Global Information Assurance Certification Paper

Merging Physical and IT Security and Remote System Surveillance

GSEC Practical Version 1.4b Option 2
Pavel Okorn
July 16, 2003

Abstract:

There is a growing number of evidence showing that companies whether private or public, are trying to merge their security operations.

This paper gives a detailed explanation of how I merged both words into one in the project of securing swimming pool premises, connecting buildings together through wireless network, connecting wireless cameras to the network, securing the wireless network, securing the entire system, teaching employed personnel about security measures and putting the entire system under control from my company.

» Let our advance worrying become advance thinking and planning. « Winston Churchill (1874-1965)

Introduction:

To point out factors that can help us understand the fact that companies whether private or public are trying to merge their security operations we should underline the most important ones:

Firstly, digital technology, video and sound manipulations have moved to the territory of physical security products. Cameras are becoming completely digital with embedded Linux and can be connected directly to the Ethernet cabling. Computers have huge possibilities to manipulate and store video streams, remote system surveillance and storage, messaging system and remote camera manipulation.

Secondly, as **economic conditions** all over the world seem to be deteriorating, companies do whatever they can to minimize their expenditure and increase profits. Security budgets are not to be neglected, especially when considering the fact that IT security is becoming very important and can cost a considerable amount of budget chunk.

Thirdly, **security threats are somehow computer related,** as companies have become more computer and internet dependent. Malicious hackers and thieves have discovered that computer technology data as well can pay off and are worth the trouble [(1)].

"**Corporate IT systems have become complex, ungainly and difficult to manage. It is almost as though the technology took over, « says Irwing Wladawsky-Berger, General Manager of IBM.** [(2)] It can be said that human factor can play a substantial role in implementing IT systems and can be the biggest obstacle if not properly managed and supported from the management. The latter must strive to keep in touch with the **constantly learning society**.

Managers of the company asked us for a solution to their problems regarding physical security in the swimming pool.

Our task was:

- To install cameras in dressing rooms, where people left their belongings before entering the pool. There are four places with two rows of lockers in which locks have been broken repeatedly.

Examining and defining the existing system:

After examining the whole system, the following was discovered:

- The rooms with the lockers were small and the placement of the cameras could cause problems, as a rather wide angle of the lenses had to be used. Furthermore, thieves or vandals could easily reach cameras.

- Lights in the rooms were not sufficient for the cameras to operate satisfactory.
- There were two stand-alone computers at the cash desk with Win98SE.
- Programs for the cash desk in DOS environment were still in use.
- There were four computers in the first floor lecture room, not connected to the network, Win98SE installed.
- Computers in the headquarters building about 100 meters away from the pool were connected to the internet by ADSL, all with Win98SE installed.
- The system in HQ was completely unsecured with outdated virus definition tables. Windows 98SE not updated with recent critical updates as well as Win Office too.

After discovering that the existing system was badly managed lacking many very important issues especially regarding security, we proposed the company to merge IT security and servicing as well as physical security under one roof and one leader, who could control the entire corporation and manage the system. Thus, there would be a substantial reduction in expenses and the whole system would be more flexible and easier to operate, as for the time being they were outsourcing two companies - one for the physical and one for managing their IT system.

Decision making:

»Physical security assessments include evaluations of security requirements, including threats and vulnerabilities, policies and procedures, personnel response, mechanical and electronic security measures, access control, employment of closed circuit television, alarm systems and other measures necessary to ensure detection, assessment, response, delay, and neutralization of potential adversaries. Vulnerabilities and associated risks are identified, and recommended countermeasures such as improvements to facilities, equipment, personnel, plans, and procedures are selected. « (3)

In order to abide by detailed security assessment directive, our task to implement efficient system was not an easy one. Technology is advancing at such a pace that it can be hard to keep up to date and offer the best value for money at the same time.

