



I need  
complete network security  
that's affordable....  
and  
I needed it yesterday.

# Intrusion Defense: Lessons learned from medieval times. Is your Castle Protected?

**Kevin Prince  
Chief Security Officer  
Perimeter eSecurity  
May 2007**



Complete. On Demand. Affordable.

## Introduction

My 10 year old boy came home recently with a very large homework assignment due two weeks later. He had been learning about the medieval times, and had to build a castle. The castle could be made out of any material, but had to include all of the items from a long list provided by the teacher including thick walls, moat, draw bridge, guard towers, arrow loops, and murder holes just to name a few. These items had to be positioned properly in the castle and labeled in order to receive full credit.

As we built the castle, my boy was eager to describe for me why all of the different defensive elements were important. He would tell me that if the enemy could get past the moat, then the archers would shoot through arrow loops until which time the enemy passed over the draw bridge to the gate where they would dump boiling water or hot oil on the enemy as they were ramming the gate.

I often wish we could deploy murder holes on the perimeter defenses of networks to scald hackers, spammers and other malicious people as they attempted to do us harm. But unfortunately network security is more complicated, although many of the same concepts used in medieval times can certainly be applied today. In particular, the use of a layered security defense model.

## Background – Building a Good Foundation

Originally, castles were made of wood, until a clever soul realized that you could light the end of an arrow with fire, shoot the castle from afar, and burn it to the ground. This quickly led to the building of stone castles which were largely resistant to fire attacks. Much like this, attacks against largely unprotected networks in the early to mid 1990's led to the need to deploy firewalls.



These devices were so effective for the next few years, the common belief was that all you needed to stay protected was a firewall. Unfortunately, this mentality remained intact to a large extent until just a couple of years ago.

With better castle defenses, alternative ways of attacking a keep came about. Battering Rams, Ladders, and Catapults were often the methods used. During these “dark ages” where companies and networks felt protected behind their Magi not Line type defenses, several things changed in the way in which an attacker would attempt to compromise a network. Exploiting known vulnerabilities was a common method. Running a port scan and identifying services that were available such as FTP or Telnet. These could then be compromised using brute force attacks (breaking a username and password based on using either dictionary words, or systematically trying all possible combinations). Attacks like these were largely unorganized with a successful attack usually leading to the hosting of illegal programs, pornography or the defacement of a web site.

Castles were so popular that they quickly became the center of social society with aristocrats entering and leaving with their entourages. Similarly, the Internet quickly took on a life of its own in the mid to late 1990's. If you wanted to impress your customers, you had a web site. Next, your web site had to be interactive with all sorts of services such as online banking or other transactional applications. Each one of these services being offered to customers added another door attackers could use to compromise networks.

Modern day movies lead us to believe a castle siege would occur within a couple of hours. The reality is that these sieges could go on for months or years. I know of a successful attack of a network that led to the compromise of 20 million dollars in intellectual property. In this instance

the attackers waited patiently “pinging” or checking to see if the firewall was active every five minutes for more than 18 months. During a service release where something wasn’t working right, the company that was being monitored thought the firewall might be the problem and took it temporarily offline. During the following 23 minutes, all the intellectual property of the company was stolen.

Tactics to divert water into the citadel, cut off supply lines, or use catapults to launch diseased bodies over the walls were often used in an effort to drive people out of their strongholds. Pressure from partners, vendors, travelers, telecommuters, and others with the promise of a new ease and speed of doing business have forced companies to open their private networks to 3<sup>rd</sup> party and other remote connections. Each of these has a unique set of security risks and challenges that are often overlooked.

I couldn’t write this paper without making the obvious Trojan horse parallel. But this type of attack (in addition to malware, spyware, and other programs) has literally exploded recently. These attacks can permit remote attackers to do anything from keystroke logging to full remote control and are now commonplace. Combine this with peer-to-peer applications, instant messaging, and malware sites, and now your employees become the largest liability you have.

Someone broke into a home in my sister’s neighborhood a few winters ago. I found it interesting that you could see the footsteps of the perpetrator in the snow go from house to house, window to window, looking for the easiest target. Much like locking a door or window, companies that have deployed any security technologies would often raise them above the “low hanging fruit” status and therefore be bypassed by attackers until new methods of attack become available. Many strategists have said that a full siege of a castle would usually incur a loss of life at the ratio of 10:1. This was what the attacker had to be willing to lose in order to gain the prize. Until recently, this meant that because there were fewer attackers than there were targets, many networks were secure by virtue of the numbers. “Security by obscurity” is what I call it. Unfortunately, the tables have turned in this regard. With the advent of compromised systems called “zombies” being added to a network of similar systems called a “botnet” (robot network) where a single attacker can use the force of literally thousands of systems simultaneously to wage an attack, a siege is not nearly as difficult as it once was. In fact, it is quite easy to perform a distributed denial of service (DDOS) attack and take a company’s systems offline and this is just one common use of these botnet systems.

Combine this with the myriad of ways an attacker can gain unauthorized entry to a network, much like digging tunnels into the courtyard worked in medieval times, and the way in which we need to protect our networks has changed enormously in the past few years.

## **Defending your Castle – Is Your Network Really Protected**

Much like medieval times, a layered security approach was used to protect the castle and its inhabitants. Like wooden walls before stone walls were used, each defense devices protective capacity diminishes over time. This doesn’t remove the need for these devices. I don’t think I could convince too many people to turn off their firewalls, but we do need to realize that each risk mitigation component we use is only part of the overall defensive strategy.

