Global Information Assurance Certification Paper

Greg Wilson
GSEC Practical
Option 1 Version 1.4b
Thursday, 20 May 2004

Defence in Depth – Ancient Methods for a Modern World.

Abstract

Defence in Depth is the concept of securing valuable information, data or resources behind a series of multi-layered protective barriers. By offering up multiple barriers, you are able to enhance the protection through a series of fail-safes that will allow you an opportunity to protect your valuables.

This paper will use the examples of two types of the fortifications used during medieval times and describe how, using Defence in Depth strategies, these systems protected the important resources of people and knowledge. Then, the paper will discuss how IT Security groups can employ Defence in Depth strategies, using modern technologies and concepts.

This paper will not attempt to provide a comprehensive solution to Defence in Depth but will hopefully providing guidance on steps that are often overlooked in IT Security systems; nor will it provide a comprehensive listing of attackers, but merely compare and contrast potential pitfalls in existing technologies and methodologies.

Background

There has always been information.
As societies developed, the effort to acquire information has always been great. To capture that information and distribute it has required more effort. It was always easier to lose than to gain. The individuals that created knowledge by application of their skills (carpenters, stonemasons) or had memorised or learned it from others, (monks, teachers) relied heavily on a civilised society that protected their knowledge and gave them the ability to spread and benefit themselves and their community. However, this hard won wisdom would disappear if a raid on their homes killed them. It became apparent that to progress, to become more civilised, a society had to protect its data, its sources of information, and its methods of distributing this information.

By the time of Medieval England, this responsibility had fallen to a King or Emperor. Royalty had become the protector of these valued resources. They built fortified towns and castles where the creators and holders of information were safe and secure from raids and destruction. In the earliest example of information security management, the security of these resources passed from royalty to the knights of the realm. They delegated this responsibility further on to the specialists, such as stonemasons, carpenters, and soldiers who created, fortified and patrolled the towns. These are the earliest examples of security specialists.

In modern times, this methodology is still in use. In most companies, The Board of Directors nominates the CEO. The valuable resources consist of the financial and human resources that create, maintain, and use the data that the company produces in its ongoing functions. The CEO delegates responsibility down to the mangers that will then delegate down to the specialists in each area.

More often than not, Information Security (InfoSec) specialists will have more specialised knowledge about the data and the systems than management, but will still have to fight an uphill battle for any kind of approval for security strategies.

However, the InfoSec specialists are providing the same function as the knights, soldiers, stonemasons, and carpenters of medieval times. Protect the sources (creators), the users, and the distribution of the propriety data. This time however, the data belongs to the company or the department, rather than the society.

Information Security Principals

It is important to note that all InfoSec principles are focused around the concepts of Confidentiality, Integrity, and Availability. (CIA):

"**Confidentiality**. Assurance that information is shared only among authorised persons or organisations. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e mailing or creating documents and other data etc. The classification of the information should determine its confidentiality and hence the appropriate safeguards.

Integrity. Assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose. The term Integrity is used frequently when considering InfoSec as it is represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but also whether it can be trusted and relied upon. For example, making copies (say by e-mailing a file) of a sensitive document, threatens both confidentiality and the integrity of the information. Why? Because, by making one or more copies, the data is then at risk of change or modification.

Availability. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. "i

Traditional protection

Before the royal lines of England were established, the country was divided into little pockets of concern that would generally incorporate the village and its inhabitants. There was generally a Chief amongst the villagers who was responsible for the safety and wellbeing of the village. These areas were the remains of Roman towns that had been abandoned as the Roman Empire crumbled into dust and legend.

Among the earliest forms of protection for a village were the Motte and Bailey designs for a castle. There are over a thousand recorded Motte and Bailey variations throughout the British Isles. The completed Motte and Bailey design would have a little like the drawing at Figure 1.