When deciding what kind of system to produce, our primarily goal was to offer and possibly install a system that would focus on:

- The cost of the system,
- Efficiently using the existing system,
- Scalability,
- Compatibility,
- Openness for future expansion,
- Required maintenance and service,
- Risk and cost-balanced physical security enhancements,
- Simple and proof control of the cameras,
- PC hardware stability,

- Stability of the recording software working together with the software already used by the personnel in the cash desk,
- Efficient backup of the system,
- Overall security of the system,
- Security against inside intrusions,
- Traceable usage of the system and implementation of the usable and not expensive IDS,
- Easy to manage,
- Make good and understandable policies for using the system by employees and management,
- Efficient response plan,
- Social engineering.

Our proposal was to use digital cameras, which could be plugged directly to the network as existing computers could be used for recording activity of the cameras. As there was no network between existing computers, we proposed to install network cabling for existing computers as well as cameras and at the end install a camera in the swimming pool, which could be reached directly from the internet as web camera. Web camera can be effective for marketing purposes since web page with camera can attract more visitors to it as well as swimming pool. We also proposed to connect the whole system to the main building and to the internet. As the main building is around 100 meters away, we decided to offer wireless connection, which would be cheaper and more convenient as well as scalable for the future use as there were plans for new buildings, therefore the relocation of the wireless system would be very cost-efficient.

Summarizing the problems prior to building the system:

Since the beginning, we had been aware that it was going to be a difficult task. We decided to tackle physical security first, which was the primary goal granted from the company and to later connect the whole system to the internet and at the same time do security on the system as a whole.

To summarize what problems such system can pose to the company implementing it, I would like to point out a few that cannot be neglected and pose serious threat to the system implementation and overall usability:

- Having both systems on the same network - physical security and computers - malfunction of the system can occur with both systems collapsing.
- A further difficulty for employed personnel – learning curve and possible "obstruction" from inside.
- Vulnerability of the system connected to the internet - intruders can access cameras as well as computers for recording.
- There are few IT companies that can manage both systems – Broader knowledge is required, as there is Linux in the cameras, not to mention various Windows operating systems on the computers and special software for controlling cameras. There are few companies with IT personnel that can cope with cameras and adjust

lenses, programming all the possibilities in the cameras - cameras are by no means easy to program.
- Negative attitude towards new system among employees.
- Privacy concern for the visitors of the swimming pool.
- Wireless security problems and possible "blackouts" or broken connections caused by instability of the connection and possible interference.
- Badly secured wireless can be very popular among wardrivers and malicious hackers.
- Effective "defense in depth" security is necessary.

Building the system:

We offered the company **11 main stages** of the physical as well as IT security installation of the system. Those stages we than realized through **15 sub stages**.

1. Auditing and documenting the premises
- Identification of assets,
- Snapshots of the premises and infrastructure,
- Creating the documentation for later analysis and brainstorming,
- Human resources, level of IT knowledge,
- Hours/Days of operation,
- Activities performed at facility,
- After hours personnel - when and where,
- Is facility exterior/ interior patrolled - when and where?
- Suitability of site and landscape for wireless connections,

2. Analysis
- An analysis of the current threat to all qualifying assets,
- The locations of all organization's operations,
- A review of security and criminal incidents within the premises,
- Theft by non-staff,
- Theft by staff or contractors,
- Possible sabotage,

3. Defining needs
- Hardware and software needed,
- Human resources to take active part in the project,
- Possible future expansion needs,

4. Making complete installation plan, wiring diagram, position of cameras and computers, routers and switches

5. Finding possible weaknesses and vulnerabilities
- Brainstorming the plan, consulting managers of the company and employees and taking active part in the project,

6. Implementing policy
- Time schedule,

- Considering possible outages of the existent system when implementing, Making efficient timetable to maximally reduce possible outages,

7. Security policy

- Physical and IT,
- Complete assessment of the usage,
- Control, auditing and management of staff, contractors and visitors,
- Specifications,
- Contract documentation,
- Backup policy,
- Reporting,
- People in charge,

As for the foremost importance, we weighted security of the system, possible **vulnerabilities, risk and possible losses of assets** versus the implemented system. We evaluated possible losses in data assets and stealing valuable information. The weakest point in the whole system was surely operating system. We were forced to stick to the preinstalled Windows 98SE environment. This was the fact and risk acceptance. We made **BIA- business impact analysis**. We determined possible impact levels on the operations of the company. As they are outsourcing all major and very important operations-accounting, payrolls, risk acceptance was somehow easier to determine and obtain.

