The Concept of Layered Security

Written for KAMIND, IT, Inc.

By Ravi Das

Introduction

In the traditional model of security overall, only one layer of defense has been used. This is most commonly associated with that of legacy systems, especially that with of the Critical Infrastructure, which includes the oil and gas pipelines, water supply lines, the national power grid, nuclear facilities, agricultural and food supply chain, etc. But as the world is becoming almost fully digital and virtual, using just one layer of security is clearly not enough.

When it comes to protecting an IT and Network Infrastructure and the assets that reside within them, the call for using a Two Factor Authentication (also known as "2FA") is now being implemented. In this instance, two layers of security are used. For example, when it comes to Physical Access Entry applications, very often an employee is now issued a Smart Card which stores their credentials.

After swiping this into a reader, he or she is then allowed into the main point of entry, and in order to gain further access inside the office to other areas, they may have to enter a PIN number on a specialized console. The same holds true for Logical Access Applications.

With regards to this, an employee will often still have to enter a password to log into their workstation, and use a more specialized device, such as an RSA Fob or even a Biometric device (such as Fingerprint Recognition or Iris Recognition) in order to gain access to the shared folders on the corporate server.

But even this 2FA approach is starting to prove vulnerable. For example, not only is the Cyberattacker able to break through the first layer of defense, but there are high probabilities as well that they will be able to tear down the second wall defense as well. What is a business or a corporation to do?

The new answer comes with implementing multiple layers of security, perhaps having as many as four or five layers. This kind of approach is often referred to as a "Multimodal" approach, or "Layered Security" approach. This is the focal point of this whitepaper.

What Is Layered Security?

Layered Security can be defined specifically as follows:

"[It] refers to security systems that use multiple components to protect operations on multiple levels, or layers. This term can also be related to the term defense in depth, which is based on a slightly different idea where multiple strategies and resources are used to slow, block, delay or hinder a threat until it can be completely neutralized. Layered security may also be known as layered defense."

(SOURCE: 1).

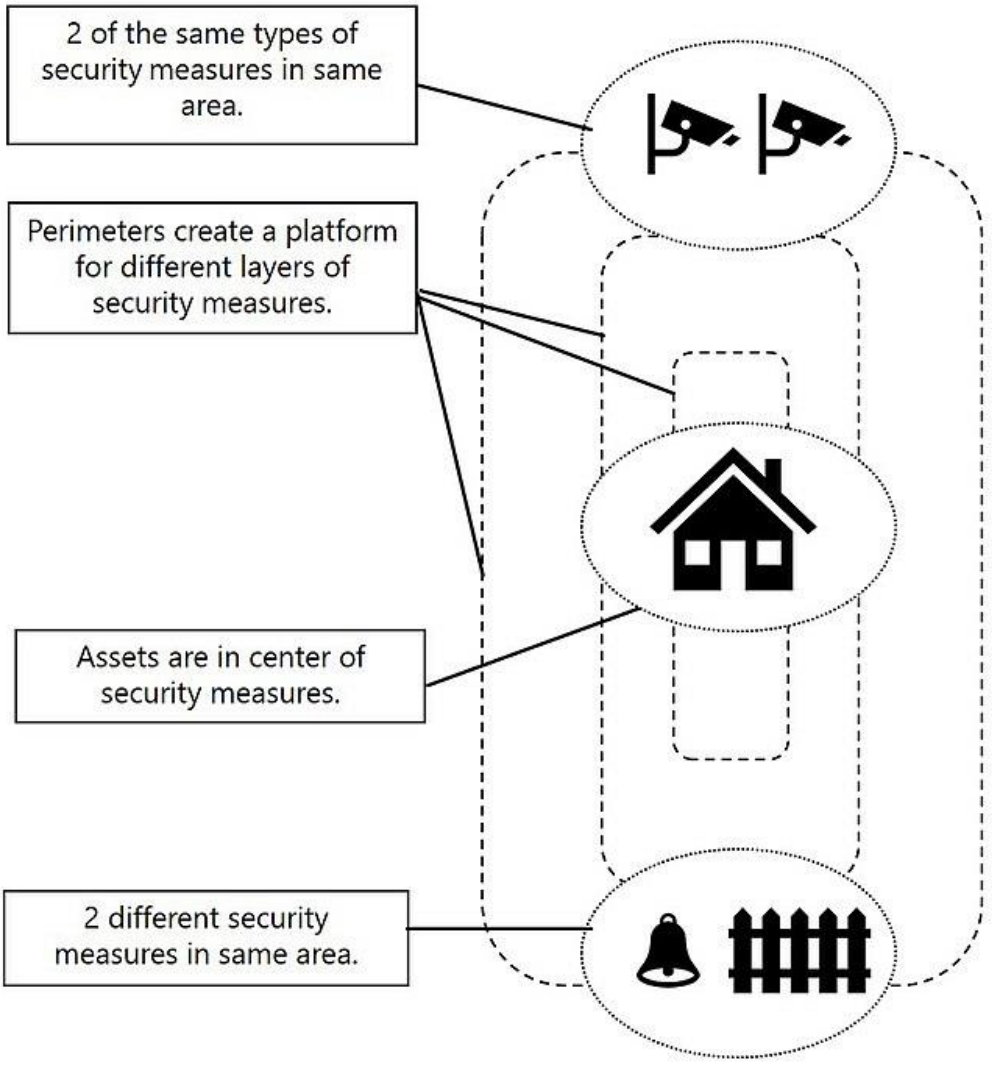
As can be discerned from the above definition, the basic premise is that deploying at least three or more layers of defense has a much higher statistical probability of thwarting off a Cyberattacker than just having one or two layers of it. In other words, the likelihood that a Cyberattacker will reach their ultimate target will diminish each and every time that they break through a line of defense. Thus, in the end, having as many layers of security as possible is the best scenario for any business or corporation when it comes to protecting their IT Assets, primarily that of the Personal Identifiable Information (PII) of their customer base.