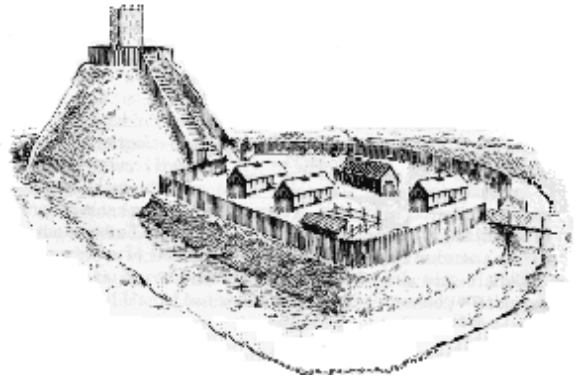

Figure 1 Motte and Bailey (http://www.castles-of-britain.com/castlesa.htm)

At the top of the hill would be a secure keep to allow defenders a clear line of sight of the surrounding area. More often than not, the surrounding tree line would be removed to make the walls and keep; this increased the clear line of sight.

The village would also be raised off the ground and surrounded with a stout wooden perimeter fence, this also served to keep chickens and livestock contained. Often there would be a moat or river surrounding the whole facility, which added an extra deterrent to the approaching enemy. In order to access the village, there would be a fence with a retractable drawbridge or some form of removable passage over the moat. The gates would be barred on the village side to slow down the attackers again.

This design provides a two-stage defence of the village and contents. Defenders in the keep would shoot arrows and throw rocks at the enemy while they were building bridges to get over the moat. If they successfully overcame the moat, the defenders would beat a hasty retreat to the top of the hill, surrendering the village to the attackers, while still being able to control the approach to the keep, as there was only one way in and one way out.

Traditionally, what would happen is that the attacker would plunder anything that was left behind in the village, set fire to the keep at the top of the hill and leave with what they had found. A smart defender would leave a small amount of valuable treasure, food or livestock in the village for the attackers to find. This would often assuage the attacker and they would leave, vowing to return with more fire and arrows for the rest of the valuable items. Truly persistent attackers would wait for the defenders and villagers to come out of the burning keep and then kill them, walking away with all the loot and valuables.

A New Approach

The arrival of William and the Normans (1066) and conquest of the Anglo-Saxons radically altered the course of English history. Rather than attempt a wholesale replacement of Anglo-Saxon law, William fused continental practices with native custom. By disenfranchising Anglo-Saxon landowners, he instituted a brand of feudalism in England that strengthened the monarchy. [ii]

By introducing the feudal system into the structure of Britain's monarchy, William the Conqueror was able to incorporate European practices of castle design and redirect the protection of the people by the Crown away from the traditional village defences into a more structured city based design.

Over the centuries of British monastic rule, there have been countless designs for castles and fortifications. One of the greatest examples of these designs is Beaumaris Castle in Wales.

"Beaumaris, begun in 1295, was the last and largest of the castles to be built by King Edward I in Wales. Raised on an entirely new site, without earlier buildings to fetter its designer's creative genius, it is possibly the most sophisticated example of medieval military architecture in Britain." [iii]

This partial map of north Wales, in Figure 2, shows the locations of what many consider the important or major castles for North Wales.

