Scientific Research Publishing

Journal of Computer and Communications, 2018, 6, 128-153
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Case Study on Security Recommendations for a Global Organization

Devashi Tandon, Pratyush Parimal

Computer Science, Columbia University, New York, USA
Email: dt2450@columbia.edu, pp2485@columbia.edu

How to cite this paper: Tandon, D. and Parimal, P. (2018) A Case Study on Security Recommendations for a Global Organization. *Journal of Computer and Communications*, **6**, 128-153.
https://doi.org/10.4236/jcc.2018.63010

Received: February 9, 2018
Accepted: March 25, 2018
Published: March 28, 2018

Abstract

In today's world, computer networks form an essential part of any organization. They are used not only to communicate information amongst the various parties involved but also to process data and store critical information which is accessible to approved subscribers. Protecting critical data, ensuring confidentiality, and thwarting illegal access are primary concerns for such organizations. This case study presents security recommendations for any such organization, to assist them in defining security policies at various levels of the network infrastructure.

Keywords

Networking, Network Infrastructure, Security, Network Security, Security Framework, Access Policies, Threat Prevention, Intrusion Detection, Firewall, VPN Security, Network Attacks, Hacking

1. Introduction

In order to present the security considerations required in a corporate setup, we created a fictitious company by the name of *MediSecure* Corporation and tried to give it a real profile. The profile of *MediSecure* Corporation is as follows.

MediSecure Corporation (referred to as our company or the company hereon) is headquartered in the US with 20 satellite locations worldwide. Manufacturing takes place in all locations, while R & D is limited to US and some satellite locations. Satellite locations are constantly in contact with the headquarters for communication and exchange of data, ideas and other forms of intellectual property. The communication networks have to run 24 × 7 × 365 to support the needs of all offices.

Main Headquarters house the core infrastructure, which is connected to the

satellite locations. Each location has an internal LAN, and the LANs from different satellite locations are connected by a private WAN.

2. Portfolio of the Company

The various divisions vis-à-vis the computer networks and their functions in *our company* are described in Figure 1. The profile of each division, mentioned in Figure 1 is described below:

2.1. Research Center

Most pharmaceutical companies invest heavily in research, so they have advanced research facilities, which contain sensitive information that needs to be protected from data breach. Confidential data may include intellectual property pertaining to their on-going research, information about proprietary drugs, procedures regarding testing and trials and other procedures, all of which needs to be protected.

2.2. Manufacturing Sites

Our company specializes in mass production of drugs/healthcare products for millions of customers. The orders can be placed online via public website and also offline via phone or paper contracts. Shipments are delivered to customers, from all locations. As manufacturing is automated, the sites consist of many digitally controlled production devices, operated locally or remotely, as well as a large number of monitoring and controlling stations for ensuring quality.

