, many companies, organizations, or individual users need to consider them when developing their security policy

and contingencies. Forces of nature range from fires to floods to severe weather including hurricanes, tornadoes, earthquakes, etc. When these types of threats happen, they can cause the most physical and financial damage because loss of life, equipment, and data can result. For natural disasters, the appropriate security measures should be put in place to mitigate the amount of damage resulting from an actual occurrence. Depending on the threat, thoughts need to revolve around the physical location, best practices for protecting the equipment and data, evacuation plans, information for people to know what to do in case of an occurrence, and various other protective measures.

Chapter 2 – Review of Layered Security & Over Reliance on Any One Layer

With all the various threats facing users and organizations alike, whether internal or external, they need to be taken seriously and appropriate security measures put in place to protect against them. Just as there are a multitude of threats to protect against, there are a variety of security solutions available in the marketplace. Then again, there are different systems (single or multiple) requiring information security protection. Depending on the information to be protected, the system being used, and the owner, these factors play a part in determining what security measures are implemented.

Layered Security

Layered security can be implemented at any level within an information security strategy. This approach can work for anyone, whether they are a system administrator of their own machine accessing the Internet from any location, or the information network help desk person sought after by company employees with network problems. What users need to realize is that no solution is perfect. "Any single defense may be flawed, and the most certain way to find the flaws is to be compromised by an attack – so a series of different defenses should each be used to cover the gaps in the others' protective capabilities" (Perrin, 2008). For example, firewalls are used to provide additional levels of defense supporting traditional routers giving more capability for tighter and more complex rules for communication between network segments or zones. They can be used to incorporate demilitarized zones (DMZs) to protect the control network with several DMZs being created for various functionalities and access privileges. Intrusion detection systems can also be used to monitor a network for unauthorized or even unusual activity.

Based on the various kinds of threats listed above, having multiple layers of security to protect a system becomes obvious. Some of the threats can be prevented or mitigated by

developing and enforcing a strong security policy for a single user or networked system. Another measure may be to tighten down on read/write controls for multiple applications. The measures taken to physically secure a system are additional steps in providing protection from various threats.

When thinking of layering security, not only should there be one layer being looked at to protect. According to Bouchard and Mangum (N.D.), “threats are becoming more elusive” and “hackers are shifting their attention to focus less on exploiting network-layer vulnerabilities and more on those associated with application services, logic, and data itself”. A more traditional approach to layered security included firewalls, Virtual Private Networks (VPNs), spam filtering, antivirus, and intrusion prevention. However, this older layering method did not necessarily have these functions working together or integrated in a way enabling the user to leverage information regarding one layer to make other layers more effective.

Today, there are newer layered security solutions that enable greater flexibility and allow for the intelligent cooperation amongst the various layers providing for dynamic detection, blocking, and reporting of malicious traffic, but letting benign traffic through efficiently. One such layered security solution is the Intelligent Layered Security (ILS) Architecture. In this architecture, there are six layers. The external security services layer provides for technologies extending protection beyond the firewall and gives information empowering the user or the administrator to be more efficient. In the data integrity layer, the data packet integrity and packet conformance is validated. At the VPN layer, secure and private outside communications is ensured. The stateful firewalls layer restricts traffic to certain sources, destinations, and ports specified within the security policy. Within the deep application inspection layer, conformance to application layer protocol standards is enforced, dangerous files with certain file or pattern

types are blocked along with risky commands and changing of data in order to prevent any sensitive system information leaks. Plus, the content security layer includes a gateway antivirus, intrusion prevention, anti-spyware, spam filter, and URL filtering.

Single Layer Over-Reliance

Many users when trying to secure their system have experienced failure in one area or another. There are those whose IT knowledge is fairly limited. In these instances, users may only think that by implementing a very strong firewall they significantly reduce their chances of getting attacked. This is not to say these users will not have some form of anti-virus, anti-spam, malware protection in place for their system. Only that they concentrate on one area of security for their system, not realizing that by doing so they are actually leaving other areas susceptible to attack or in weakly protected state. An article in TopTenReviews (N.D.) discusses the importance for users to acquire and install an internet security suite on the PC to help protect the system from online threats. Another example of single layer over dependence is those users that use their system for mainly accessing the Internet for their needs, so they acquire and implement a security solution with strong protection against online threats.

There are many users spending lots of money on intrusion detection and/or firewall systems as they are designed to protect the system perimeter. Unfortunately, what many people do not realize is the perimeter is considerably more permeable than thought. This means a great many security breaches occur at the application layer and not the physical layer – nearly 70 percent according to Gartner (Adams, N.D.). Companies will do this because they feel they need to beef up the external layer when opening it up to remote employees, customers requiring access to various applications, and other business related reasons. Part of the problem seems to stem from software developers not having the same strict guidelines when it comes to creating

software, so the end result is a product with vulnerabilities. By concentrating on the perimeter, users and companies will overlook several security vulnerabilities, maintain and provide a false sense of security, and perhaps give greater opportunity for harmful business logic attacks.

Research Factors

Users cannot just think about the best way to harden the perimeter. Emphasis must also be placed on the application layer, and the network layer, and the system layer, etc. When thinking about strengthening the application layer, the issue arises regarding how to write secure code. According to Adams (N.D.), roughly 64 percent of software developers are not confident in their abilities to write secure code for applications. With such a high chance for attacks at the application layer, seeing the majority of money and time being spent on the perimeter for protection versus improving software at the application layer is troubling.

Another reason for lack of confidence in writing security codes may be the way researchers and developers think about what they are creating to help provide security for a system. According to Campbell (January 2006), human intuition can be viewed as a model for familiar events, which means researchers and developers will take into account certain assumptions about how things will act in various conditions. However, the basic assumption may be inconsistent with the actual behavior or nature of the threat leading to less protection for the system than thought. For example, the origin of the threat is usually viewed as coming from outside the network with the sole intention of subverting defenses through weaknesses in accessible applications. Hence, the thought is if the external threat origin is unable to access an application inside the perimeter, then everything within the perimeter is safe from external attacks. In this case, the thought may be to disallow any remote users from connecting to an internal device. As technology has changed, so has the method for attacks. Now, users and

companies need to be concerned with client-side attacks which include hostile email attachments and Web pages that let arbitrary code run in light of security problems within the browser or email client.

Chapter 3 – Risk Analysis Methodology

This study focused on researching the problems arising from users and administrators relying on one layer of a layered security solution. In order to assist in making this decision, a qualitative methodology encompassing secondary research and risk analysis was conducted. The various kinds of threats, ranging from a human factor to political factors, was identified which can be an influencing factor in concentrating more heavily on one layer. Next, the risk potential associated with the over-reliance on any given layer and what the assessment of this impact may be was studied. Once this had been accomplished, what could be done to manage each risk based on its value was looked at. Finally, a decision was made regarding if changes in the security solution were needed.

Interpretivism

In using interpretivisim as a qualitative research methodology, insights can be gained by discovering meanings through enhancing comprehension of the whole. The entire layered security process must be examined in order to understand it better. By studying layers of a security solution and how they can be affected by multiple internal and external security threats, discovering why or how users may come to rely heavily on one layer can be seen. This way a perspective is provided into the possibilities for single layer over reliance.

A problem is many security professionals end up narrowly focused on a single layer which creates a risk by itself. This risk analysis uses a qualitative methodology to develop risk mitigation strategies for their infrastructures. In the process of describing the various internal and external threats, performing a thorough risk analysis is validated. With this validation, using a layered security solution is still considered the best security protection a user can have for their system.