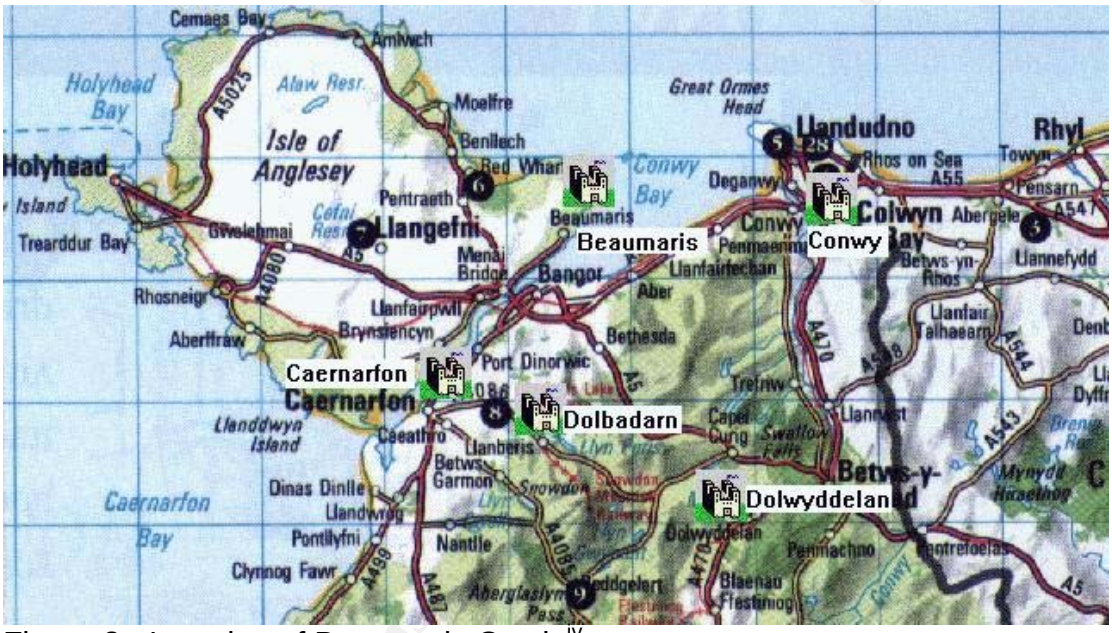

Figure 2 - Location of Beaumaris Castle[iv]

The layout and design of Beaumaris Castle is possibly one of the best examples of Defence-in-Depth available from the period. The layout of the castle can be seen below in Figure 3.