The most important was **defining anti virus and firewall policy**. There was none before. Our policy when installing antivirus and firewall protection as well as other malware detection is uniform if possible with all the systems we support. We secure all machines and the whole system separately. We stick to **Norton antivirus [13]** products, **ZoneAlarm [10], Blackice [17] and AdAware [9]**. We tested behavior of them on various systems and various circumstances. We prepared short guidelines for users we have contracts with. Therefore, we can easily solve the problems over telephone or direct connection over internet. We are prepared that lines are hot for the first few days, after implementing new software.

We also prepared **short guidelines and policies with security measures** of how to use mail and how to "safely" browse the internet.

Upgrade policy and patching is also very important. We do the job weekly and this service is very well documented in our servicing contract too.

8. Training policy

- Security awareness training for an organization's staff to improve their personal level of security in the workplace or at home ,
- If possible, we find in company a person with better knowledge and will to be a "contact". We always discuss such policy with the managers of the company who have to apply policy for the person involved.

9. Installing hardware and software

10. Monitoring and testing

Stages 9 and 10:

1. In the first stage, we installed all the cabling for the existing computers, planned cameras, as well as predicted possible future connections.
2. Installation of the software and configuration of the cameras.
3. Testing of the system and giving instructions as well as teaching the personnel.
4. Installation of the wireless multipoint router and switch in the main building, connecting the system to the internet and rearranging the network and computers there to comply with the security demands on such system.
5. Installing the wireless router in the newly installed network in the swimming pool and connecting the whole system to the main network in the main building.
6. Making second network segment in the second floor of the swimming pool and connecting that network over wireless to the main system.
7. Testing the whole system for few days for possible malfunction or possible bottlenecks.
8. Connecting the camera in the swimming pool intended for internet use to the internet and transforming it into web server.
9. Installing VNC software on all machines to be able to control them and help people solve the problems from remote office, as well as make possible reprogramming of the cameras.
10. Installing special software on our server to respond to security messages sent from the system in swimming pool.
11. Installing of the backup system for controlling the cameras at second location
12. Installing remote camera and illumination on the parking lot.
13. Installing PC with Linux, Kismet and Snort to control and register possible intrusion detection.
14. Installing wireless access point and the camera for the swimming pool outside.
15. Connecting web camera to FTP server, sending there stream of pictures and having that FTP server as web server for the camera.

First Stage:

Installation of the cables was straightforward without problems. Power supply bank was installed for the cameras to control everything from one room to avoid possible grounding loops and have all cameras and the main computer on the same UPS. We planned to install the software for the cameras on the existing computer in the main entrance control room, where there were two computers for cash desk. For the first stage, this would be the main system to control the cameras in the dressing rooms. We installed the switch and power supply bank for the cameras. As there were only four cameras to control for physical security, we supposed there would be no substantial burden on the computer. We simply installed extra hard disk and memory.

Second Stage:

Installation of the software for camera recording. Working environment on the machine was windows 98SE. We had to take into consideration that there was software used in dos environment for cash desk and bookkeeping as well as printing of the invoices. We had to stick with Windows 98SE environment. This was a considerable problem as windows 98SE system is completely insecure.

Third stage:

This stage was the most problematic. Not the testing of the system but giving instructions to the personnel working there, which was completely unaware of the responsibility, they were entrusted with. The knowledge about computers and operating system was on such low level, that we spent a considerable amount of time explaining practically elementary knowledge and possible control of the software. This stage was planned for testing and teaching the personnel how to use the whole system and how to react in case of burglary or system malfunction. As the recording is completely automatic, there is no extra burden on personnel. The software installed has all kinds of messaging systems employed and cameras as well. The software has visual as well as sound messages in case of malfunction. As the cameras are recording only when movement is detected, 40 GB disk was sufficient for few days of recording. Recording is automatic and working on first in first out basis when the capacity of the hard disk is reached allowed recording maximum.