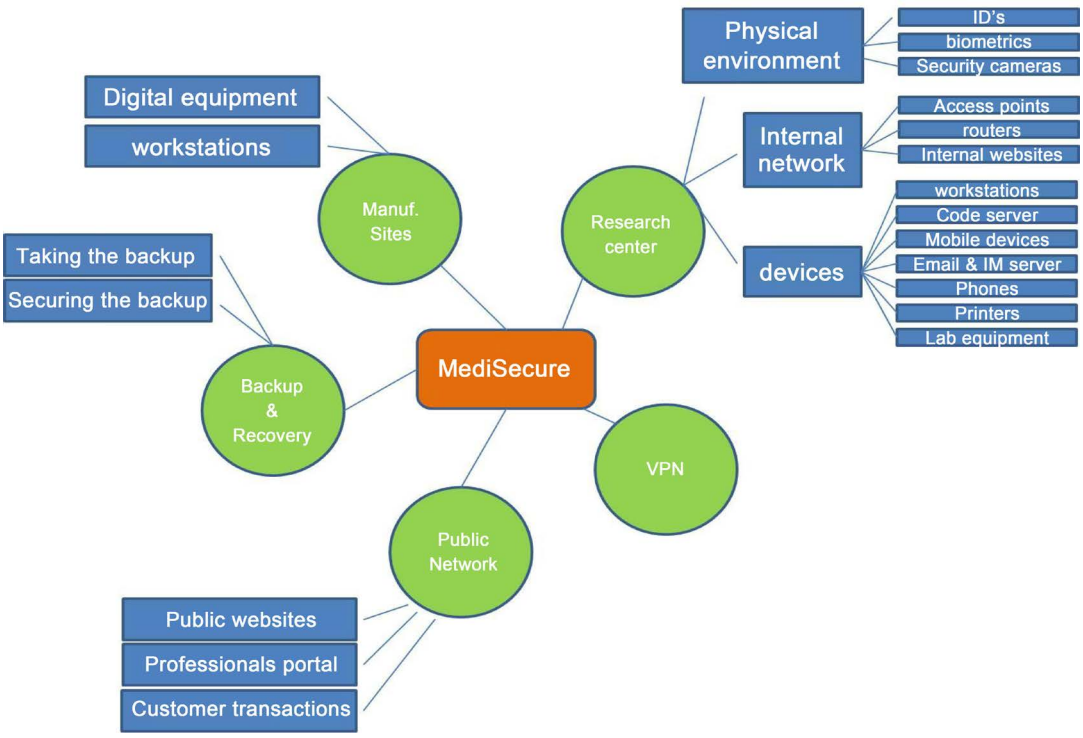

Figure 1. Network model of the company.

2.3. Public Facing Network

The public facing network consists of a public website through which people can learn about the company. There is a login based secure site for healthcare professionals, which provides health care professionals a secure way to interact with the company resources/professionals. They get to know about new medicines/ vaccines etc. and their test reports about efficacy to help them decide which medicines to prescribe. The company also benefits from these interactions by understanding their requirements. Another secure login-based website helps pharmacists who buy medicine from the company. They can securely carry out transactions and place orders online.

2.4. Backup and Disaster-Recovery Management

The company portfolio requires the company to ensure proper data backup so that it can be re-instated in times of any kind of disaster. Scheduled backups are necessary and required frequently enough to ensure minimum loss in case of retrieval. Backup is an extremely sensitive activity and needs to be carried out securely to avoid any breaches during backup.

2.5. External Access and VPN

The company provides secure VPN access to its employees to access its internal network from an outside network.

3. Security Recommendations for the Company

In order to arrive at the recommendations for the company, we studied articles specifically targeting pharmaceutical sectors [1] [2] [3] [4] and general methods to develop security policies for protecting corporate assets [5]. We have broken down the divisions, going down to the device level granularity. This level of granularity helps in making suggestions which (although relevant to the considered portfolio) are not restricted to a particular company portfolio and can be applied to other portfolio's which use a similar set of devices/assets/resources/ in their systems.

3.1. Research Center

From a security perspective, the R & D center can be thought of as consisting of different devices, the network which connects them, and the people involved from end to end. Let's take a look at these in turn.

Devices can be categorized into the following:

3.1.1. Workstations

Laptops & Desktops used by employees require host-level security. These may further contain peripherals like network card, digital camera, microphone etc. Along with the laptop/desktop, the peripherals need to be protected too. If attackers gain access to the microphones/cameras of the desktop/laptop he could

potentially record conversations which might give them company confidential information. Updated host-based security software (recommended later) should be installed on workstations. Patches should be pushed by the company network regularly, or as and when a vulnerability is discovered. The patch application process should be such that the workstations get updated within a deadline of one day and employees are informed through pop-ups if reboot is required. Besides this, the growing trend is to support laptops as workstations due to their ease of mobility. Hence these devices must also be protected from getting stolen [6]. Laptops may be a soft target for stealing confidential data. Hence data encryption should be enabled for all the data residing in the hard-disks of laptops. When the laptop boots it should ask for a PIN which only the owner employee is aware of. This way even if the laptop is stolen, confidential data can be protected.

3.1.2. Code Server

The code server would be holding the data for the research (like chemical reaction simulations) being undertaken at various facilities. First level of security is to restrict access only to employees of research units who work on this data. Second level of security is to back up the data in code servers (discussed in detail later) regularly. Third level of security is to station the servers separately in a secure and monitored network. There should be a network firewall and IDS monitoring the traffic to the servers. The fourth level of security is to physically station the servers in a restricted area which is well monitored by security cameras and only the administrators should have access to that area.

3.1.3. Mobile Devices

Mobile devices aid employee productivity by allowing them to connect to the internal network through Wi-Fi from any location in the company. They can keep track of their simulations etc. at their convenience from anywhere within the facility. Since mobile devices access multiple wireless networks inside and outside the company, some of which are unsecured, they are more prone to getting infected compared to other devices. More and more rootkits are surfacing which target mobile devices specifically [7]. Hence there should be a well-defined security policy on what is allowed on the wireless networks. Highly critical data like code access should not be allowed through these devices. Also, the wireless network should be configured in such a way that it only allows the devices which have the VPN software (discussed later) installed on the phones. The phones should also have the company recommended anti-virus software installed on them. The VPN network server residing behind the access points should check the presence of these softwares on the devices before granting access to the network. If the mobile device doesn't meet the requirements it should be denied access to the network. To allow access a registration policy should be adopted. This means that only devices registered with the network may be allowed to access it. This could be done by one-time registration of the IMEI number and then reading and matching the number from the database, every time a device

tries to connect to the Wi-Fi. This wouldn't cause any inconvenience to the employees since they don't change the equipment very often and would probably be using the same phone most of the time.