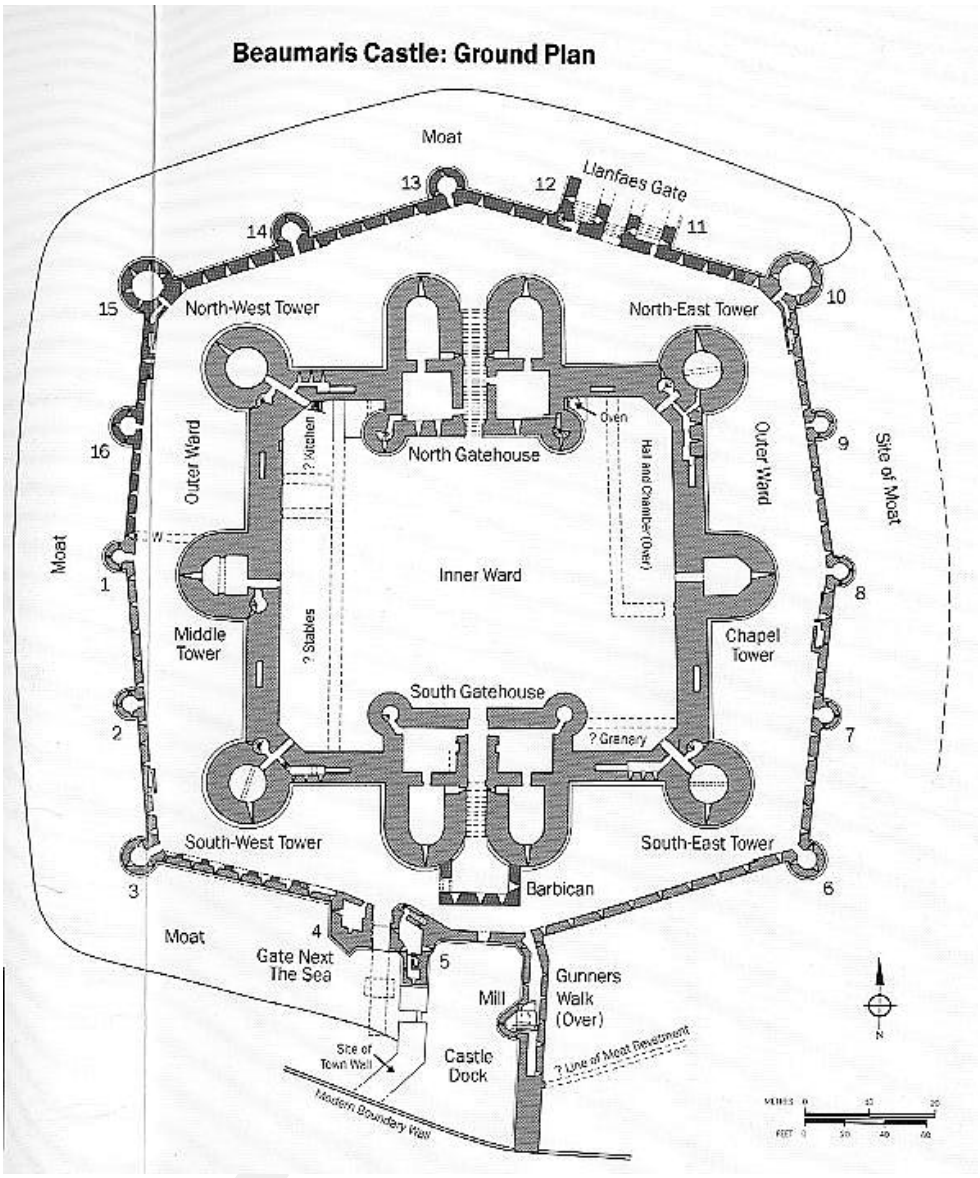

Figure 3 – Beaumaris Castle (http://www.castlewales.com/database.html)

As can be seen on the map above, the castle was situated on a raised area that was located close to the sea. The architect, Master James of St George, allowed seawater to flow into the moat, which provided the second stage of fortification by slowing the approach to the outer walls. Access to the castle is limited to the Llanfaes Gate (pronounced Tlanfaes) on the Northeast wall, which provides land access for defenders and the Sea Gate on the Southwest wall. This gate was protected by an extension of the wall, which allowed access for gunners and archers, allowed naval access to reprovision supplies and remove the wounded during extended sieges.

The outer wall consists of 16 towers that would contain archers, boiling oil and stones, which would be dropped onto attackers that had breached the moat and would be attempting to scale the walls.

The northern face of the castle was reinforced to provide a much more difficult target. The eastern and western walls were thinner, yet still thick enough to cause a significant challenge to attackers. The defender would discourage attacks on the eastern and western walls and would drive the attackers with archers around to the northern wall. This would

sometimes be encouraged by weakening the northern front to make it seem easier to attack.

The inner keep's walls were of a much thicker design with passages and hidden niche for weapons and supplies. On each of the towers surrounding the inner keep, there would have been catapults or arbalests that would provide an added level of defence by throwing rocks, oil, cows and other less savoury matter at the enemy. (I'm serious about the cows!)

In the event that the enemy broke through the outer wall, the defenders would retreat to the inner keep and bolster the defences. The enemy would be hard pressed to operate siege equipment such as catapults against the inner keep wall, due to the relatively close proximity of the outer wall to the inner keep. The enemy would have to resort to battering rams in order to take down the gates and then gain control of the castle.

Modern interpretation

Now that the history and concepts of the Medieval Defence-in-depth approach has been discussed, how does this relate to the modern InfoSec methodologies that should be adopted?