Identify Threats

When performing a risk analysis, the first thing to do is attempt to identify all the different forms threats may arise in. Threats can come in the following forms: human, operational, reputational, procedural, project form, financial, technical, natural, and political. The human threat can be an internal or external threat. From an internal perspective, the risk analysis needs to take into account an individual that may be uneducated in security policies, unfamiliar with computers, or perhaps working against the company by trying to gain unauthorized access to parts of the network. Identifying the external human threat takes into account people trying to gain access via multiple methods such as using human illness, death, etc to gain access into the system.

Operational threats to consider when doing a risk analysis are things that can or will cause disruptions in the day-to-day supplies or running of the business. Anything causing failures in the distribution chain is an operational threat to be considered. Any causes for lacks of access to equipment or essential assets to the business or network should be brainstormed. Even people being out of the office and needing to work from a remote location is an operational threat to consider if they are unable to gain access from a remote location.

Reputational threats are not necessarily tangible or easily identifiable. These types of threats will be caused by the business losing face with any, some, or all of its customers or business associates. Employees becoming unhappy or disillusioned with the way the company is doing things or with decisions made by management is another reputational threat to be aware of. In these situations, negative publicity will cause damage to a business' reputation with perhaps long reaching consequences.

Some threats needing to be identified are procedural in nature. Not necessarily the kind of threat a person may initially be concerned with, but nevertheless a threat needing to be considered when performing a risk analysis. Procedural threats arise in the form of accountability issues spiraling out of control. They may occur when internal measures and controls are not practiced and followed. Employees within an organization committing fraud or when organizational policies are not enforced will become procedural threats causing severe repercussions for the organization.

A different kind of threat to think about is anything related to the success of business projects. Should the cost of the project push to the right creating cost overruns; this is a threat to the success of the project. This may then threaten the company's reputation depending on the size of the project. Depending on the type of project, any delays in schedule would be a threat. Derailments in the management of a project such as service or product quality are also threats to be considered. When projects fail enough times, business longevity then becomes jeopardized.

A threat to any system or network is always the financial constraint. Whether a solution is well planned out or not, the amount of funding available at a given time may delay the procurement and implementation of the solution. There are also other factors of life requiring financial assets that will affect the amount of funding available. Additionally, depending on how well the money is managed when it comes to payrolls, interest rates, investments, etc will have an impact on how much is available to be used for various necessities.

Technical threats can take on many forms as well. One form involves the advancement of technology. Technical failures leading to glitches with applications, loss of data, and possible down time are another form. An effect of technical failures, when severe enough, leads to

discontent amongst the employees and negatively affects their performance even if just for a short time.

Threats of a natural origin are not to be taken lightly. Bad weather can wreak havoc with signals and the transmission of data. Natural disasters can wipe out property, jobs, and equipment and cost considerable amounts of money to recover from depending on the severity of the damage caused by the disaster. Other natural threats originating as diseases or accidents should be considered when identifying natural threats during the risk analysis phase.

Threats of a political aspect should also be thought about as well. Perhaps not so much for individual users, but changes in tax structures can affect businesses. Depending on stances a company may take, public opinion can have positive or negative repercussions. Government policies for various types of businesses can effect what decisions the business will make in following the policy if it applies to them. And if the company deals with foreign entities, the effects of foreign influence need to be thought about as well.

Estimating Risk

Now that the various types of threats have been considered, the next step deals with estimating what the likelihood of each threat happening may be. Estimating the human threat is difficult. Depending on the type of business, the human threat may be considered minimal or extensive. For example, how well have the employees been vetted? To what extent are they trusted? What controls and security policies are in place? Is the information they have access to vital to the operation and integrity of the business? What measures are in place to keep out or mitigate external human threats? When relying too much on the perimeter defense to keep out external human threats, the possibility of overlooking and not defending against the internal human threat exists.

Once the likelihood of a threat has been estimated, the individual or IT team should assess the impact of the threat and determine a value of what the cost will be to the system owner or company. Whether internal or external the human threat will happen, it is just a matter of time, degree, and effect. Determining what the cost will be depends on what kind of damage was done, when it was caught and stopped, and if there were any work interruptions or stoppages due to this threat. Did the impact of the threat cause the network (or part of it) to have to be taken off line? The cost here may be minimal if personnel are still able to work on the system while the effect from the attack is corrected. If the attack caused real information destruction or causes the entire system to be taken down for a while, then the cost associated with that downtime and corrective response is measured in the loss of employee production, company operations, and the cost associated with putting new security measures in place to keep this kind of attack from taking place again. In these instances over dependencies in a layer can be discovered.

Estimating operational risks is tricky. How often are supplies delivered? What are the chances of a delivery not being made? With so much or almost all, of a person's job dealing with computers and electronics, what are the chances of there being a power outage or a glitch causing data errors or corruption? Anything with the capability of disrupting the day-to-day operations of a company must be thought about to determine the possibility of the threat coming to fruition. For instance, ensuring the uninterruptible power supply is fully operational and capable of handling the system load long enough for the system to be shut down properly in the event of a power outage is important to keep in mind. However, along with thinking of the right uninterruptible power supply to have in place, ensuring it will keep the system up long enough for someone to get there to shut down the system should the power go at night is important.

Having an inadequate uninterruptible power supply does no good if in the end the system could not be shut down properly and data was lost anyway.

When estimating the value of a personal or business reputation, this can be hard since they are built over a long period of time but easily lost. Reputations take a long time to develop and maintain. Unfortunately, a bad word or a lapse in judgment or business practice or just plain bad luck can degrade reputations or take them down fairly quickly. People and businesses should look at what losing their reputation means to them in order to know what is required to keep, build on, develop, or shatter it.

Additionally, the cost associated with having to build up a lost or tarnished reputation is extremely high. Part of this is because building a reputation usually takes a long time (i.e. it does not happen overnight, in a month, etc.). The impact of losing a reputation may mean lost business, lost production as employees look for work elsewhere, and trust displacement. Building a reputation back up will require a thorough overhaul of business (or personal) practices which will require being patient, putting forth a lot of money depending on the company, and more time to re-cultivate new and perhaps old customers. With the Internet and usual word-of-mouth recommendations, rebuilding lost or tarnished reputations may be impeded as the impacts of the damaged reputation will be wide spread. In this case, if reputation is everything, then the company will have placed a great amount of emphasis on their hiring process and background investigations. Once an individual is inside, they may have free rein everywhere. The company may not be concentrating on some internal layers of security because they put so much emphasis on the hiring and vetting process, which may lead to them discovering differently down the road.

With procedural threats, are there any reasons or issues currently known that would give management concern? Procedural lapses may be apparent. At management's request, an outside

source came in, performed a review, and provided a report to them on what was occurring along with one or a few options for fixing the problem. Another thing to consider is if procedures have been running fine, but perhaps there is the concern of complacency developing amongst the employees.

Assessing a procedural concern can be straight forward, but determining the cost associated with a procedural lapse may not. Not following a procedure can lead to unauthorized access to someplace in the network, leaving infrastructure unprotected, not shutting down properly, and maybe something as simple as leaving user identifications and passwords in an unsecure fashion. Placing a value on procedural lapses can be as little as zero because co-workers keep others in check and remind them of what they are supposed to do. However, the value may be as high as having to reassess the current procedures in place, put new ones in place, enforcing the new procedures, and perhaps being involved and paying out royalties and judgments due to a suit because procedures were not followed and privacy act or proprietary information was leaked.

When projects are concerned, the type of project may be a factor as well. One factor is the project schedule status. Other factors causing delays with a project include funding, personnel, supplies, and dependencies. Placing safeguards to prevent data loss or minimize the amount of lost data due to power surges, outages, or other causes shows planning.