In spite of the almost automatic recording possibility, we had to teach them to observe messaging possibilities and sound reproduction of the security messaging system of the software. They were given enough time to get used to the system, before proceeding to next stages.

We were not aware of the possible problems with the local physical security company, which was working over night. They broke into the system because they were interested about the possibilities of the system and software core. They also presented their solution at the public competition, but lost it as their offer was not scalable and offered only physical part of the security possibilities. At the beginning we did not secure the software with passwords because of the testing, therefore the access was not secured. At first, we thought that system was breached by working personnel there, but at the end, we found out, that night shift was "researching" the system. We immediately secured the software with passwords and restricted the access. Unfortunately, the windows 98SE were almost impossible to secure, so we had to stick to the security implemented in the software for cameras only.

We learned here, what was evidently true in implementing security measures in IT systems, that there was considerable threat to security measures from within the company or contracted companies.

Fourth stage:

This was the most important stage. Headquarters of the company were located in the building about 100 meters away from the pool. There we had to change the existing system to be able to accept wireless connection and distribute the signal to the pool. We found out that the existing system was completely unsecured and connected over router and ADSL modem to the internet. The computers were also unsecured and connected to the internet over the hub and router. Virus detection software was outdated and there was no intruder detection software installed.

We proposed to the management of the company that all the machines as well as complete system on the router side had to be secured separately. First, we tested all machines with updated virus detection software from Symantec internet site. Then we installed Symantec upgrades. We tried to explain to users that upgrading machines with latest virus definitions is crucial and that sometimes viruses can "come" into the system with unsolicited mail and infect it before our system can be upgraded with new virus definition. Then we upgraded all the machines from Microsoft automatic update site. This did not proceed as smoothly as we expected. We left automatic upgrade facility off, as burden of the newly installed software and messaging system would pose heavy weight on the users. The company that was servicing the system before was not paying attention to upgrades-security or to regular Microsoft upgrades of the operating system. We used the time to give advice to the personnel and teach them what we were doing and how important it was to understand what could happen if the system was not secured properly, not to mention why it was important to upgrade the operating system with the latest patches. We also changed hub with switch, as to extend security on the network.

We tried to explain to employed personnel as much as possible about worms, viruses and other malware as well as how there are plenty of possible sniffing methods in the wild.

After upgrading all the machines, we discovered that one of them had problems with the previous software for bookkeeping installed. We had to contact company that installed it and obtain new version. There were also problems with banking software, which was malfunctioning with the new explorer ver.6.0. Again, calling the bank and installing new version with all security precautions.

We installed **Norton antivirus** [13], **ZoneAlarm** [10], **AdAware** [9], **Blackice** [17] and **VNC server** [11] on all machines. If we just look at the recent CERT note about malware, we were on the "right side":

http://www.cert.org/incident_notes/IN-2003-01.html

Again, a considerable amount of time was spent giving instructions to personnel why all this software was installed why it was needed, how it was functioning and what has to be done when these utilities were displaying various messages. Although very useful, functioning and need of these programs can sometimes be very hard to

understand for people without knowledge of operating system capabilities and functions. Neither were the managers aware of what could happen and what measures had to be taken on not only IT side, but also that employed personnel had to be aware and had to learn about security precautions and how to react when something happened. At the end, we decided together with the manager of the company that our company would completely overtake all the possible controls of the system and implement policies for security measures regularly.

We demonstrated the security of the system with very interesting security testing possibilities company **GFI** is offering on site:

http://www.gfi.com/emailsecuritytest

Firewall functionality can be tested with **Firewall Leak Testing Utility,** as well as easily demonstrated to users.

http://grc.com/lt/leaktest.htm

On every machine, we installed **Microsoft Baseline Security Analyzer** [15], **Regclean** [16] and **Startup Cop** as well. These are very useful utilities for testing the system from time to time.

We taught them also some very important features about backups of the system. We make always two partitions on the disk. One for programs and the other for data. In addition, when everything (supposedly) is installed, we make image backup of the primary partition to CDs. The same we applied through this project.

We configured the wireless router as multipoint, implemented WEP security and installed software for automatic WEP key distribution. We also left the possibility to control the router from the internet for the initial time, which we needed to control the port routing and forwarding to the internal network as well as Web camera.