It is important to note that the Layered Security approach can be used in both Physical Access and Logical Entry applications, but it is typically much more deployed for the latter scenario, especially when it comes to Network Security.

A Diagram of Layered Security

A simplistic view of how a Layered Security approach can be used for a Physical Access Entry application can be seen below:

LAYERED SECURITY – VISUAL EXAMPLE



"COMMUNITY SAFETY GUIDE – SECURITY PLANNING FOR EVERYONE" 2018. PG 33

PATRICK W. CONESA

Why Layered Security Is Important

As it has been alluded to earlier, deploying a Layered Security approach is very important for two reasons:

- It can protect the customer base of that organization;
- It can protect the business entity.

The details of the strategies that need to be implemented in both instances is further described:

From the Customer Standpoint

1) Protecting the confidential information:

   This includes the username and password, as well as any financial information that is transmitted from the customer to the server. In this case, the use of Secure Sockets Layer (also known as "SSL") certificates is most appropriate.

2) Detecting Fraud:

   By instating multiple layers of security, any fraudulent activity that takes place upon an unsuspecting customer can be much more easily tracked down, and very quickly. In this case, using Artificial Intelligence (AI) tools would be of great strategic advantage.

3) Message Integrity:

   Whenever a customer is signing legal documents electronically, it is up to the receiving party (which is the business entity that is selling the products and services to this customer) must ensure that the documents remain intact during network transmission. This is also known technically as "Message Integrity". In this regard, multiple layers of Encryption and Cryptography must be used, especially when it comes to safeguarding the electronic signature so that it is not easily forged.

4) Electronic Communications:

   Although the phone option for accessing customer support to an organization remains, the use of Email and chat agents is becoming much more popular for the customer. In these instances, the messages that are transmitted via both of these mediums must be protected with multiple layers of security, by using the principles of Encryption and Hashing.

From the Business, or Enterprise Standpoint

From the perspective of the business, there are two very broad types of Cyberthreats that they can be exposed to, thus making the case even stronger for using a Layered Security approach:

- Passive Attacks:

  This is when a Cyberattacker tries to tap into and covertly listen into the lines of communications between a business or a corporation, and their respective customers (as well as potential customers) and suppliers/distributors. This can be done either using a Network based or a Systems based approach. This kind of attack has been deemed to be one of the most difficult to detect.

- Active Attacks:

  This is when the Cyberattacker tries to break down the walls of defense of an organization, in order to get access to the IT Assets that reside from within the IT and Network Infrastructure.

It is important that although both threat variants are actively used, it is the latter which gets the most publicity and notoriety. Examples of this include the Marriott Hotel Group breach, the Target security breach (where millions of credit card numbers were stolen), the British Airways website hack, the Equifax security breach, etc.