Assessing the impact of the risk associated with a project not on schedule may be positive or negative. A positive impact is when the project is running ahead of schedule which may lead to production or monetary gains sooner than expected. Whereas a negative impact will cost money depending on how far behind schedule the project is and what will be needed to get back on schedule if possible. Once the cause or the reason for the project being negatively affected

has been determined, then a value can be associated with what it will take to fix or mitigate the threat. Here, if a lapse in any of the security layers was discovered to have been overlooked, the lapse can be taken into consideration in the future and corrected.

Money is always a factor to consider. The situation may require waiting until enough is saved up to afford the next upgrade, release, or acquiring a new installment of hardware and software. An issue may arise shifting where and how much money is being put towards a previously developed priority list due to unforeseen events causing the order of the itemized list to alter. Another factor to consider is how the money is being managed and if there are any reasons to worry about where it is being invested.

A financial assessment needs to take into account the budgetary constraints of the user or company. Whether an individual user or a company, does the initial assessment realize a constant funding source? The financial assessment will consider the life cycle costs associated with the current infrastructure, replacement costs, and software upgrades and patches. The value can be figured out in advance once known what needs to be done and when. The cost will be considerably greater in looking at a network overhaul or replacement versus only having to do maintenance upgrades over a few years. The availability of money may be a reason, users or companies place a certain amount of dependency on only one layer. Shortage of funding is an understandable intentional reason for over-reliance on a particular security layer until there is more money available to beef up the other security layers.

Approximating risk associated from a technical aspect can become a harrowing proposition. The user (single system), networking administrator, Chief Information Officer (CIO), etc., need to be aware of technological advancements in the field in case they affect their network. This is going to happen and tend to happen very frequently since technological

advancements are always being made. These people should be constantly monitoring various websites, publishings, and news networks for new or ever changing bugs. In this case, technological advancement is not a matter of if, but of when. They must habitually monitor their system for unexplained glitches, degradation in resource consumption, and power failure in case the backup uninterruptable power supply needs to kick on giving the user or network administrator personnel enough time to safely shut the system down without losing any data at all. Imagine having a great layered security solution in place and the administrator is concerned with a new threat that has surfaced. The administrator knows their security solution is the latest, so they only concentrate on what they need to do to keep this new threat from affecting their system. A different threat may sneak in because the administrator is concentrating on this new threat.

A technical assessment involves knowing what will be required to keep the system current. Depending on the technology available, whether it is commercial, non-commercial, or developmental, will play a factor in assessing the technical impact of a system. Obviously if the technology is commercially available, then the value will be lower overall because it is generally sold to the public. With non-commercial technical products and services, they may be more expensive due to what the product is, what it does, and who the customers are. Until a developmental technical product is prototyped, tested, proven effective for the purpose it was designed, and a customer base determined, then a value will be unknown. Also, the value associated with having a contingency plan in place for technical assessments needs to be considered.

With natural threats, the amount of risk perceived depends on the geographical location. Any natural risks considered and their estimation of occurring, depend on the type of natural

threat, the frequency with which they happen, and to some extent the magnitude of the damage that can be caused. Should the threat deal with flooding for example, one immediate solution would be to place all the hardware up off the floor (possibly even several floors up) to prevent water damage. If the threat is more destructive in nature (i.e. tornados, earthquakes, or hurricanes), then a couple of solutions may involve hardened basements a few floors down or remote backup systems at other locations without these same threats.

Impacts caused by natural threats are fairly easy to assess depending on the threat. Users and companies do what they can upfront to mitigate any damage from a natural threat depending on their location. The value of the solution may be as little as buying surge protectors, keeping items off the ground, acquiring and strategically placing lightning rods, or placing the equipment in a stable and hardened area. However, should worst case scenarios unfold and lightning or electrical surges have direct hits, flooding occurs, earthquakes shake everything up, etc, then the value assessed for the impacts of these threats is full replacement value.

Determining the effects of political threats is hit or miss. If the threat is taxing in nature, it is a risk bound to happen; but to what extent and if a loophole exists in the system allowing some relief is unknown. When public opinion is involved, people need to seriously consider what type of business they are in, where they want to have their business, and think about the ramifications involved should they place their business in an atmosphere not necessarily conducive to their views. The CIO and other IT professionals need to take into account any federally regulated policies and perhaps globally mandated policies to determine any risks associated with running their business or what effects they will have on their network system. The Institute of Electrical and Electronic Engineers (IEEE) has taken on the role of leading industrial standards for information technology (among many others). In this arena, the CIO

needs to be aware of what standards and other federally and internationally regulated policies exist that they need to adhere to.

Political impact assessments are known to change frequently based on political parties and economic factors. As tax structures are known throughout, values associated with taxes can be determined. When changes occur due to political influence, then the value is unknown. Public opinion can affect tax and economic value by impacting where a company is located and how successful it becomes. Regulation and policy assessment risks will affect the value by setting guidelines and rules users and companies must follow. The risk assessment value for the impacts caused by these kinds of threats will be based on what users and companies must follow when establishing their network. When new taxation rules take effect, many users and companies begin concentrating on how it will affect them (for a little while) and depend even more on what they currently have in place.

Managing Risk

The next step in the risk analysis process is to decide which option provides the best risk management strategy for the user, administrator, or CIO. Based on the risk, the chances of the risk coming to fruition, and the assessment of the risk's impact and value associated with each one, a decision must be reached as to whether the best alternative is mitigation, countering, accepting the risks, elimination, or a combination of all four. Mitigating a risk implies certain steps are being taken to reduce the impact of a threat. In countering a risk, existing resources are or can be used either by improving existing methods and systems, changing responsibilities, or making improvements to accountability and internal controls to name a few. When the decision is made to accept a certain amount of risk, this is usually done by creating a plan to minimize the effects if and when the risk occurs. This can be done by developing a sound contingency plan

capable of being implemented right away with minimal project control should the need arise. Contingency plans are key parts of the Business Continuity Plan or Business Continuity Management. Elimination is another strategy that can be considered, but is usually cast aside because the cost associated with eliminating the risk would be higher than just letting the event occur.

When choosing a layered security approach, the initial thought process is to mitigate these risks since the chances of them occurring to some degree or another is very good. According to Ogren (February 2004), on average 25 percent of a company's IT budget goes to staffing costs because many security models are very labor intensive and that the emphasis should be placed on overall network integrity by implementing perimeter defenses, a network integrity systems layer, an application gateway layer, and a host integrity layer. From this and from any individual having experienced working on a computer system, and then gotten frustrated because they spend a lot of time working a network problem, discerning why users and companies want to find and implement solutions that will not be quite as heavily labor intensive is easy. Layered security approaches require quite a bit of work to be done up front in terms of thought, planning, and implementation to hopefully ensure all the threats, risks, and layers involved are analyzed. Then, the best security solution can be developed (or acquired), installed, configured, and implemented. Taking into account that the right layered security solution has been implemented well, the amount of labor involved maintaining the network integrity will be kept minimal.