Fifth stage:

At the side of the swimming pool, we installed the wireless access point/router to connect the whole segment to the main segment in the main building. We realized that our presumption was right and we had very good signal without extra antennas. We "put" the access point/router on the window, configured WEP and measured the signal strength. We were at 11 MBps. When testing the connection for few days, the connection fell down few times. We connected the scanner to the system and found out that one network card was malfunctioning. When you have cameras on the network for security purposes, you have to be very strict in deploying the system, as stream of pictures can easily congest the system, causing severe trouble.

Sixth stage:

At the second floor at the swimming pool, we had a small network segment and we connected it with wireless access point/router to the main system. Again, signal was very good without extra antennas. We configured WEP.

Seventh stage:

Now was the moment to test the whole system, especially reliable connection over both wireless systems to the internet and from the internet. We also measured the usable perimeter of the signal around the transmitter. We discovered that the signal was very weak in the first nearby buildings and not strong enough to be used by possible intruders there. This was our luck, as we did not need to use special antenna or booster to connect both buildings; therefore, the complete perimeter was not reaching the nearby buildings. The greatest problem proved to be the parking lot, as there somebody could easily scan the system from the car. We checked the connection to the whole system and individual machines as well as web camera from our office over Cable network and discovered that there were no bottlenecks on the system.

Eighth stage:

Now was the time to connect to the open Web camera.
We tested the connection to it from various sources and at the same time, to test possible congestion of the system.

Ninth stage:

This stage was considerably interesting from the security perspective. Access to all machines was tested with **VNC** client software as to find out if it could be of use to employees that we could help them from our offices over internet in case problems arose. We demonstrated usage and possibilities.

Tenth stage:

Now we were able to put into function backup software for messaging system over IP on our server at the main office that could intercept alarms from the security software at the pool. We made the tests and everything was functioning without problems. There were three possibilities employed. System sends mail message that there are problems, sends pictures to the FTP server at our office as well as message over TCP port.

Eleventh Stage:

Now was the time to install backup system for the cameras. We installed it in the special room, away from the main system. This machine is recording in parallel and has the same function as the main one, which is now used only for live control at the cash desk. The room is secured and distant and one of the cameras controls access to it.

Twelfth stage:

Surveillance wireless camera was installed on the parking lot. As we installed cameras with built in wireless on other projects, which are functioning without problems, the integration into the system was straightforward. We installed two strong reflectors with movement detection sensor as well for night detection and better quality of the picture. Again, we installed WEP.

Thirteenth Stage:

This stage is very important as well. We have employed considerable wireless system connections. We were in doubt what measures to implement, to control the wireless access and detect possible intruders, or better, as intruders first scan the system and test its vulnerabilities it is very important to be able to trace them before the final attack. We decided to install Linux on unused machine, which was outdated for hungry Windows operating system but appropriate for Linux implementations. We used Kismet for testing purposes or **Netstumbler** **(12)**. As Kismet is proper for this, we installed it on the Knoppix Linux distribution. We use **Knoppix** **(6)** on CD to test systems that are down, malfunctioning and have possible viruses or worms "installed". Knoppix has also some other very usable tools on the distribution – **Ethereal**(8) , **Nessus** **(7)** and its best is, that can be started from CD. What can be better, when testing systems that were breached or infected?

In parallel with **Kismet** **(5),** we installed **Snort** **(14)** for intrusion detection. Both are very effective and we configured the system to send logs to our web page.

Fourteenth stage:

This stage was simple. We installed access point; connect it to the main switch in the pool, install WEP in both, camera and Access point and camera can transmit from outer pool during summer openness.

Fifteenth stage:

We will finish this stage in parallel with the Web page for the pool. Web cameras can be programmed to transmit live stream to FTP server, which can then be the main server for both cameras.

As of controlling such systems, we made considerable effort to be at hand in case of malfunctioning. Many problems can be solved with **VNC**. That is why all our technicians have notebooks and can connect to the systems we have in control over internet from wherever they are. Whether in a hotel at home or in another company. ADSL as well as cable connections are becoming more and more widespread in our country and quality of connection as well as speed satisfactory for such implementations.