3.1.4. Email & IM Server (Spam, Malware)

Emails and IMs bound to be one of the primary forms of communication as offices span over different geographical locations. Also, since emails are a documentary evidence of the communication, they might be preferred over other forms in certain contexts. Emails reside on the email server, and any security breach of the server can leak confidential information. A link clicked in malicious emails by an unnoticing employee, may result in a drive by download malware getting downloaded on their machines. This may then spread across machines in the network and breach the security to carry out attacks. An employee could receive malicious emails which may look genuine as an internal information broadcast asking them to change their password. By acting on it they may leak their username/password which may then be used to gain access to the internal network by the hackers. Hence it is important to have a good spam filter and an anti-virus on the email server which scans all attachments before downloading them on the client machine to save employees from getting phished. Suspected emails should be blocked and investigated before passing on to an employee, especially when they are from an outside network. Advanced file inspections as part of antivirus are necessary so that attachments are scanned from its contents. Recommendations on anti-virus and spam scanner are discussed later.

3.1.5. Network/IP Phones

Telephone network helps in managing communication across the various centers distributed globally. It helps in conducting conference calls for interacting with other teams. These conference calls may be used to communicate confidential information and thus it is necessary that they be secured like any other digital communication. Since *our company* uses IP phones for all its phone communication, it is important that the software on the phones be protected. Phones are forms of embedded devices with limited memory, processing power and software. They don't have any anti-virus or monitoring software installed in them. Hence, they can be soft targets. Upgrade of firmware on the phones is not a regular activity and may happen rarely. Hence, we recommend that the phones have a provision to hard lock the firmware upgrade, and the unlocking/upgrade be done only when an upgrade is absolutely essential. This will protect the phones from any malicious code getting installed on them. Also, the upgrades should be carried out through a secure network by the administrators, which should require additional login credentials to prevent employees from unlocking the phone and triggering upgrades (insider threat).

3.1.6. Printers

Our company's premises have a large network of printers with each facility hav-

ing multiple printers stationed on every floor of the premises. The investment on the printers has been done because the employees would need to take print-outs of various documents to assist in their daily work. The documents may contain company confidential information and thus need to be secured. Besides this, most of the printers are multi-functional as they can carry out printing, copying and scanning of documents. Since the scanner needs to save the digital copy of the data, the printers have a small hard disk and support emailing. If not well protected they could be used to carry out attacks like sending spam through the email facility of printers, similar to the refrigerator attacks [8] which was carried out recently. Again, similar to phones, the software upgrades on the printers should be hard-locked. There should be a software installed on the printers to purge the data from the hard-disk once it has been retrieved by the user/employee so that there are no traces of it. Before decommissioning a printer, all the information must be deleted, hard-disk removed and cleaned. There should be well defined processes for all these activities so that any new administrator also knows the process to follow.

3.1.7. Lab Equipment

There may be various lab equipment used to carry out testing of drugs and in carrying out research. Some examples include equipment like centrifuges, chromatography testing equipment, analyzers and software which may be used to analyze the results from the equipment. To secure them, they should not be connected to the network. Many equipment may be digitally controlled but need not be remotely controlled. We recommend that for security reasons they should not be network operated/controlled or monitored. Individual workstations which are offline should be connected to them if needed. Also, the lab premises should be well secured with restricted access and monitored via cameras.

Internal network equipment can be categorized into the following:

3.1.8. Access Points

Wireless networks may be a part of the entire facility, so that the network is easily accessible from any location within the company. They can also be an easy medium to gain access to the internal network, especially if the wireless network is not well protected. To address this, it should be ensured that all access points should be password protected, and default password must be changed to something secure. They should have access control lists that allow only registered devices.