The rest of this whitepaper will examine the types of controls that are needed to be implemented for a Layered Security approach for the business enterprise, and what the specific components are for a Layered Security Model. A future whitepaper will examine how this approach can be used for protecting the customer in much more depth.

What A Layered Security Approach Should Address

The Layered Security Model for a business or a corporation should contain the following types of controls:

1) Administrative Controls:

   These are the specific policies and procedures that have formulated to mitigate the risks of a Cyberattacker from penetrating any known and unknown vulnerabilities, gaps and weaknesses. These are typically that have been set forth to handle confidential and sensitive data, both business and customer wise.

2) Physical Controls:

   This involves protecting all the physical (or tangible) IT Assets of a business or a corporation, which includes the servers, workstations, and any form of wireless device that has been issued to an employee. A Layered Security approach can make use of a combination or all the following:

- Standard door and electromagnetic locks;
- Smart Cards that can be swiped into a reader;
- Biometric devices (primarily that of Fingerprint Recognition and Hand Geometry Recognition);
- CCTV Cameras;
- Trained security guards.

3) Technical Controls:

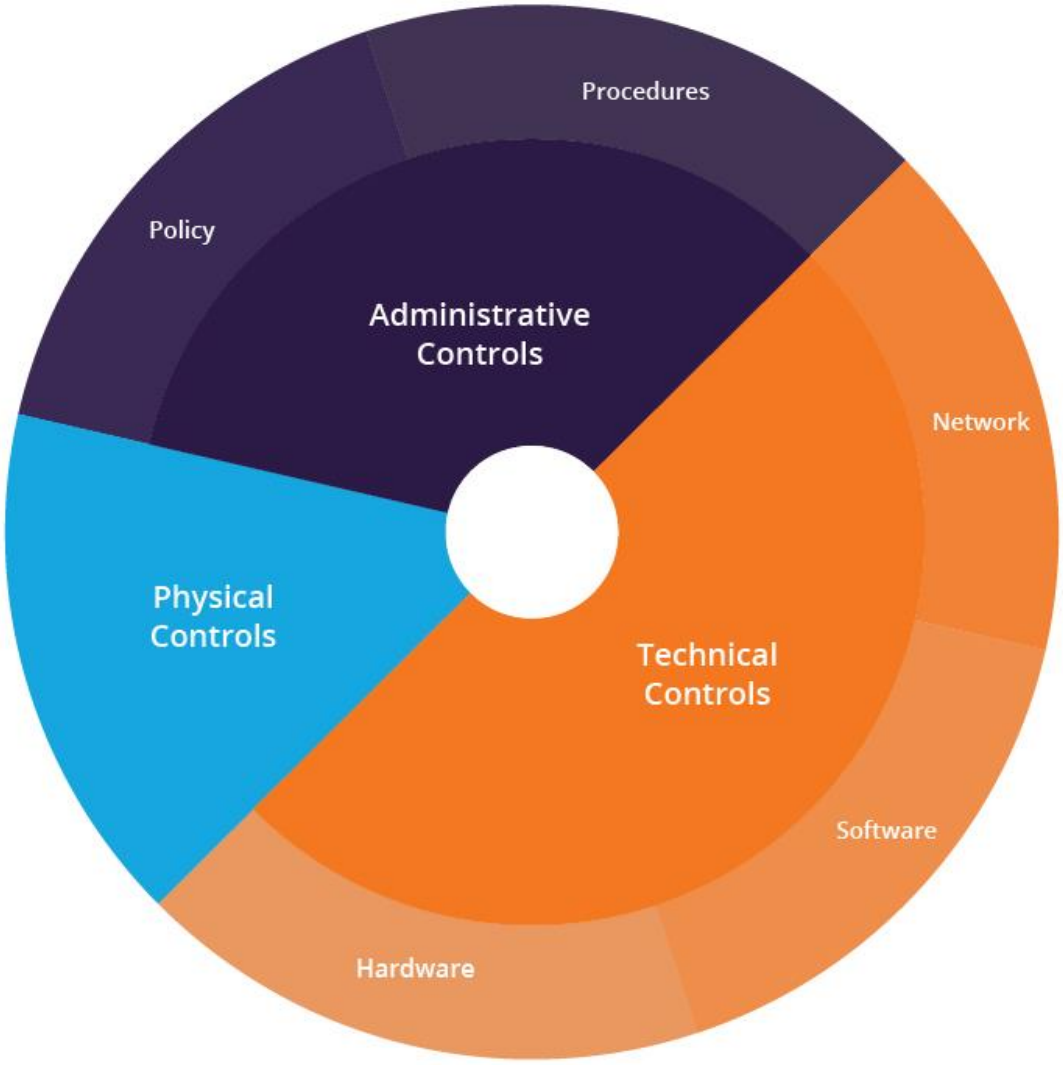
   This includes protecting all the Digital based (or intangible) based IT Assets of the organization. This can be a quite exhaustive list, but a representative of this includes the following:

   - Antivirus and Antimalware software packages;
   - Firewalls;
   - Network Intrusion Devices;
   - Routers;
   - Email Encryption;

- Password Managers;
- Single Sign On Solutions.

A Diagram Of the Controls

The above three controls are visually depicted in the diagram below:



(SOURCE: 2).

The Components Of A Layered Security Approach

When trying to craft a Layered Security Model for your organization, it is very important to first create a plan for it, test it out in a Sandbox like environment (this is where you test all of the security layers that you plan to implement in a controlled environment), and if all goes well, then deploy them into the actual production environment. In fact, the Layered Security Model that you ultimately decide upon should even be a part of your overall Security Plan. But all of this will be reviewed in greater scope in a future whitepaper as well.

The subsections below review the important components that are to be part of an overall, Layered Security Model. Broadly speaking, there are two types of them:

- Preventative Components:

  These are the kinds of tools that allow the CIO/CISO and their respective IT Security staff to mitigate as much as possible Cyberthreats before they become a reality.

- Defective Security Controls:

  These are the types of tools that also permit the CIS/CISO and their team to ***take a proactive security stance*** when it comes to combatting Cyberthreats. Being proactive in this regard means that steps are being ***taken ahead of time*** in order to thwart off any potential risks to the organization. Typically, these would be used in a Threat Hunting or Penetration Testing exercise.

Preventative Security Components

These include the following:

1) Malware/Spyware Detection:

   Typically, this mostly involves deploying the appropriate Antimalware and Antisoftware software packages on all the servers, workstations, and wireless devices. But simply doing this is not enough, a regular schedule must be implemented and strictly followed so that they are updated on a regular basis by the IT Security staff.

2) Software Upgrades:

   Apart from the above, the same IT Assets also need to have a regular schedule in which their respective software updates are also deployed on a timely schedule. In this regard, Microsoft comes out with their regular software patch schedule on the second Tuesday of every month; this is known as “Patch Tuesday”. Bulletins are normally published immediately following the release of these patches, which classify them as “Immediate”, “Medium”, or “Low”. More details about this can be seen at the following link:

   https://portal.msrc.microsoft.com/en-us/security-guidance

3) System Hardening:

   Typically, when a new security tool is first acquired, it is normally set to the thresholds that have been set by the vendor. However, keep in mind that these are just minimal, and more than

likely, will not help prevent a major Cyberattack from occurring. Instead, it is important that the IT Security team take the time to carefully ascertain what the real requirements are for their particular environment and ***set those thresholds accordingly before deploying these new tools***.

4) Network Access Control:

This involves two critical aspects:

- The deployment of the appropriate devices:

This involves the implementation of the Routers, Firewalls, and Network Intrusion devices that constitute a major part of your lines of defense. In this regard, it is very important to get away from the mindset that deploying more hardware is better. The truth of the matter is it is not***, as this only increases the attack surface for the Cyberattacker***. Rather, a risk analysis should be done first, in order to determine where they should be strategically placed. In other words, it is far better to work with a fewer number of tools versus procuring them and implementing in large numbers.

- The appropriate permissions must be established:

As is always the case, just the right amounts of rights and privileges should be established in order give your IT Security staff and other employees for them to conduct their daily tasks that are required for their positions. The mantra to be remembered here is, "No More, and No Less". However, these permissions should be monitored on a regular basis to make sure that no employee (or an unauthorized user) is gaining illegitimate access to any IT Asset.