»One of the many challenges facing Microsoft administrators is how to manage remote systems in a secure manner? In the world of the UNIX, the answer is quite

simple: using the SSH, protocol is sufficient. Thanks to the SSH, we can manage remote systems not only in the text mode, but we can also run remote X-Window applications by using the protocol tunneling technique. And all of that by using strong cryptography, which protects transmitted data from unauthorized access.

Unfortunately, providing secure remote access to the MS Windows systems is not as easy.... the solutions that offer remote MS Windows management possibilities either don't encrypt transmitted data (like VNC) or their implementation often comes hand in hand with the additional, significant costs.« **Remote Desktop Management Solution for Microsoft** *by* Artur Maj [18]

This article describes perfectly, if I can say, low cost but efficiently encrypted VNC connection to Windows boxes.

In this project, we were forced to evaluate pros and cons with the strong consideration of budget possibilities. Our intention was that the functionality of the system could sustain considerable network load, camera upgrade and reasonable security protection. Investment into security on both sides-physical and IT have to be weighted against possible loses. We have backup system and remote surveillance system in our company. There is a very fast and sufficient signaling and messaging system that can inform personnel, if security is malfunctioning or is somehow broken.

The only problems are ISP outages and congestion of the local internet. We use cable ISP and the system we installed has ADSL connection to Internet.

As we designed scalable system, there is no problem to change critical equipment or add new. Cameras are very reliable with embedded Linux, very secure and easy to maintain.

For IP subnet, we are not using DHCP. For security reason, we prefer fixed static addresses.

Mac filtering was used on the router to restrict access to the system to possible intruders.

When the network was finished, we also disabled broadcasting of the SSID.

On the router side at HQ, we enabled option for logging activity on the router. Log provides us with a log of all incoming and outgoing URLs or IP addresses for the Internet connection. With logging enabled, you can choose to view temporary logs or have a permanent record using the Log viewer software. Temporary logs can be accessed from the Log tab by clicking either the Incoming Access Log or Outgoing Access Log buttons. The Incoming Access Log gives you a log of all the incoming Internet traffic while the Outgoing Access Log lists all the URLs of Internet sites that users on your network have accessed. Of course, port 80 is enabled for web access as well as access to the web camera from the pool. We cannot block the router to be accessed from the wan. This is a considerable flow back as it has to be opened for

the web camera. We will close this gap with stage 15, when we connect the camera stream to the FTP server outside the system.

One of the biggest problems is operating systems on the machines. Company is still using win98SE, which is almost impossible to secure sufficiently, unstable so we have "to wait" for the machines to be replaced and **Linux** or **Windows XP** as operating system installed. Then we will make necessary rearrangement and security measures to sufficiently secure data on the network.

11. Summary of the results:

Considering the security Consolidation:

Pros:

- Provides better protection as everything is on the same system and one can have a coordinated response plan
- Saves money – this was the first and foremost consideration and it paid out
- For the time being, there were no problems on the physical nor IT side of the system, so we can speak about effectiveness of the system

Cons:

- This can be effectively handled only by companies that have personnel with mixed skill sets
- Can, when used and planned improperly, congest the network and pose sustainable threat to operation of it
- Wireless is still "problem" to secure
- Problems can arise with employees due to extra burden and lack of security knowledge and awareness

If we overlook the whole implementation and possible problems, we reached some very interesting conclusions. Psychological attitude and subtle measures have to be observed, when installing new technology and security measures. When dealing with personnel problems unexpected can occur, which are by no means against technology burden. Employees are afraid of being over controlled, have no or very little attitude towards intellectual property, which can be breached and stolen by intruders, which are not "here" and could not be caught by local police. They hardly understand that systems can be broken and used from attackers' world wide, only using one system to attack other systems from it. It is hard to understand that knowledge about security measures is the best return of the investment. This is the problem with management personnel that have to realize how important this part of computerized and connected society is.