Even though implementing a layered security approach may be labor intensive up front and require thorough and extensive planning, this security solution risk management method will provide maximum protection, reliability, and performance. An administrator does not want to be

in a reactive mode all the time. If they do get caught up in a reactive role, then they will always be getting attacked from some threat because they are concentrating too much in one area and over-relying on at least one security layer for the majority of the other threats. In virtually all aspects of the IT arena, the sophistication, frequency, and complexity of security threats have increased. Due to this, there are several vendors currently offering what is commonly referred to as Unified Threat Management (UTM) appliances. These appliances incorporate many security functions including firewalls, VPN, antivirus, intrusion prevention, and spam filtering. Users need to take into account, these functions normally do not work together nor do they integrate in a way to allow the user to leverage information regarding one layer effectively to another layer. Configuration of a conventional UTM is complex and transcribing information from one layer to another can be inconsistent. In a conventional UTM process, the core network is protected with security layers starting with the gateway antivirus, followed by spyware protection, spam blocking, uniform resource locator (URL) filtering, then an intrusion detection/prevention functionality accompanied by a VPN, and finally the firewall. With these issues, misconfiguration is more likely to occur, leading to higher chances of poor security protection.

In recent years, newer layered security philosophies have been developed minimizing configuration problems that could lead to security degradation. One such solution is the Intelligent Layered Security (ILS) architecture developed by WatchGuard. With this more recent layered security implementation, better protection is delivered. According to WatchGuard (November 2005), the ILS architecture implements six security layers (listed in Chapter Two) intelligently working together in order to dynamically detect, block, and report malicious traffic, while letting harmless or wanted data to pass through efficiently resulting in a more superior system that is able to defend against known and unknown attacks minus performance

degradation. For this system, the security layer is a sound idea defining conceptual boundaries between components of the system's security infrastructure with each security layer encompassing a different security technology. With this type of layered security solution, a user's reliance on any given layer may be mitigated because these layers actually work together in detecting, blocking, and reporting malicious traffic.

The UTM is improved upon with the ILS architecture by its engine running through the security layers like a central nervous system allowing it to take advantage of and reinforce the capabilities of the other layers. When transferring the information of all traffic processed from layer to layer, additional protection, reliability, and performance is guaranteed. The type of protection provided by the ILS architecture is briefly stated. Beginning with the External Security Services layer, additional technologies exist with the ability to extend protection past the firewall plus having information that enables the user or administrator to be more efficient with their time management. In the second layer, data integrity is managed through the validation of data packet integrity and conformance. Within the third layer VPN functionality, safeguards secure and private external communications. The use of stateful firewalls in the fourth layer restricts traffic only to the sources, destinations, and ports provided for in the security policy. The fifth security layer, otherwise known as the Deep Application layer, guarantees application layer protocol standards conformance, blocks harmful files via pattern or type, and stops dangerous commands and the modifying of data that would normally allow for the seeping of vital network data. The internal sixth layer at the core of the system; content security, encompasses the gateway firewall, intrusion prevention, antispyware, spam protection, and URL filtering. Here, all traffic is regulated and analyzed checking for appropriate content.

Further analysis of the six layers reveals a little more detail on how they work. For the External Security Services layer to be as effective as it is vulnerability assessments and desktop antivirus are included providing assistance to the administrator or user in making smart choices in the most optimum way to configure the firewall and any other associated systems. The Data Integrity layer acts as the first line of defense by validating incoming data and assuring it complies with data packet protocol guidelines. This line of defense is also the cheapest and best area for stopping attacks and at the same time allows for quicker traffic filtering. In the VPN layer, a determination is made as to whether or not the traffic is encrypted from a known partner, customer, remote personnel, or branch office. If a determination is made, decryption processes take place and if not, then the packet is dropped. Unencrypted traffic is left to the next layer for policy decision making.

Within the stateful firewall layer, the administrator has configured the stateful firewall to deal with allowing or not allowing traffic to pass based on the source or destination IP and the port. ILS actually implements another step by tracking the port and protocol information on all the connections and their state in order to activate shunning traffic if an attack is detected. If traffic proceeds to the Deep Application Inspection layer, then a decision is made determining if the traffic is appropriate. Should the traffic be okay, it is allowed through for optimal performance with new transmission control protocol (TCP) connections built on both sides of the firewall. In this layer protocol anomalies, buffer overflows, unauthorized connections, TCP hijacking, network data leakage, usage of potentially harmful commands, and dangerous attachments are either detected, managed, prevented, or denied.

Within the Content Security layer, the actual data is looked at. A gateway antivirus service exists, along with an intrusion prevention service. This service contains anti-spyware,

enhanced performance which is assisted by more efficient processing based on the protocol being used, and an extremely effective spam protection service removing 97 percent of spam mail. Also included is a URL filtering service enabling who does and does not get access and the type of access.

The various layers of this architecture are created to cooperate with and pass along information to other capabilities within the same layer or in other layers due to the many capabilities and functions existing within this design. Also, these layers are designed specifically with the intention of being able to work together to produce multiple benefits to the user. One benefit is enabling superior security by blocking several inherent threats without any window of opportunity for them to exist, proactively seeking various attacks and their behaviors and dropping them from the site, and minimizing false positives. A second benefit is considerable ease of usability with the deep application inspection functionalities always on, well-designed defaults blocking the majority of attacks without the added necessity of complex configurations, and proactive prevention. Finally, the third benefit is better performance as the layered architecture allows for the detection and stopping of attacks with significantly less processing.

Additionally, layered security having been improved upon over the last several years (from UTM to ILS), many companies that were unable to effectively deploy this type of security can now do so with the resources at their disposal. UTM solutions provide layered security but without the appropriate level, ease of use, or performance many customers want. Administrators have a bigger role in integrating a UTM solution which may leave them open in some areas if they feel they have properly implemented certain security layers and then they do not keep an eye on it. Newer solutions, ILS in this example, are able to provide an intelligent, multi-layered defense where all the layers cooperate with each other multiplying the level of security provided.

Another important aspect is with technology and the security environment continuously changing, flexibility, scalability, and extensibility are necessary characteristics of any network security solution.

Initially, the firewall is a security aspect for any system that should be considered in any risk management analysis. Software firewalls tend to have the distinction of monitoring inbound and outbound network traffic and being able to identify suspicious activity. According to Rebbapragada (May 2006), software firewalls allow to some degree the setting of the security level, white-listing and black-listing certain applications, and enabling specific ports and network protocols. There are some very good firewalls with the ability to distinguish between good and bad network traffic, give the user some notice and information regarding suspicious traffic so they can make a more informed decision on whether to allow it or not, and warn the user when suspicious or malicious traffic has been spotted. In trying to mitigate risk, one thing users or administrators do not want is a less effective firewall alerting them often providing insignificant and useless data causing them to deny wanted traffic or turn it off altogether. Based on the range of security settings available when configuring a firewall, users or administrators may want more flexibility in the settings based on other security features they have.

Other security tools users and administrators need to consider in managing risk includes anti-spam protection, backup software, disk tune-up tools, and parental controls in order to block undesirable sites. Users may want URL filtering capabilities or a more specific ability known as Smart Filtering Dynamic Real-Time Rating in order to categorize Web sites not currently stated on any user- or software-defined white-list or black-list. Plus, users may require privacy controls to protect against sensitive information leaving the computer or system and/or offer a feature scanning instant-messaging clients for infected attachments.

Another good feature to have is the capability to be warned of interlopers riding on a Wi-Fi connection. Relying on these other security aspects is important, but if a user accesses the Internet quite a bit through Wi-Fi and does not implement some sort of encryption or security mechanism, the other security layers in place may not protect against threats getting through via the Wi-Fi connection. Even though many great features are desired, users need to be careful of having too much of a good thing because then they may think all the security layers are in place causing them to become complacent.

There are many helpful things to know when trying to mitigate multiple risk factors. Ensure only one antivirus tool is being run on the system. Prior to installing any security software, check the hard drives health and run Windows Update to ensure the system is up-to-date. Should a user or administrator choose to have a secondary antispyware application, make sure it is not scheduled to run while the other application is running. Document or take a snapshot of any problems or errors and send those in to the technical support or help desk. Do the same with any suspicious emails or files. Also, optimum security success depends on all security products being kept up-to-date or renewed frequently.