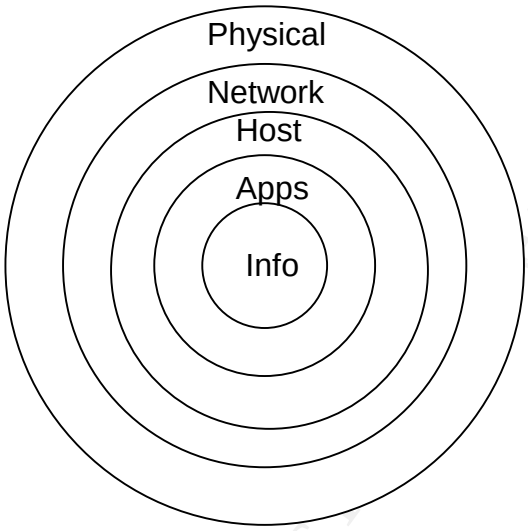

Figure 3 – Defence in Depth model

The concept of Defence-in-Depth can be looked at like an onion. An onion has multiple layers surrounding the core, with each layer requiring removal and cleaning. Unlike an onion, Defence-in-Depth should not make you cry.

With more and more information being made freely available, steps have to be taken by InfoSec practitioners to protect the organisation's valuable information. As in the medieval models, Managers and Executives mandate InfoSec to create protective zones surrounding the information that is generated by the organisation.

The model above demonstrates the practices of Defence-in-Depth all to maintain the principles of CIA for all information held on the network. When considering InfoSec on a network, the basic aspects are:

- Physical Security
- Network Security
- Host Security
- Application Security
- Information Security

In the early days of InfoSec, life was simpler; there were not so many attackers and fewer connections to the outside world. Universities exchanged information in the interest of scientific advancement. Computer Systems were complex, expensive rooms full of technology that would be used to calculate the movement of air across a wing, or the effect of a tornado through an American Mid-West town.

The Internet was still in its infancy, connections were often very low speed (8k, 16k, 31.2k and heaven forbid 56k baud rates). High-speed connections were rare and expensive mainly used by Military and Universities.

Attackers were generally highly experienced programmers who would target institutions looking for commercial data or military secrets. Historically, the "hackers" were gathering information to sell to the highest bidder. The final buyer would often be foreign governments or corporations.

In recent times, with the advance of Information Technology, low cost, high-speed home systems have enabled the attackers to become more knowledgeable and therefore more virulent. Operating systems are easier to use, Broadband connections provide faster access to international computer systems and there are more exploitable vulnerabilities that can be identified with less high-end knowledge.

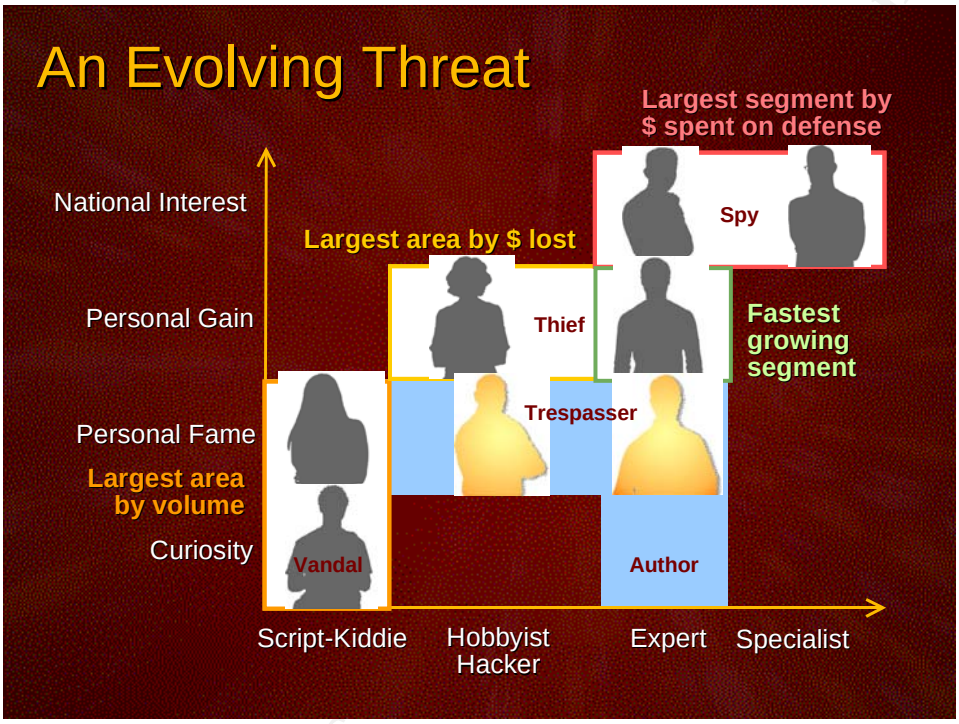

Figure 4 - Extract from Keynote Address Microsoft Australia Security Summit March 2004[v]