Systematically we implemented elementary knowledge as well as security measures and how to react, when something happened. I have to say that company is doing "almost" nothing to educate its people in this field. That is why at the end we made special agreement on servicing the whole system remotely as well as controlling the system there. In parallel, whenever possible, we instruct the personnel and implement security policy measures.

The scalability of the system was well designed. We experienced no problems with the technology applied.

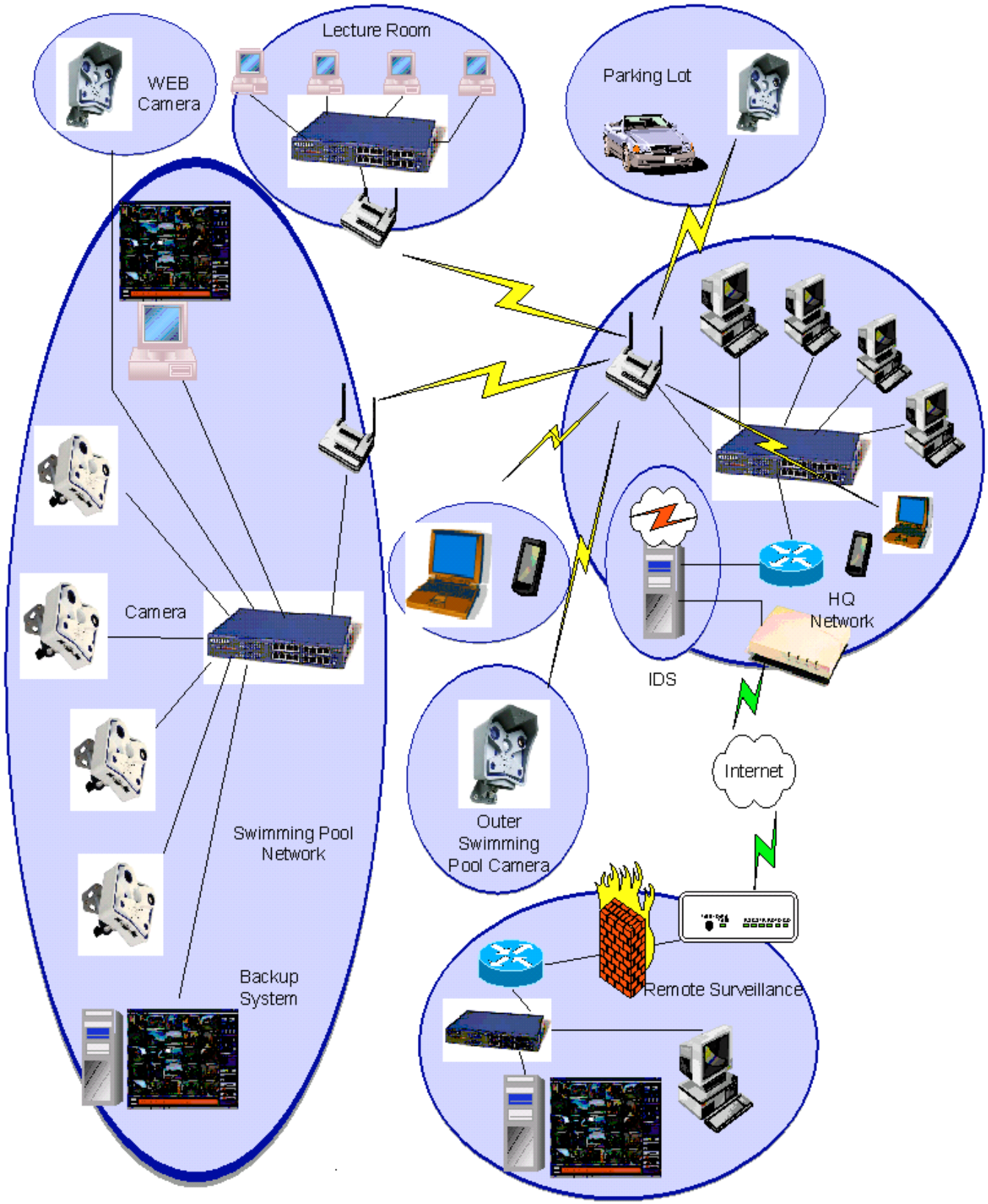
Remote control is very useful. Virtual Private network possibilities can be implemented and are pretty well secured. We have to take into consideration that the cost has to be proportional to the value of the physical valuables protected, as well as data on the system that can, when misused or stolen, pose a threat to the company.