3.1.9. Routers

Routers form the backbone of wired network. There would be plenty of them deployed within the company to build a large internal network connecting all the departments at a particular facility. Unsecure routers can be used to carry out attacks and infiltrate the network. Routers are also involved in routing advertisements using OSPF and BGP which are vulnerable to a separate class of attacks which involve compromising a router and sending false route advertise-

ments to adjacent ones, in an attempt to route traffic towards the malicious routers. To make routers secure, the first thing to keep in mind is that any default passwords must be changed to something strong. The routers are often advanced enough to support fine-grained control or even firewalling, which should be properly utilized to disable any form of traffic from an unlikely source. In order to address the OSPF and BGP vulnerabilities, it is a good idea to have a PKI system for routers so that every route advertisement can be signed, and the source of every route advertisement is known and authenticated. This scheme has limitations to the effect that it involves a complex certificate management system which can scale to a large number for a big firm. Also, it provides no security against falsely configured routers, and hence requires additional monitoring stations to verify that the routes are topologically correct.

3.1.10. Internal Websites

Companies usually don't care about internal website security compared to external ones. We suggest that same level of security should be applied to internal websites too since they can be hosting confidential data, and/or the servers may be used to gain access to other network resources.

Physical Security can be categorized into the following:

3.1.11. IDs

Access to the facilities is usually managed by RFID cards. Since the access is digital, it needs to be well protected. Unauthorized access would cause a security breach which may lead to damage to the company. Security access should be of different levels *i.e.* only required personnel have access to any of the restricted areas. In order to avoid spoofing the ID cards, the employees can each have a key-pair registered with the company, and the data on the ID card can be signed using their private key for authentication. This also ensures that once registered, the same card will work at any office within the company.

3.1.12. Biometrics

Biometrics could be used to further enhance the level of security provided by ID card access. This additional level of security would be useful in protecting the restricted areas within the company premises. But biometrics come with their own weaknesses, e.g. facial recognition can be fooled, or it may read incorrect data if face is altered naturally, or voice recognition can fail in case of an illness. Similarly, fingerprints can be spoofed using gels, etc. The solution is to use biometrics under supervision so that spoofing using physical means can be avoided. Also, biometrics should be used in conjunction with another identifier like names so that matching time is reduced, instead of using the digitized biometric itself for a lookup.

3.1.13. Security Cameras

Security cameras stationed at all the critical places can act as deterrent to people trying to sniff. Also, they can provide critical evidence in case there is a break-in

and hence the camera feeds should be well secured. There should be an additional security staff managing the security at the facilities. Security cameras should be installed in tandem so that there are no blind spots. Access to camera feed should be restricted, and the videos should be backed up in addition to being saved. Access to those tapes can be restricted based on the biometrics for the security personnel.

3.2. Manufacturing Sites

3.2.1. Digitally Controlled Equipment

There would be mechanical equipment controlled digitally to manufacture and package medicines. An attack on such equipment could potentially turn the company bankrupt. This is because if for example the manufacturing equipment are compromised to print wrong label on the medicines, it could affect people's lives, the company could be sued and may have to close down. There can be other similar attacks like contaminating a particular medicine with chemicals being used to manufacture other medicines and so on. Hence very strict security policy measures are required to protect such equipment. These measures are discussed in detail while discussing impact of *Stuxnet* and how to prevent it from disrupting manufacturing sites and their digitally controlled equipment.

3.2.2. Workstations

Being an advanced facility, each manufacturing site may have multiple workstations for employees and personnel, as well as multiple monitoring / controlling stations to regulate operations. It is important for the company to ensure that these workstations are not compromised. All of the measures for workstations discussed in workstations at research centers apply here as well. However, there are some additional measures that need to be taken into account which are discussed while discussing impact of *Stuxnet*.

3.3. Public Facing Network

Since public website is accessible from anywhere, it's also a highly sought-after target for attackers. There is no need to be part of the internal network to attack the servers. The attacks on web-servers are both in form of traditional (generic) attacks as well as advanced ones targeted towards specific web-servers [9]. Some of the known forms are explained below:

- SQL injection attacks: Insertion of malicious SQL statements into an entry field for execution. This is mostly used against data driven applications, which may be relevant to *our company* as it has various databases to maintain for customer-data, credentials, company-data, etc. If the user-input is not strongly validated, unexpected SQL code may be embedded into it, and may get executed in this manner.
- URL interpretation attacks: This attack is possible in situations where an attacker can adjust the parameters of a request. The syntax of the URL is maintained, but its semantic meaning is altered. For example, changing the

email address parameter in the GET request of a password-reset page.

- input validation and buffer overflow attacks: This is a very common type of attack against web servers, which is made possible when the scripts/programs handling the data entered by the user are not written securely, and don't perform sanitization or bounds checking, allowing execution of malicious code.
- cross site scripting: This particular vulnerability allows attackers to inject client-side scripts into web pages. It may also be used to bypass access controls. It typically uses known-vulnerabilities in web applications, their servers, or plugins.
- attacks on the medical professionals' portal: Communication on this portal requires login credentials, which make it a good target for attackers. Leakage of this data can enable attackers to listen in on confidential discussions or to masquerade as another user.
- attacks on the customer transaction site: Since this operation has a financial facet, it is also an attractive target for attackers. Needless to say, a successful compromise of this subsystem can lead to theft of financial details of users, which has also been seen in many recent attacks like the one on Sony PlayStation server which lead to breach of data as well as loss of credit card information putting customers at risk [10].