While the list of attackers grows, so do the avenues for attack:

"Among these new crimes are computer hacking, denial of service attacks, unauthorised access to information, on-line fraud and potentially, cyber-terrorism. Recently, the massive distributed denial-of-service attack on major US web portals refocussed the public's attention on the disruption that may be caused if web security is breached."

"… The Internet is the medium for increasing the range and content of computer based communications. The growth of the Internet is estimated to be doubling somewhere between every 100 days and every 12 months. Between 1996 and 1998 the number of adult Australians with access to the Internet at home increased from 262,000 to 4.2 million."[vi]

"According to University of Queensland's (UQ) Director of Information Technology Services and AusCERT Nick Tate, a total of 8197 computer security incidents were reported to AusCERT last year representing a four-fold increase on the number reported in 1999.

"Incidents were commonly either network scans, viruses or distributed denial of service attacks," Mr Tate said.

"The number of Distributed Denial of Service attacks has increased. In part this is due to the development by the intruder community (also known as 'hackers') of more sophisticated versions of these tools."

The following statistics were drawn from incidents reported from sites both inside and outside Australia, although the majority of incidents were reported by sites within Australia and New Zealand.

Year Total incidents

1998-1342
1999-1816
2000-8197"[vii]

Putting Defence-in-Depth into practice

Traditional computer systems were focused generally on mainframe systems. These consisted of large central processing units and input was through a dumb terminal, which was normally hardwired into the system through dedicated lines.

As such, the early forms of Defence-in-Depth focused on only two or three layers to maintain the CIA of the data and systems. The most cost effective of these measures was Physical Security, as the belief was that if you couldn't physically access the computer room, you would have great difficulty stealing information.

Early Days

In order to demonstrate the early forms of Defence-in-Depth, the following compares Motte and Bailey fortifications and InfoSec Defence-in-Depth.

Physical Security –

- In medieval times, a raised keep that was secured by wooden exterior walls, a moat and a big lock on the door determined physical security.
- Early InfoSec practices consisted of computer rooms and labs generally kept within secure buildings behind locked doors and security guards. An attacker would not have been able to access the labs without the appropriate clearances and there was generally a "no-alone" policy in place.

Network Security –

- In medieval times, the moat, drawbridge and guards on the door would discourage unauthorised access.
- Early InfoSec practices consisted of administrators limiting external connections to the network and ensuring user authentication.

Application Security –

- In medieval times, rocks, arrows and men with swords would keep away attackers and other potential threats.
- Early InfoSec practices consisted of the installation of simple antivirus software, thereby reducing potential damage and as access was limited through the use of dumb terminals and aggregated user accounts, the only potential problems would be introduced by the user.

Today

Current network technology allows access to local networks from almost anywhere in the world using high speed switching environments and the standardisation of the TCP\IP protocol suite.

As medieval attackers became more sophisticated, so too did the medieval architects, developing stronger layers of Defence in order to keep the people safe. In a similar manner, Security Professionals are required to implement new levels of protection to secure organisational information from the modern attackers.

Physical Security –
- Stout exterior walls, a deeper wider moat surround the Keep. A bigger lock is put on to a thicker door with a portcullis or gate in front of the door.
- Computer Rooms and Labs are still maintained within secure buildings behind locked doors, alarm systems and sensors and security guards. There is no access the labs without the appropriate clearances, and there would often be a “no-alone” policy in place.

Perimeter Security –
- Guards would patrol the surrounding area, and maintain vigilance throughout the night.
- In order to maintain a logical perimeter around data, Firewalls and Virtual Private Networks (VPN’s) Quarantine can be installed.