Physical security of the premises and values there is also problematic, when merging it together on the existing network as security measures have to be implemented strictly, if we want the system to function without being off frequently. Merging is not usable or possible to implement everywhere. We have to plan carefully. It is a time-consuming process as well as a heavy burden for people and can have many negative effects. Especially in countries, where awareness about global criminal on IT systems is still neglected as a threat. There are very good systems that can be used in physical security and are implemented, but very bad or none in IT security. Especially in small and middle sized companies. It is the problem of the value, which can easily be "measured" when physical and very hard when that is data. There is of course the biggest problem on Physical site of security measures. Personnel from those companies are not educated in IT field of security problems. They are former police officers, secret agents and retired people, who are used to physical labor and have no knowledge on how computer systems work and at least how to secure them. They can protect property but do not know what to do when the intruder is on the system from the "wild".

Conclusion:

Finally, I would like to state that the entire project was designed, guided, programmed and finalized by myself, although we did have contractors for parts of it. I am still occasionally instructing the personnel about security measures, taking into consideration patience and common sense. SANS Security Essentials are of important guidance for implementing measures and solving possible problems. Of course, the field of combining both systems is rather new and not adequately covered yet. Not only that, but sometimes much more expensive as well as complicated to solve adequately. It is somehow necessary for small and middle companies, especially when budgets are tight. It is important to be in contact with the companies and counsel them as there is not enough awareness, however, tight partnership can solve many problems. There is another very important but many times neglected importance – **psychological knowledge and attitude towards personnel**. You can manage good arrangements with management of the company, but dealing with subordinates can be time consuming and costly when neglected. Not to mention that it can pose a considerable threat to the system and its behavior. It is important that there is a person in company that can be a leader of the project, is able to understand the implementation of the system, and can help considerably when problems arise.

»The best prescription is knowledge.« dr.C.Everett Koop



References:

(1) http://www.csoonline.com/read/090402/beast.html

(2) Corporate computing tries to find a new path
FT.com site, Jun 04, 2003
By Richard Waters
Corporate information systems have become complex, ungainly and difficult to manage. "It's almost as though the technology.

(3) http://www.saic.com/infosec/pdf/physical.pdf

(4) http://www.cert.org/incident_notes/IN-2003-01.html

(5) http://www.kismetwireless.net/

(6) http://www.knoppix.org/

(7) http://www.nessus.org/

(8) http://www.ethereal.com/

(9) http://www.lavasoftusa.com/software/adawareprofessional/

(10) http://www.zonelabs.com/store/content/home.jsp

(11) http://www.uk.research.att.com/vnc/

(12) http://www.netstumbler.com/download.php?op=viewdownload&cid=1&orderby=hitsD

(13) http://www.symantec.com/

(14) http://www.snort.org/

(15) http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp

(16) http://www.createwindow.com/wininfo/regclean.htm

(17) http://blackice.iss.net/

(18) **Remote Desktop Management Solution for Microsoft - http://www.securityfocus.com/infocus/1677**

http://zdnet.com.com/2100-1105-996345.html

http://www.eweek.com/article2/0,3959,1042335,00.asp

http://www.silicon.com/leader/500013/1/3272.html

http://www.silicon.com/news/500013/1/3166.html

http://www.gemplus.com/companyinfo/press/2003/security/OSE15042003.html

http://opensecurityexchange.com/info/faqs.htm

http://www.mobotix.com/mx_english/mx_produkte.htm

http://www.syngress.com/catalog/sg_main.cfm?pid=1525

http://www.axis.com/solutions/video/surveillance/applications.htm

Wireless Demilitarized Zone WDMZ – Enterasys Networks Best practices approach to wlan security.pdf
Wireless Network Security 802.11, Bluetooth™ and Handheld Devices /Tom Karygiannis, Les Owens