The attacks related to inputs and code injection can be handled by proper input validation and sanitization before passing on the input to the backend scripts or databases. Server application(s) should start as non-privileged user, so it can't compromise protected files. Scripts should be allowed only in certain directories which can be maintained easily, and *suEXEC* (Apache Web Server) or similar feature should be used to switch ID's before running scripts. Proper patches must be applied to the server software so that it remains bug-free. Access to server must be over TLS, with the key stored in encrypted form, readable only by the administrator.

For the professionals' portal, login must be done using credentials stored securely in a database. This particular portal can preferably be hosted on a separate server. Firewalls should be in place to ensure that there is no way to contact the server bypassing security filtering layers. Thus, the company should have a DMZ-minded layer of firewalls to ensure network isolation.

For the customer's financial transactions, the traffic should be over TLS and authenticated. It is best to keep the server hosted on a separate machine so that the compromise of any other service should not weaken the security of this part. Help of a 3rd-party vendor can also be taken for this. A good example is OAUTH.

3.4. Backup and Disaster-Recovery Management

In the unfortunate event of a complete or partial data loss, it's important to have a backup from where the last known good state can be re-instated. From the

point of view of security, it mainly involves looking at the following two processes:

3.4.1. Taking the Backup

Following parameters need to be taken care of while backing up date:

- Content to be backed up.
- Source to get data from.
- Frequency of the backup operation.
- Location of storage (backup server).
- Duration for which the backup has to be kept.

Since backing up involves sending data over the network to a backup server, the operation is vulnerable to network attacks and vulnerability in backup mechanism may make it a soft target for attacks. As a counter-measure, the company can use certificate-based encryption for securing the backup data during transit. Validation of the backup server ensures that the data is being backed up to an authentic server, and not leaked to some other location. Validation of the client certificate ensures that the source of the data is genuine and from within the company and doesn't contain anything malicious.

Backup data is likely to have a large size, and the longer it stays in transit, the more vulnerable it gets. In order to minimize the transfer duration, it might be a good idea to compress the backup before sending. Less sensitive/important data may be backed up at lower frequencies to reduce transfers. To further minimize the transit operation, each location can have its own backup server, backing up independently.

It makes more sense to have backup servers in the same location where R & D takes place, instead of routing it over to the central headquarters (which may be done at a much lower frequency). Blind backup which involves backing up everything indiscriminately should be avoided. Priority should be given to more sensitive data and data which changes frequently like codebases and research data. Some data changes are in-frequent like databases for employees and customer details, etc. In order to maintain consistency, the data may be updated at the back-up node along-with the primary node whenever there is an update to the database. This would ensure consistency on the back-up node and also avoid the need to back-up such data. Incremental back-ups could be adopted as a general measure. However, backups should be taken frequently enough, either daily or semi-weekly, to be minimize data loss in case of an eventuality. Moreover, there should be policy which rotates the validity of the backup, before the expiry of which, a new backup must be taken to replace the old one.

3.4.2. Securing the Backup

It is just as important to secure the backup, as securing the live servers. Stealing the backup from central back-up servers gives attackers more advantage as then there's no need for stealing the same data individually from their respective sources (which is more difficult). Security of the backup is essentially a case of

host-based security and involves mostly the same parameters. Apart from being compressed, the backup data must be encrypted even in stored form. The individual subparts of the backup may be encrypted using separate keys (for each source) so that the compromise of a particular key doesn't put the security of the whole backup at risk. The backup server must have a good host-based IDS which can monitor any operation being performed on the backup files within the server. Physical security of backup server should be ensured too and any physical access to the servers must be allowed only when absolutely necessary and restricted using biometrics.

Backed up data has an advantage over live data. Since backups are stored more frequently than being retrieved, a back-up versioning system could be used, with older backups getting removed after a certain period of time. Even if reading from backups (which is rare and only in case of damage to live data) is extremely slow due to highest levels of encryption, it can be adopted as an acceptable trade-off.

When a backup server gets decommissioned, there must be a policy in place which mandates the erasure of all data on the server before disposing off the machine.