Many other aspects of managing various risks (operational, reputational, procedural, natural, etc), whether accepting, mitigating, or countering, will most likely be accomplished the same way regardless of the security solution chosen by the user, administrator, or CIO. Ensure sufficient security policies and processes are in place and that they are enforced. Any tangible risks (procedural, project, financial, and technical) should be monitored and watched closely in minimizing any negative impacts and determining new courses of action should potential setbacks be seen coming in the future. Users and companies also need to take the necessary precautions when managing natural risks. Finally, for political risks, employing the right person

can go a long way to watching out for various pitfalls and keeping the companies best interests in sight.

Reviews

The success of any security solution includes reviewing it periodically. These periodic reviews should occur frequently and consistently (every two months, quarterly, or semi-annually) depending on how well things are progressing with the network and what the environment is producing. Having a formal process and team in place will dictate a higher level of review. For example, an outcome of the risk analysis may be to systematically perform formal reviews of the entire process, test systems regularly, or even test any contingency plans currently existing to determine how well they work. Not every risk will apply to a user or company. The reviews will help determine if the risks are changing for the better or worse, all but eliminated, or if new ones are emerging. Also from these reviews, the layered security strategy can be determined if the risk management is appropriately using the resources at its disposal, developing or creating new resources, determining the cost effectiveness of the security solution being employed, and if there has been over-reliance on any single layer within the security solution.

After implementing a layered security solution, the reviews performed should provide useful information to the user or company as to whether or not they are working as intended. In regards to the layered security solution, the reviews should show improved protection against multiple threats, reduction of spam mail, increased resource management and cost effectiveness, reduced processing time, overall improved performance, smaller percentage of false positives, better and more accurate intelligence with network traffic, and greater ease of use. The results of the reviews performed will tell the user or the CIO if the desired outcomes have been achieved

using a layered security solution and if perhaps there was any over-reliance with a given layer. If the answer is yes, the risk analysis will also tell the user or administrator where the dependency was spotted and why the dependency developed. From this, the problem can be resolved and prevented in the future.

Chapter 4 – Risk Analysis Results

After performing a risk analysis with layered security and over-reliance in any security layer, the results for why there could be a dependency on a given layer is annotated. Regardless, the numerous threats identified (human, operational, reputational, procedural, project, financial, technical, natural, and political) must be considered. Even if the likelihood of the threat happening was determined to be fairly small, a value needed to be assigned to the impact of the threat and where that could lead when concentrating elsewhere. During the risk management phase, mitigation was the prominent way to manage risks while accepting some forms were going to happen. Frequent reviews revealed the superior effectiveness and performance of the layered security approach even if relying too much on any given security layer within ILS because they worked intelligently together. With a UTM solution, the possibility of over-reliance with a security layer could result in increased attacks.

All of the threats identified were considered, but reputational, natural, and political are threats that must be dealt with when they occur. The human threat can be mitigated greatly, but is still a possibility when over-relying on the perimeter defenses. Two different layered security approaches (UTM and ILS) were discussed covering implementing firewalls, VPN, intrusion prevention and detection services, URL filtering, spam blocking, spyware protection, and gateway antivirus. However, with the second layered security approach (ILS) included, the capability to intelligently communicate traffic between the different layers reducing the amount of work required from one layer to the next and decreasing the possibility of threats due to depending on any given security layer. These security features included improved technologies extending protection beyond the firewall and empowering the user or administrator to be more efficient, conformance of protocol standards, blocking harmful file types and commands, and

permitting greater flexibility, scalability, and growth. In keeping solutions as simple as possible, the complexity is diminished allowing for reduced operational, procedural, project, and technical threats. The financial threat has to do more with managing current and new resources, maximizing their potential, planning smartly, and implementing the solution well. Over-reliance on a security layer may still be an issue to some degree, but in performing a risk analysis the dependencies will be found and then they can be corrected.

Chapter 5 – Conclusions

The emphasis of this research was to demonstrate there could be over dependencies in using a layered security approach implemented on a network. Using interpretivism, various threats were considered initially starting with multiple internal and external threats. Every threat could impact whether or not there could be over-reliance with any given security layer. To some extent, every user or administrator performs a risk analysis. However, a thorough risk analysis should always be done that includes identifying threats, estimating the risks associated with those threats, managing the risks, and then constantly performing reviews to ensure decisions made previously were the best choices or determine if changes need to be made. In performing a risk analysis, any over dependency with a particular security layer should surface. The added benefit of the risk analysis will also tell why there was an over-reliance and then a solution can be derived and implemented.

After researching various layered security solutions and discussing the UTM and ILS approaches, a user or administrator becoming over-reliant on any layer is understandable with these solutions. Even though knowing not everything can be guarded against 100 percent, the layered security approach provides the best threat protection due to each layer placing another level of security a threat must bypass if successful to that point. Plus, the ILS offers intelligent traffic management along its central nervous system providing even greater system security and with this approach there is greater flexibility, scalability, and increased performance. Conducting and maintaining thorough risk analysis assessments is the best way to keep from becoming over dependent on any single layer of a layered security approach. The protection of IT computer systems from various threats by using a layered security approach is still the most optimal method of protection available today.

References

Adams, E. (N.D.). Over-Reliance on network defenses: Don't forget the software. *Security Innovation.* Retrieved July 23, 2010, from http://www.securityinnovation.com/pdf/dont-forget-software.pdf

Bouchard, M. & Mangum, F. (N.D.). Multi-Layer security platforms: The New definition for best of breed. *Fortinet.* Retrieved May 8, 2010, from http://www.fortinet.com/doc/whitepaper/MultiLayerSecurityPlatforms.pdf

Campbell, S. (January 2006). How to think about security failures: Understanding complexity and feedback in security models highlights the need for better failure modes in solutions. *Communications of the ACM, Viewpoint, 49(1),* 37 – 39. Doi: 10.1145/1107458.1107482

Introducing the watchguard intelligent layered security architecture: Better security for the growing business. (November 2005). *WatchGuard Technologies, Inc.* Retrieved May 11, 2010, from http://www.infosec.co.uk/ExhibitorLibrary/71/wg_ils_wp.pdf

IObit Security 360. (September 2007). *IObit.Com*. Retrieved October 6, 2009, from http://www.iobit.com/security360.html

Ogren, E. (February 12, 2004). Using a layered security approach to achieve network integrity. *Computerworld*. Retrieved May 10, 2010, from http://www.computerworld.com/s/article/89861/Using_a_layered_security_approach_to_achieve_network_integrity

Oppliger, R. (May 1997). Internet security: Firewalls and beyond. *Communications of the ACM, 40(5),* 92 – 102. doi: 10.1145/253769.253802

Perone, J. (December 31, 2009). Expect new, evolving computer viruses in 2010. *New Jersey Business News.* Retrieved May 27, 2010, from http://www.nj.com/business/index.ssf/2009/12/expect_new_evolving_computer_v.html

Perrin, C. (December 18, 2008). Understanding layered security and defense in depth. *TechRepublic.* Retrieved April 23, 2010, from http://blogs.techrepublic.com.com/security/?p=703

Rebbapragada, N. (May 25, 2006). All-in-one security. *PCWorld*. Retrieved May 19, 2010, from http://www.pcworld.com/printable/article/id,125817/printable.html

Why additional software is needed to protect your computer from online threats. (N. D.). *TopTenReviews*. Retrieved October 7, 2009, from http://internet-security-suite-review.toptenreviews.com/why-additional-software-is-needed-to-protect-your-computer-from-online-threats.html

Annotated Bibliography

Adams, E. (N.D.). Over-Reliance on network defenses: Don't forget the software. *Security Innovation.* Retrieved July 23, 2010, from http://www.securityinnovation.com/pdf/dont-forget-software.pdf

The majority of the funding spent on protecting a system tends to go to the firewall and intrusion detection areas to harden the perimeter. Unfortunately, the perimeter is still fairly permeable allowing for a high percentage of breaches at the application layer. Once inside the perimeter, anyone is free to go wherever they desire inside the network. This is because there is not the same strict guidance to developing software leading to vulnerabilities within the application layer.