Network Security –
- Traditional segments would involve the separation of valuables into multiple chests within the castle.
- To protect the network, administrators should install a series of network segments, encryption of network packets using IPSec and run a correctly configured Network Intruder Detection System (IDS).

Host Security –
- Stonemasons and carpenters would constantly inspect the walls for cracks, holes, or signs of excavation. Often the best means for defeating an exterior wall would be to dig under and then set off explosives.
- This layer protects the operating system that the data is accessed through. Measures to consider when securing a host are OS hardening; closing ports, removing known vulnerabilities and changing default install components; establishing a Patch Management policy; access authentication through the use of a token or strong password policy; and the implementation and maintenance of a Host IDS.

Application Security –

- Literacy was rare, and the majority of information in medieval times was stored in the minds of the clergy and master builders. The simplest way to secure this information was to lock them up to avoid having your knowledgable people stolen.
- This layer of security encourages the hardening of application through the removal of default administrator passwords, known backdoor vulnerabilities and installing antivirus software and a policy that allows regular updates to keep up with the number of virus variations that are released.

Information Security –

- In the rare times that knowledge was recorded, the information itself and access to the information would be severely restricted.
- This last layer of security uses strong encryption of data and Access Control Lists (ACL) to compartmentalise user access so that only those who need to have access are able to do so. This process is often referred to as Need-to-Know.

In the Motte and Bailey fortification example, the defenders would often leave valuables behind in the village to try to deter attackers from continuing the attack on the main keep.

This style of security could be compared to a Demilitarised Zone (DMZ) with Honeypot attachment. Valuable information is stored within the private network, in this instance the Keep. The village at the bottom of the keep would be a DMZ. The DMZ acknowledges the fact that attackers will attempt to access the system, however, while they are in the DMZ it can be monitored and the defences prepared if the DMZ appears to be in jeopardy of being bypassed.

By leaving tangible information in the DMZ in the form of a Honeypot, the standard attacker is deterred. Only the truly persistent attacker will ignore the Honeypot and make attempts on your inner keep. Thankfully, there is little chance of the truly persistent attacker setting fire to the keep wall and waiting for you to run outside carrying your valuable data.

Honeypots can, however, lead to serious Security incidents, especially if the attacker realises that they have been mislead. A good hacker may well desire some form of revenge upon the network that is protected in this way. This strategy should be used with caution.[viii]

Lastly, one of the keys to having a good Defence-in-Depth strategy is the establishment of an IT Security policy and awareness program for both Users and Administrators alike.

The SANS Institute define IT Security Policy as:

“A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an “Acceptable Use” policy would cover the rules and regulations for appropriate use of the computing facilities.”[ix]

Examples of IT Security Policy would cover:

- The connection of PDA's, laptops and portable devices to the network,
- The classification and aggregate access levels to the system, outlining clearance requirements for the users,
- Auditing policies, outlining legal requirements and management expectations for the system's Administrators, and
- Incident Handling Policies for the IT Security personnel.

One consideration when writing IT Security Policy is that the policy should have Executive Management endorsement. There should also be active enforcement of the policy, having a policy and storing it on the shelf, is as useful as having a fire system with no water pressure.

A recent article in ZDNet Australia on Security Education Programs suggested:

"A corporate security awareness program aims to make all employees understand and appreciate not only the value of the company's information assets but also the consequences in case these assets are compromised."

"E. Kelly Hansen is the CEO of Neohapsis, an information security consultancy and enterprise product-testing lab. She stressed that executive buy-in is paramount. "Without a corporate leader visibly backing the program, people are not going to be as eager to participate. Training takes time away from people's regular job functions. In a day in which many companies are understaffed, training doesn't seem to be a valuable trade-off. Tyranny of the urgent rules most organisations. Without visible executive stewardship, information security awareness programs are doomed to fail." [x]

While developing education awareness presentations, it is important that the delivery is targeted for the appropriate audience. Giving an in-depth presentation on the inner workings of the Network Intruder Detection System is not going to impress the Human Resources Manager. It is also important to vary your delivery methods.