3.5. External Access via VPN

Access to VPN allows employees access to company's secure network through a VPN tunnel. It is used to connect to the research center and the manufacturing sites. Being run over an unsecure public network, it makes VPN communication an attractive target for attackers. Issues compromising VPN tunnel:

- VPN fingerprinting: while not an attack in itself, it does give the attacker useful information by identifying the type, version, model, etc. of the device.
- Insecure storage of credentials by clients: storing the user credentials in unencrypted form, or using weak forms, whether in the memory or the registry.
- Username Enumeration: usage of pre-shared keys enables this kind of attack.
- Offline Password Cracking: This type of attack is made possible when a valid username is obtained using the previous vulnerability, and the hash of the username can be obtained from the VPN server to launch an offline password cracking attack.

The issue of username enumeration is quite new and can be addressed from the vendor's side. Addressing this will take care of the password-cracking attack too. In order to address the remaining threats, it's imperative to use the strongest possible encryption methods, like EAP-TLS and IPsec. Usage of two-factor authentication products like RSA SecurID is also recommended. VPN access should be made available to personnel with a valid business reason. A strong password policy should be implemented and enforced, which is different from the one used in internal networks, so that compromised credentials only allow access to what is available through VPN. The limitation with this security is that the remote user may himself be compromised in the first place, which can then

render some of these protections less effective. A safe approach would be to ensure that the remote users themselves have strong antivirus, antispam and personal firewall, and they must be required to use it. One method is to allow only company issued devices for VPN access. The devices can be validated through the serial keys of the hardware. Also, the system could be checked for meeting the security requirements every time a user logs in, before granting access to the network.

3.6. Additional Class of Attacks

There are two more classes of attacks which apply to almost all the divisions described above. We chose to address them separately, as they apply to multiple scenarios, and are quite important from that perspective. They can be listed as follows:

3.6.1. Insider Attacks

We mention insider attacks [11] separately, as they apply to almost all aspects of the company in terms of security. The following observations were notable:

- It is important to identify the several most important entities that need to be protected within the company and secure them with the highest priority. This doesn't mean just encryption, but also restriction on access, and rigorous monitoring of who interacts with it, and under what circumstances. The circumstances can be used as a basis for a set of policies that clearly outline when the access is allowed. Physical security of assets is also one aspect which should not be ignored at any cost.
- The company should be extra careful in times of someone's resignation or employment termination, especially if they're from a high post. Suspicious behavior must be brought to notice.
- Centralized logging tools can be used to track all data exfiltration. Proper auditing should be enforced so that no operation on sensitive data goes unmonitored.
- Access to sensitive data should be allowed on a need-to-know basis only, and privileges must be rescinded once the project/operation is done. An employee must be asked to submit a valid, signed (digitally or otherwise) reason for accessing sensitive data.
- It should be possible to remotely erase a disk on a smartphone or laptop in case of theft.
- There should be a proper training course based on general security guidelines and best practices which trains users about the importance of strong password policies, proper emailing protocol for different situations and browsing recommendations, sharing of information with outsiders or colleagues, etc.

3.6.2. Peripherals and Removable Devices

Devices like USB sticks, flash drives, external hard disks, smart cards, and mobile phones are examples of set of entities which are very effective as tools for at-

tackers. In many cases, they turn out to be either the starting or ending point of a successful attacks, involving mostly theft of data by carrying it off on one of these. Since they can be used with a variety of devices, in different environments and without need of prior installation of any software, they prove to be an effective out-of-band channel for attacks. They are also harder to track because of their removable nature and the human factor involved. We chose to mention them separately, as they apply to all of the divisions of the company as presented above.

We recommend the following guidelines for dealing with them:

- In general, it's best to avoid the use of removable devices as much as possible.
- If the use of removable devices cannot be avoided, it's best to have them registered so that they can be tracked. Un-registered or ad-hoc devices must be rejected.
- Some removable devices like USB sticks can have native password protection. It's recommended to use those, to protect data against theft.
- Workstations, and any other devices which have USB ports or CD trays, must have the auto play option permanently disabled.
- The antivirus software on the host device must be configured to scan the removable device as soon as it's attached.
- The HIDS must monitor ALL data travelling to/from a removable device, even if it's registered.
- It may be possible to encrypt data if it's copied out to one of these removable devices.
- For mobile phones, registration should be recommended, and the user must be required to have sufficient protective measures like antivirus, GPS locators, etc. on the phone. We also discussed mobile phone registration earlier while discussing threats on the research center devices.

The limitation of the above strategies is that they might turn out to be too cumbersome to implement and carry out in a large company. The tradeoff of security vs usability states that if the users tend to face a lot of delays or difficulties in working with these restrictions, they may tend to bypass them. Hence, employees should be trained against the harmful effects of such negligence.