What is gained here for the reader is the idea that users need to be made aware the software they use is not beholden to a particular set of rules or guidelines when it comes to what needs to be considered in terms of security purposes. Simply put, thinking too much on strengthening the perimeter may lead users to overlook many security vulnerabilities, feel overly safe in what they have in place, and give greater opportunities for business logic attacks.

Blackwell, C. (2008). A multi-layered security architecture for modeling complex systems. *ACM,CSIIRW, 288(35)*. doi: 10.1145/1413140.1413180

In order to assist with developing a more complete security model, the semantic, logical and physical layers are discussed. System goals at the semantic (top) level and their dependencies on system components and external entities at lower levels are demonstrated. The logical or intermediate layer has to do with public keys, accounts or processes acting on the behalf of the user but without their ability to control directly. The physical or bottom layer represents the tangible objects or anything with electromagnetic radiation.

A simplistic breakdown of looking at the minimum layers for securing a system and what they entail is covered. Plus, the things that should be considered within each layer are explained and how they interact with the other layers to help users in seeing what they need to consider and how they can go about providing protection.

Bouchard, M. & Mangum, F. (N.D.). Multi-Layer security platforms: The New definition for best of breed. *Fortinet.* Retrieved May 8, 2010, from http://www.fortinet.com/doc/whitepaper/MultiLayerSecurityPlatforms.pdf

Up until recently, it was standard for companies to acquire best of breed point products to meet their security requirements. Many things in recent years have happened to change the way people thing in terms of meeting their security requirements, such as the growth of communications services, the expansion of information technology and applications, the birth of regulatory compliance, and the exponential growth of hackers. Best of breed now refers to which multi-layered approach works best for a given set of circumstances. The evaluation criteria to be looked at are multi-layer security, performance, cost effectiveness, and flexibility.

In this white paper, some historical background is provided to assist in explaining why previous thought patterns for securing a system had to evolve. Out of this necessity for change, new methods of thinking of system security emerged to assist users in thinking about the various aspects of their system and what methods exist to protect their system for them to consider.

Campbell, S. (January 2006). How to think about security failures: Understanding complexity and feedback in security models highlights the need for better failure modes in solutions. *Communications of the ACM, Viewpoint, 49(1),* 37 – 39. Doi: 10.1145/1107458.1107482

Considering how long technology has been around, and how long there has been known threats, there is still consternation when it comes to protecting a system. Even though the problem is not new and finding solutions is a high priority, it is not simple. One thought is to look at human intuition and how it can affect how complex system security is created. The emphasis is placed on looking at why the solutions fail.

In this viewpoint, it is suggested to look at the underlying assumptions made and how they may be inaccurate. Just because an internal application is considered safe from external threats, does not necessarily mean it is completely safe (i.e. there could be client-side attacks).

Choi, H., Song, H., Cao, G., & La Porta, T. F. (March 8, 2007). Mobile multi-layered IPsec. *ACM Digital Library, Wireless Networks, 14(6),* 895 – 913. doi: 10.1007/s11276-007-0031-z

Wireless networks, including mobile, have a couple of vital issues always being looked at: data confidentiality and integrity. IPsec is the most common method used today in transferring data end-to-end in order to ensure data confidentiality and integrity. One way of transferring encrypted data and still allowing certain portions of the user information to be accessible to specific intermediate network elements going one direction is multi-layered IPsec. There is also mobile multi-layered IPsec which includes dealing in a mobile environment.

It was interesting to read about encrypted data being allowed to show some piece of the user's information via multi-layered IPsec without slowing down the actual transfer of data. One key note is only the ability to effectively authenticate and distribute the key between the home, outside network, and mobile host was discussed.

Control systems cyber security: Defense in depth strategies. (May 2006). *Idaho National Library*. External report #INL/EXT-06-11478. Retrieved April 26, 2010, from http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

Especially within the control system domain, many information infrastructures share similar attributes when it comes to IT deployments and data communications. The protocols and communications standards used in the control system domain are the same ones that are being compromised. This brings about many security challenges that are faced: hostile mobile code, escalations of privileges through code manipulation, network reconnaissance and data gathering, covert traffic analysis, and unauthorized intrusions. Defense in depth strategies look at securing each of the core zones while offering administrators more opportunities for information and resources control and at the same time featuring cascading countermeasures without impeding business functionality.

Various strategies include the use of firewalls (packet filter, proxy gateway, and stateful inspection) to provide levels of defense supporting traditional routers and providing greater control, creating demilitarized zones, using intrusion detection systems to monitor the network, and of course having an effective security policy. Five key security countermeasures for control systems that can be used effectively are security policies, blocking access to resources and services, detecting malicious activity, mitigating possible attacks, and fixing core problems.

Crameri, O., Knezevic, N., Kostic, D., Bianchini, R., & Zwaenepoel, W. (2007). Staged deployment in mirage, an integrated software upgrade testing and distribution system. *ACM*

Symposium on Operating Systems Principles: Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles (pp. 221 – 236). Retrieved October 15, 2009, from http://delivery.acm.org.dml.regis.edu/10.1145/1300000/1294283/p221-crameri.pdf?key1=1294283&key2=2079365521&coll=ACM&dl=ACM&CFID=56661474&CFTOKEN=29535875

Users need to be concerned with software upgrades affecting other applications running on the PC. Vendors can only try to anticipate what applications may be affected by a software upgrade. Various categories of upgrade problems exist (i.e., broken dependency, testing strategies, buggy upgrades, incompatibility with legacy configurations, etc). Vendors (companies) employ a three-phased approach to dealing with upgrades: upgrade deployment, user-machine testing, and reporting.

This provides insight into some of the issues surrounding software releases to the public because it brings into focus the fact that there isn't only one or a few applications in the market software companies need to be aware of when upgrading their software. So users may add or upgrade their security software thinking all is okay and find out the hard way that it has caused a problem with another application.

Defense in depth. (N.D.). *IWS – The Information Warfare Site*. Retrieved May 5, 2010, from http://www.iwar.org.uk/iwar/resources/belvoir-iw-course/dis.htm

For those unfamiliar with the term Defense in Depth Strategy (DIDS), it means "the practice of layering defenses to provide added protection. It raises the cost of the attack by placing multiple barriers between an attacker and the business-critical information resources." DIDS contains people, technology, and operations as its key three elements.

A definition of DIDS is provided coming from a Network Computing resource. Other sites of interest are given along with their area of influence or expertise for interested parties to go to and look at.

Defense in depth: A Practical strategy for achieving Information Assurance in today's highly networked environments. (N.D.). *NSA*. Retrieved April 26, 2010, from http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Basically, the defense in depth strategy is in existence to achieve Information Assurance (IA) for highly networked and technological systems. It is founded in the ability for users to intelligently integrate and configure today's technologies and techniques. To be successful at this, organizations need to know who their adversaries are, what the motivating factors are, and what attacks will be used. Three elements to look at are people, technology, and operations.