Delivery methods that are currently used within the Australian Department of Defence include:

- Presentations to staff and administrators about social engineering
- Monthly newsletters outlining new devices that can be used to bypass IT Security systems
- Advice on new or unusual types of Malicious Software (Malware) and Virus attacks that have been identified in the media
- Stickers and posters reminding people of their responsibilities

One of the greatest historical examples of failed security policy and education was The Trojan Horse.

The Greek philosopher and writer Homer recorded the story of the Trojan Wars in his epic books, 'The Odyssey' and 'The Illiad'. Additional information can be found on the Internet and most recently, glorified in the movie 'Troy'.

In short the story goes that after 10 years of battles and siege, the Greek army had finally reached an impasse at the city of Troy. In order to end the extended siege, the Greeks built

a giant wooden horse, which they then left at the gates of the city of Troy as a peace offering and then withdrew from the siege of the city.

The Trojans, believing that they had won the battle, tore down a section of the wall in order to bring the wooden horse into the city and began to party like there was no tomorrow. The handful of Greeks, who were secreted inside the horse, waited until the early hours of the morning when the last Trojan had fallen into a drunken sleep. Then they leapt out and slaughtered the Trojan defenders mercilessly.

The Trojan horse analogy is often used to describe known viruses. Trend Micro Systems, a leading vendor of anti-virus software provide this definition:

“A Trojan is malware that performs unexpected or unauthorized, often malicious, actions. The main difference between a Trojan and a virus is the inability to replicate. Trojans cause damage, unexpected system behavior, and compromise the security of systems, but do not replicate. If it replicates, then it should be classified as a virus.

A Trojan, coined from Greek mythology's Trojan horse, typically comes in good packaging but has some hidden malicious intent within its code. When a Trojan is executed users will likely experience unwanted system problems in operation, and sometimes loss of valuable data.”[xi]

Apart from being a great story, lessons can learnt from the Trojan mistake. Multiple layers of security may well surround data, however, without educating users and administrators about sensible security, the keys may as well be left in the lock and the doors and windows all left open.

Summary

As can be seen, there are not that many differences between building a castle and securing an organisation’s data. It is essential that strong boundaries be established both physically and logically around the data and information that is being protected.

Recognition of vulnerabilities in systems through awareness programs for all staff will reduce the likelihood of attackers getting through the security systems and methodologies that have been put into place.

Information, either literal or electronic, is the key to any Kingdom, whether medieval or corporate. It must be protected at all times.

References

i Extract taken from http://www.yourwindow.to/information-security/gl_confidentialityintegrityandavailabili.htm

ii Extract taken from http://www.britannia.com/history/monarchs/mon22.html

iii Extract taken from http://www.castlewales.com/beaumar.html

[iv] Map taken from http://www.castlewales.com/wales_n.html

[v] Microsoft Australia Security Summit March 2004 presentation obtained from http://www.microsoft.com/australia/security

vi Extracted from Australian Federal Police's Director of Technical Operations Federal Agent John Geurts report presented at the Australian Chapter of the American Society for Industrial Security Conference 'Fraud — The New Frontiers' in Canberra March 1999. http://www.afp.gov.au/raw/Publications/Platypus/Mar00/intfrd.htm

vii University of Queensland (2001), AusCERT notes substantial growth of computer security incidents

viii For more information on Honeypots, refer to http://project.honeynet.org/ or http://www.honeypots.net/

ix Extract taken from SANS Institute http://www.sans.org/resources/policies/

[x] Success Strategies for Security Awareness by Ruby Bayan, TechRepublic 07 May 2004 extract taken from http://www.zdnet.com.au/insight/security/0,39023764,39146878,00.htm

xi Extract taken from Trend Micro website http://www.antivirus.com/