4. Measurement of Security Posture

Measurement of security posture refers to the steps the company can take to measure how secure they are at any given point in time. It can be interpreted in a systematic way if we look at different things the company can look at, in order to determine the state of their security.

These "things" can include the security alarms generated by their:

- host-monitoring systems
- network monitoring systems
- physical security mechanisms

The best way to look at these alarms is to use some kind of an IDS visualiza-

tion tool. Since the company has a distributed architecture containing many locations, each having many machines, all connected through LAN's and WAN's, a good example for visualization can be *IDSradar* [12] tool. The tool has provisions to visually depict each node from each location and their network connections within a single representation, which gives a holistic idea of what is going on with the company in terms of security threats.

The following properties of *IDSradar* can prove very helpful in obtaining this representation:

- servers and workstations—nodes are shown as arranged in circles indicating a common corporate network. The bigger nodes are those with high priority. Locations are ordered by IP address. This can be used to take a look at any of the nodes in the whole network, and to see any security-relevant statistics.
- alert types—each alert type is shown in a separate color, and the width of each arc is corresponding to its percentage. This gives a kind of visually proportionate size to the importance of an attack.
- timeline & histogram—time is depicted using animation, and the histograms below each alert type are drawn clockwise along the alert-type arc in real time. They're updated every few minutes. This can help the company keep track of attacks/alerts over time, and can be used to figure out a pattern, if any exists.
- attack correlation—triangles are used to connect source IP, destination IP and the top of the bar of histogram below the alert type, in the current time span. The nodes in an alert are highlighted. This can be especially helpful in case the hosts/networks in different physical locations are being targeted systematically. The correlation can help filter out random attacks from deliberately targeted ones.
- interactive design—interactive filtering is provided in the form of clicks on hosts, servers, alerts types, etc. as well the ability to zoom-in/out, play, stop, etc. Detailed information about any entity can be seen by mouse-hover. This provides information in various ways, and being visual, it's easy to be interacted with by personnel who may not know about the setup or commands or similar technicalities of a particular system.

Apart from visualization, the company can consolidate the security alarms and reports from different locations and try to use behavior-based learning methods to glean patterns or statistics out of the reports. The statistics can be collected based on location, time, type of attack, or any relevant metric which can help in detecting any kind of trend in the attacks. If so, the company can take steps to address that particular concern proactively. This methodology of pro-active threat assessment will ensure that the companies resources are secure, and breaches can be avoided before they take place.

5. Selecting a Security Product

Table 1 gives an example of a set of generic security features and a list of evaluation

Table 1. Criteria for comparing security product from different vendors [13].

Criterion	Evaluation Elements
Data	Type of Data, Amount of Data, Origin of Data
Detection Range	Accuracy, Completeness, Known Attacks, Masquerade Attacks, Denial of Service, Malicious Use, Leakage, Attempted Break-Ins, Penetration of Security Control Systems
Resources	Overhead
Network	Network based or not, Portability
System Architecture	Methods of Detection, Real-time Operation, Human Supervision, Manipulation Level, Behavior Modeling, Attack Resistance
Alarm	Countermeasure Activities, Detection Time
System Change	User Behavior, Sensitivity Levels, Expanding System, Knowledge Base

elements on which products from different vendors could be compared. This can be taken as a baseline. There is multiple criterion which must be considered before selecting a security product to be installed in the company. Each criterion should be matched by the network requirements of the company and whether any of those criteria would act as bottleneck in case the network resources are expanded. Also, the projected network growth and pricing of security products must be considered before purchasing/deploying a product to ensure least security cost to company. Other parameters include:

- Network speed supported by the device when the security features are enabled.
- Number of concurrent sessions supported.
- Inter-operability with other vendor security appliances already installed in the network or the ones which would be installed.
- Inter-operability with other TYPES of appliances. For example, inter-operability of vendor X network IDS with vendor Y Host IDS.
- Support of required features.

A list of security features (not exhaustive but informative) provided by various security devices in the market:

(They can be either at the host level or the network level or both)

- Firewall
- Antivirus
- Anti-Spam
- Signature based Intrusion Detection
- URL Filtering
- Application Identification
- Protocol Anomaly Detection
- Traffic Anomaly Detection
- IP Spoofing Detection
- *DoS* Detection
- *AppTrack*

- *AppFirewall*
- *AppQoS*
- *AppDoS*
- Application Signatures
- SSL Inspection
- Stateful Signature Based Inspection
- Protocol Decodes
- Traffic Normalization
- Zero Day Protection
- Recommended Policies
- Active/Active Traffic Monitoring
- Packet Capture

In order to arrive at this list, we referred to Juniper Data Sheet [14], Cisco Data Sheet [15], McAfee Data Sheet [16], Palo Alto Networks Data Sheet [17] and some other articles [13] [18] [19] [20] [21] on product comparisons. [22] is an informative resource on Intrusion Detection Technologies and [23] can be referred to learn more about anomaly-based Intrusion Detection Systems.