In this overview, it brings to the forefront the main elements organizations need to always consider when attempting to develop and implement an effective security strategy. With people, the consideration lies with hiring, policies and procedures, training, systems security administration, physical and personnel security, and facilities countermeasures. Technology entails the IA architecture and criteria, the procurement and evaluation of researched products, and systems risk assessment. The security policy and management, certification and accreditation, key management, readiness assessments, and recovery and reconstitution fall under the Operations umbrella.

DeWitt, A. J. & Kuljis, J. (2006). Aligning usability and security: A Usability study of Polaris. *SOUPS; 149*, 1 – 7. doi: 10.1145/1143120.1143122

For a long time there existed the belief that security and usability did not go together. A study was done on Polaris, an alpha release using the Principle of Least Authority to keep viruses from editing files, in regards to its usability and security. Once installed, it did not require updates but did require initial configuration and for users to make decisions as to how to open files safely. Even though the software was designed to be transparent, it was not and users were found to be willing to compromise their security in favor of speed and ease of task completions.

Overall, the study showed that where security decisions could be made by the system they should be so users would be less tempted to compromise their system and that ease of use needed to be made as transparent as possible.

Hazlewood, V. (2006). Defense-in-depth: An Information assurance strategy for the enterprise. *San Diego Supercomputer Center: Security Technologies*. Retrieved April 26, 2010, from http://www.sdsc.edu/~victor/DefenseInDepthWhitePaper.pdf

Information assurance is more than computer systems security because it includes all methods, techniques, tools, people, and processes required to protect the information. Threats have been on the rise at an exponential rate and in the 2005 CSI/FBI Computer Crime and Security Survey 71% of the respondents reported having had a security incident. There is no single silver bullet to use in protecting against threats. A comprehensive Defense-In-Depth strategy including people, the host, applications, and network infrastructure components is vital for mitigating threats.

Considering the CERT Coordination Center will not keep track of the massive outbreak of threats and computer security incidents; this is a very strong indicator of how troubling the situation is and how compelling it is for every person and business to take their network system security measures very seriously. The Defense-In-Depth strategy is a very good model for people to use in order to consider what is involved in each of the components to ensure maximization of the system's security.

Introducing the watchguard intelligent layered security architecture: Better security for the growing business. (November 2005). *WatchGuard Technologies, Inc.* Retrieved May 11, 2010, from http://www.infosec.co.uk/ExhibitorLibrary/71/wg_ils_wp.pdf

Intelligent layered security (ILS) is needed to protect against today's threats especially when Unified Threat Management (UTM) appliances offering multiple security functions are very complex, can be inappropriately configured leading to poor security, and are not designed with extensibility in mind. The WatchGuard ILS has six security layers working together to dynamically detect, block, and report on malicious traffic while letting benign traffic go through. The six layers are the external security services, data integrity, virtual private networking, stateful firewall, deep application inspection, and content security. The benefits consist of better security, greater ease of use, and better performance.

With this ILS solution, various benefits are explained. This solution allows for zero day protection by blocking threats inherently (no window of vulnerability exists for these particular threats) and against attacks that are not yet known. It proactively seeks out and blocks attackers by identifying the attacks or behavior. These layers work together to reduce the amount of data scanned and the number of signatures used. The details of what each layer does are spelled out for understanding. The ILS solution was designed for small to mid-size businesses to replace the complex and insufficient UTM appliances solution.

IObit Security 360. (September 2007). *IObit.Com*. Retrieved October 6, 2009, from http://www.iobit.com/security360.html

This website offers information regarding the IObit Security 360 security software arsenal for a user's computer. It talks about what the software features for computer users in terms of security. This includes advanced malware and spyware removal utility providing detection, removal of deeply ingrained infections, and protection from spyware, adware, Trojans, keyloggers, bots, worms, and hijackers. It's also very fast and accurate.

This is a good overview of what the product provides and comparison against other malware and spyware provided to customers. However, it also ascertains that there is no solution offering a 100 percent effectiveness rate for detecting viruses and malware.

Juniper networks layered security solution: Re-establishing the trusted campus network. (September 2008). *Juniper Networks*. Retrieved May 6, 2010, from http://www.juniper.net/solutions/literature/white_papers/200055.pdf

Lately campuses across the world are facing increased demands from students, staff, administrators, faculty, and others to access their network and so must also take into consideration improved control for those requiring access and protecting against more sophisticated threats. Multiple network locations demand various security layers. The components of the Juniper Networks Layered Security Solution consist of firewalls, intrusion prevention, virtual private networks, antivirus, web filtering, and anti-spam. As with all security solutions, there may still be other factors to consider like performance, complex applications, network integration, WAN connectivity, reliability, and management.

In this white paper, the Juniper Networks Layered Security Solution provides in-depth coverage of what protections it provides at the various layers. It helps explain how information technology personnel are able to apply the appropriate security measures at each level by stating what they are/should be protecting. It states under the various site conditions what security layers to consider. With this information, a network environment can be developed that can truly be trusted without sacrificing performance, flexibility, reliability, and/or management control.

Mannan, M. & Van Oorschot, P. C. (July 2008). Security and usability: The Gap in real-world online banking. *ACM: NSPW '07: Proceedings of the 2007 Workshop on New Security Paradigms.* Retrieved October 15, 2009, from http://portal.acm.org.dml.regis.edu/results.cfm?coll=ACM&dl=ACM&CFID=56661474&CFTOKEN=29535875

Nowadays, banks encourage customers to accomplish most (if not all) of their banking online. Unfortunately, banks are not immune to their system being exploited by attackers. Customers are asked to install a firewall, anti-virus, and anti-spyware programs on their own to ensure the security of their information.

This article enforces the idea onto users that they must do everything they can to protect their system (and also access to other systems) from threats taking into account firewalls, anti-virus and anti-spyware programs, operating system and security software updates, authentication, and maintenance.

Neill, J. (July 5, 2006). Analysis of professional literature class 6: Qualitative research I. *Wilderdom.* Retrieved August 15, 2010, from http://wilderdom.com/OEcourses/PROFLIT/Class6Qualitative1.htm

Various research paradigms are stated. They are positivism, interpretivisim, and critical science. Some assumptions regarding interpretivisim are made. Different ways of collecting data and a critical viewpoint is discussed.

Interesting to learn several people consider interpretivisim to be too subjective which can lead this methodology to be dismissed.

Ogren, E. (February 12, 2004). Using a layered security approach to achieve network integrity. *Computerworld*. Retrieved May 10, 2010, from http://www.computerworld.com/s/article/89861/Using_a_layered_security_approach_to_achieve_network_integrity

Defending a network needs to be considered more than just protecting the perimeter and patching up. Unlike what many users think, patches and a reliance on signature files do not provide great protection. It is very maintenance intensive for Information Technology personnel to try to protect against signature files they are unaware of. Everyone needs to think in terms of network integrity overall to protect their network.

For many people that are not that educated in what it takes to protect a system, this article helps explain why it can be so difficult to do so. They will realize that patches do not cover the realm of possible weaknesses in their network integrity and the general areas they must consider are perimeter defenses, network integrity systems layer, application gateway layer, and host integrity layer.

Oppliger, R. (May 1997). Internet security: Firewalls and beyond. *Communications of the ACM, 40(5),* 92 – 102. doi: 10.1145/253769.253802

Here the author orients his paper around the Internet having started as a research-oriented place where users and hosts could share information freely with mutual trust. However, the Internet grew exponentially and not all users were interested in the sharing of information based on trust or with a common goal in mind. Too many people have used it unethically and to gain information unlawfully. Even though there are those that would use the Internet to attack users and systems via successful system intrusions and various exploitations, there are available mechanisms and firewall technologies to strengthen protective measures. The main purpose of a firewall is to act as a block between a secure internal network and another network presumed to be insecure. Firewalls are necessary, but will not protect against all issues associated with incoming data (i.e., malicious code hidden within a program becomes active once program executed). Firewalls are just one of many layers needed to protect a system, to include Internet and transport layer security.