5) The use of Encryption:

As mentioned before, any information and/or data that is being transmitted within the organization and especially externally, must be encrypted with the highest levels possible. In most circumstances, this would involve the use of 1026 Bit Encryption. If the business or corporation is large enough, then the use of a Public Key Infrastructure should be used, in which both Public and Private Keys are used for the purposes of Encryption and Decryption.

6) Security Awareness Training:

This is probably one of the most crucial components of a Layered Security Model. In this instance, employees must be trained on a regular basis (at minimum once a quarter) on how to identify Cyberthreats that are both external and internal (especially that of Insider Threats) to the organization, and how to maintain the proper levels of "Cyber Hygiene".

Detective Security Components

The components include the following:

1) The Use of Change Management:

Any sort of change or configuration that is going to be implemented in the IT Infrastructure must be ascertained before it is deployed. The primary reason for this is that any change could have a

cascading effect upon addons that have been implemented into the main system. This will only create more gaps and holes for the Cyberattacker to covertly penetrate into and cause even more damage. Thus, it is very important to make use of a good Change Management tool in order to make sure that all changes are effectively and safely managed.

2) File Integrity Monitoring:

In this scenario, all files that are sent as attachments within an Email message that are both inbound and outbound must be scanned to see if they contain any malicious links, macros, or corrupted .EXE files. Using Firewalls and Routers can be of great help here, as if anything is detected, those respective data packets will be dropped immediately, and not make its entrance into the business or corporation.

3) The Use of Log Monitoring Tools:

This is one of the best weapons that an IT Security staff can have in their arsenal. Log files contain extremely detailed information and data on all activity that transpires from within an IT and Network Infrastructure. This includes the servers, the software applications, the workstations, the wireless devices, and even the network devices. The typical events that are captured in a log file include the following:

- What happened on a system;
- Who did it;
- When it transpired;
- Where the event occurred at.

The use of Artificial Intelligence (AI) can be a great boon here, as it can analyze a log file in just a matter of seconds and alert the IT Security staff of any unusual behavior or anomalies.

4) Vulnerability Management:

Regular exercises must be conducted on a regular basis in order to unearth any system vulnerabilities or weaknesses, especially those that have gone unnoticed for long periods of time. As mentioned earlier in this whitepaper, the use of Threat Hunting and Penetration Testing tools will discover all of this, and even make recommendations as to what remediative steps need to be taken.

5) The Use of Incident Alerting Tools:

These types of devices provide to the IT Security staff alerts and warnings of any anomalous or malicious behavior that is taking place. The main disadvantage with these devices is that they can generate a lot of false positives (these are merely any alerts and warnings that are generated which have no relevance to them), and thus, it can be a huge burden as well as a very time consuming process to comb through all of them to see what threat is for real and what is not. Once again, using Artificial Intelligence (AI) can be of great help here, to filter all of this, and present those alerts and warnings that are for real, so that they can be triaged and acted upon in a quick and expedient manner.

Conclusions - The Benefits of Layered Security

Overall, this whitepaper has examined what Layered Security is, its importance, as well as its relevant controls and components. The utilization of this kind of approach is a must these days, given the dynamics of the constantly changing Cyber Threat Landscape. But apart from this, there are other benefits as well, which include the following:

- There are much higher statistical odds in ***fighting off different kinds of Cyberattacks***, such as those of Ransomware, Business Email Compromise (BEC), Trojan Horses, Worms, Viruses, Malware, Distributed Denial of Service (DDoS) attacks, etc.;
- Using multiple layers of security will make your lines of defense much more efficient and effective in capturing a potential Cyberattacker early on;
- Because any potential Cyberthreats will have a greater statistical probability of being detected early in the process, any risks or downtime that a business or corporation faces if they are indeed impacted will be greatly reduced versus than just having two layers of defense;
- Because many tiers of security are being used, the IT Security team is thus less burdened which translates not into financial savings for the organization but also increased worker productivity.

Sources

1) https://www.techopedia.com/definition/4005/layered-security
2) https://www.imperva.com/learn/application-security/defense-in-depth/
3) https://en.wikipedia.org/wiki/Layered_security
4) https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_73/rzaj4/rzaj40a0internetsecurity.htm
5) https://www.ericom.com/whatis/layered-security/
6) http://www.informationweek.com/pdf_whitepapers/approved/1320416107_Tripwire_Layered_Security_white_paper.pdf
7) https://www.gosolis.com/blog/the-benefits-of-layered-security-and-how-it-can-improve-your-business/