A layered security approach is nothing new to hear. The problem, however, is that all-too-often, non security trained individuals will create a layered defense strategy that doesn’t reduce the overall operational risk. For example, I once had a business tell me they were twice as secure as the next business because they had deployed two firewalls. Digging in a bit deeper I discovered that the two firewalls were both configured identically allowing all the same inbound ports through. It took a little bit of explaining to show them how their second firewall offered no additional security value.

A layered security approach must be thought through. First, you should identify all your individual business processes and systems. Rank each of them with a score based on their value to the organization. Then list the protective measures you have already deployed for each system and rank their effectiveness in the following three categories; confidentiality, integrity and availability. Identify the “gaps” that exist in your defenses. You can even do this in a layered defense approach by reviewing the first line of defense (probably your firewall). In each defense layer, identify solutions that fill in those identified exposure areas. Because no individual solution is a “silver bullet” multiple technologies and tactics must be used to achieve a secure environment.



## **Risk Reduction Strategies – Minimize Risk without Maximizing Costs**

One common layer of defense in addition to the firewall is intrusion detection and prevention systems. These systems can look at the data that passes through the firewall using “deep packet inspection”. In other words, they look inside each packet and compare the contents to those of known attacks. Some IDS/IPS systems can also look at the behavior of some traffic and if it falls outside of “normal” thresholds, can also alert someone or stop the attack.

Using encryption is another layer of defense that can keep your data private. These systems are designed to authenticate the user to ensure they are allowed access, maintain the integrity of the data to ensure no modifications occur, and keep the data private from anyone else who might see it.

Another gap that you have probably identified is that of your users accessing web sites that may contain malware, viruses or other malicious code that can infect or compromise your network. For this layer of defense, I recommend web content filtering (sometimes referred to as URL content filtering) which can prevent your employees from accessing sites that could be a liability to your business. Combine this with browser anti-virus and you dramatically reduce the chance that viruses can come in from malicious web sites or other links that your employees may click on.

Gateway anti-virus is a method to detect and stop viruses before they enter your network. It can be found as an option on a firewall or other gateway device, or as a stand alone system. Gateway anti-virus is not meant to replace workstation and server anti-virus, but be an additional layer of defense in your overall virus strategy.

Another layer of defense is to perform regular vulnerability assessments. These “scans” can help identify vulnerable systems inside and outside of your firewall that could lead to potential compromise. They enumerate all available services and ports available on a particular system and then test those services for weakness using thousands of known exploit scripts.

These are just a few of the layers of security that should be considered from an intrusion defense standpoint. There are certainly many other useful and valuable technologies that can help protect your networks and sensitive customer information. Individual strategies around email defense, vulnerability defense, system defense, user defense and network defense should all be evaluated in addition to the intrusion defense strategies that have been discussed in this paper.

## “None Shall Pass”

Some companies have several well trained guards to protect their business from a physical attack. What I usually see is one guard that also has to lock and unlock the doors, fill out visitor paperwork, make the rounds, follow-up on phone calls and emails, watch the video camera, and keep out the bad guys. While there do not appear to be large threats on the horizon, we often feel like the physical walls and other defensive devices we have deployed should do the job and we can focus our attention elsewhere. Vint Cerf (one of the Internet's founders) recently estimated that 150,000,000 (nearly 25%) of the over 600,000,000 computers on the Internet are infected with malware or Trojan horse programs and are potentially part of a botnet army. He said this infection of Internet systems has achieved a pandemic level. Some say this is a low estimate. The vast majority of these computer owners do not know their systems are compromised. Attempting to defend your network from this magnitude of an onslaught is overwhelming. Enlisting the help of an “on demand” security provider can help with this burden. They can man the towers, monitor the defenses, guard the gate, maintain logistics, and watch for spies while you perform your other required duties.

Companies can be a little bit delusional about their ability and resources to guard the tower themselves. Lack of expertise with proper training and the appropriate amount of resources is like being the Black Knight on Monty Python and the Holy Grail. Whether you realize it or not, you may have serious exposure or some level of compromise now. You might think “It’s only a flesh wound” or are unaware of it altogether. Don’t make the mistake of thinking it hasn’t or can’t happen to you, because that is what they all say when I talk to them during or after an attack.

If you are considering using an “on demand” security provider, please look for the following when choosing a provider.

First, use one of the largest in the land. Large managed security providers are required to undergo the same, if not more rigid security scrutiny than you do by federal regulators. Knights would be required to show their pedigrees prior to contests. Ask a potential security partner to provide you with appropriate documentation that should include a SAS70 Type II report, 3<sup>rd</sup> party security auditing such as a Cybertrust TruSecure certification, and financials that show profitability and strong viability. Select a partner that is going to be around when you need them.

Select a partner that offers a wide range of security services. Vendor management is becoming nearly a full time job for some people. Reducing the number of partners you have will increase your organizations cycles for other tasks.

Select a partner that has a well developed user interface portal for reporting and management. You are likely required to present reports and other documents to executives, the board, auditors or examiners from time to time. These documents should be easy to download and should all be in one place. Ensure that the partner you use has a change request process that is recorded and auditable. This is increasingly important to auditors and regulators.

## Conclusion

Kings would often execute the architects of their castles because they didn’t want anyone to know of the secret entrances or what weaknesses the castle might have. I am personally thankful that this tradition has not continued into the modern day of network security. But designing an intrusion defense strategy that identifies the value of business processes, and implements appropriate strategies to protect these systems using a layered defense approach is not only a good security practice, but also a regulation in many cases. Perimeter eSecurity has a wide range of products and services that can protect your networks. Contact Perimeter eSecurity today for more information.