It is interesting to note hosts and users must play a game of chance. Many users do not want to risk being attacked and losing data or having it stolen. At the same time, most cannot really afford to stay away from the Internet in order to accomplish business or personal matters. Even though a firewall is necessary, it will not protect against everything and needs to be supplemented with other security features.

Payne, B. D., Sailer, R., Caceres, R., Perez, R., & Lee, W. (July 2007). A layered approach to simplified access control in virtualized systems. *ACM, SIGOPS Operating Systems Review, 41(4).* doi: 10.1145/1278901.1278905

Virtualization of systems or machines can help improve system security by providing strong confinement of virtual machines. However; users do not want complete confinement

otherwise various functions would cease to perform their job. Keeping this in mind, there should be access controls in order to share resources between the virtual machines and still allow data to flow back and forth. Another factor to deal with can be the security policy(ies) in place because the more complex a security policy is, the harder it is to use the system for its intended purpose.

By using a layered approach to security policies, the access control and complexity can be managed more easily. Start by looking at them individually; i.e., hypervisor, operating system kernel, and applications. By thinking and looking at the layers versus the entire system, security policies can be created and implemented at each layer more easily and still provide efficient protection instead of thinking of the entire system and trying to create and implement a labor intensive overarching security policy. Also, each layer is protected from the higher layers, has its own security label by which the labels of the higher layers offer refined access control information from the lower layers. By considering each layer and what it supports, more work is accomplished up front in ensuring the appropriate security is implemented with the intent to minimize and mitigate any foreseeable problems down the road.

Perone, J. (December 31, 2009). Expect new, evolving computer viruses in 2010. *New Jersey Business News*. Retrieved May 27, 2010, from http://www.nj.com/business/index.ssf/2009/12/expect_new_evolving_computer_v.html

The leading and more successful anti-virus software company today is thought to be by some McAfee. A few ominous predictions for 2010 include cybercriminals targeting social networking sites and third-party applications and relying on even more technology advanced and complex botnets and Trojans to build and execute attacks.

Even with this very bad news, the crime labs and law enforcement are expected to do very well this year in fighting cybercrime. Various new and more sophisticated attacks to watch out for are social networking sites being attacked by cybercriminals, Trojans, botnets, and malware.

This article provides interesting news and forecasts regarding other ways cybercriminals plan on attacking their victims and insights into some of their new features. This begs the question how security software can or will be updated to fend off these new or more complicated attacks.

Perrin, C. (December 18, 2008). Understanding layered security and defense in depth. *TechRepublic*. Retrieved April 23, 2010, from http://blogs.techrepublic.com.com/security/?p=703

There has been misunderstanding between what layered security is and what defense in depth is. Layered security refers to security being implemented at any level of a complete information security strategy. Defense in depth has to do with more comprehensive security strategies because the premise is that there is no possible solution or strategy that can provide complete, total security against threats. They are both different concepts with multiple areas of overlap.

Here it is important to note the differences between the two philosophies. The layering of security arises from the concept that any single defense is flawed and only by being attacked will the flaws be uncovered. In defense in depth, a wider range of possibilities are considered such as physical theft with forensic usage to recover the data, incidental threats, and exotic threats (van Eck phreaking).

Perrin, C. (March 23, 2010). Simplifying systems is the best security. *TechRepublic*. Retrieved April 23, 2010, from http://blogs.techrepublic.com.com/security/?p=3337&tag=rightCol;topRated

Usually keeping things simple when all is equal is the better way to go. Once different things start being added and something simple starts to get complicated (i.e., increasing the lines of code in computer software), then it is easier for something to go wrong (i.e., a bug getting in and wreaking havoc). As features get added, there can be various effects because of the interactions of various functionalities being dependent on other functions. Keeping things simple should be one goal of the security strategy which can be accomplished by minimizing the design, modularity, and separating concerns.

This is a very true statement, about keeping things as simple as possible. Unfortunately for many businesses and enterprises today, this does not seem feasible with all the components involved in a network system.

Randall, H. (March 2005). Defense in depth: Security is like an onion… it has layers! *Transaction World*. Retrieved May 4, 2010, from http://www.transactionworld.net/*articles/2005/march/security1.asp*

Security for a system cannot be assured by installing only one particular solution, technology or operating policy. Just like there are various areas in a system to be protected, there are multiple tools at everyone's disposal to use in securing that area. By focusing on each "area", the aggregate protection is greatly enhanced. The installation of firewalls, file integrity monitoring solutions, anti-virus, and segmented architecture (keeping segments and servers grouped by function or department and separated from other functional segments or servers) are a few things to consider in protecting the information.

This provides a gentle reminder to all users that there is not just one layer they need to consider in protecting their system – there are many. Everyone will be better able to protect their system once they start thinking in this manner and apply the correct solution to a particular layer.

Snow, B. (May 2005). Four ways to improve security. *IEEE Security and Privacy* (pp. 65 – 67). Retrieved October 15, 2009, from http://search2.computer.org.dml.regis.edu/advanced/Advanced_Result.jsp

Basically, customers need to demand more from vendors when it comes to the security of their system. Customers should look at the quality control methods used by the vendors, ensure cryptographic primitives are required, see if hardware assist mechanisms are needed, and use separation mechanisms on shared resources.

For all customers looking into security measures for their PC, this provides additional areas for them to think of. It gives them more information at their disposal in considering what is necessary to accommodate their needs.

Whitson, G. (June 2003). Computer security: Theory, process and management. *Journal of Computing Sciences in Colleges, 18(6)*, 57 – 66. Retrieved October 15, 2009, from http://portal.acm.org.dml.regis.edu/citation.cfm?id=770818.770830&coll=ACM&dl=ACM&CFID=56661474&CFTOKEN=29535875

With the dawn of Web services, security problems have been a fact of life with this wished for and extremely useful technology. As discussed in this paper, computer security refers

to preventing and detecting unauthorized use of computers (including PCs). The user or security administrator needs assistance in organizing and understanding computer security material. Certain questions an administrator or user could ask are covered. Three major facets of computer security (theory, process, and management) are discussed. Also, computer security engineering should be used to address the way ahead for creating computer security systems.

This seems to provide good information to everyone (whether novice or experienced) in terms of always needing to consider the security of the PC or system and the process involved with attempting to include every aspect and the various ingredients required to secure the system or PC.

Why additional software is needed to protect your computer from online threats. (N. D.). *TopTenReviews*. Retrieved October 7, 2009, from http://internet-security-suite-review.toptenreviews.com/why-additional-software-is-needed-to-protect-your-computer-from-online-threats.html

When considering the publicity regarding PC viruses, spyware, hackers, etc, Internet users are made very aware of the risks taken when accessing the World Wide Web. Using the Windows XP operating system allows users to surf the web with confidence via the Security Center function holding all of the user's PC security information and configurations. The Security Center has a firewall, automated update feature, and virus protection which are necessary to protect against internet threats. Even though firewalls are essential, they do not stop all viruses and worms from getting to the PC. Also, the automated update feature will help protect the PC if turned on and the virus protection feature only keeps an eye out for antivirus software installed on the PC. For whole Internet security, an Internet security suite should be acquired as well.

This has very important information for new users so they realize they need additional security software in order to completely protect their system from threats.