As attackers get more and more sophisticated, even anti-viruses (specialized to thwart viruses/malware/spyware) are becoming ineffective in dealing with the latest threats [24]. Hence, a package of products functioning and collaborating at different levels must be used.

There are some organizations like NSS Labs which evaluate IDS and other security products from different vendors and publish their report annually. Such third-party reports may be more reliable in reporting actual figures than the company data sheets which usually report the best-case figures to beat the competition. These reports are available for a subscription [25]. We recommend relying on at-least one such report before finalizing on the product.

6. Similar Threats Faced by Others

We looked at some threats faced by some other companies/organizations. There were quite a few of them related to healthcare industries, which we enumerate first, followed by some other relevant examples:

- **Utah Department of Health, March 2012**—a breach caused by weak password policy (default password wasn't changed) on a network server exposed protected information of 780,000 individuals, which included their Social Security numbers.

This is a classic case of negligence/misconfiguration brought about due to ignorance of user training. Enforcement of proper regulations (like password format restrictions in the company) would have avoided this easily.

- **Emory Healthcare, Georgia, April 2012**—lost 10 backup disks containing information more than 300,000 patient records, two-thirds of which contained Social Security numbers.

This strengthens our claim made earlier in the document stressing the security of the backups. In fact, backups need more security as they may contain data

from many divisions and must be secured with more care.

- **South Carolina's Department of Health and Human Services, February 2012**—about 228,000 patient files were compromised after former *Medicaid* employee *Christopher Lykes* illegally transferred 17 Excel spreadsheets with social security numbers and other personal information to his personal Yahoo account.

This is a good example of insider threats, resulting when a firm makes the mistake of trusting any or all entities within its physical/network boundaries, and fails to monitor their activities. To avoid/detect these kind of attacks, we think it's imperative to track all kinds of operations performed on sensitive documents or machines. This may impose a heavy burden on the monitoring tool as the number of such entities (which are potentially sensitive and should be monitored) can be very large in a big company. The company can then try to compartmentalize documents using security levels and monitor the ones at the highest levels only.

- ***Stuxnet*, Iran**—*Stuxnet* was propagated to a high security facility with only PLCs through a USB drive inserted in devices/workstations outside the high security facility. *Stuxnet* works in the following way: After infecting a less secure workstation (through a USB drive), it propagates to other networked computers and then scans for specific software manufactured by Siemens for controlling a PLC. If the computer is found with the software AND it is controlling the PLC, it introduces the rootkit by infecting both the software and the PL. Otherwise it becomes dormant on the system. Once both the software and PLC are infected, it can send unexpected commands to the PLC while the software still reports normal operation. The design of networks which were infected by *Stuxnet* are similar in nature to the manufacturing facility of *our company*. Hence it is a good idea to learn from the way *Stuxnet* propagates and operates, while designing the security systems at *our company*. First of all, it is important to highlight that traditional security methods including anti-virus and IDP would not have helped prevent *Stuxnet* since it exploited 0-day vulnerabilities and there were no signatures available for this attack before it was discovered.

The above examples cover a good variety of threats like weak protection policies, insufficient protection of backups, insider attacks which are all witnesses to the fact that healthcare industry requires proper security no less than any other industry. It also covers highly targeted attacks using malware like *Stuxnet*, which are relevant for healthcare firms which are involved in mass production of drugs using specialized devices and sophisticated machinery.

7. Impact of Snowden's Disclosures about NSA

The Snowden's disclosures on NSA [26] reveal a nexus of international agencies having an elaborate network of global surveillance. Many intelligence agencies like NSA are spying on the citizens of their country by spying on the digital

footprints of people through emails/phone conversations and so on. The agencies are able to spy on individuals with relatively simple methods using various kinds of tools. This is alarming because this highlights that other agencies could use similar tools to spy on their targets. For example, a particular pharmaceutical company could develop means of spying on *our company* to carry out an espionage and steal critical information from the company's network. With Advanced Persistent Threats, it is possible to carry out such an espionage for a long period of time before it even gets detected. So, such threats are not a one-time affair and can last over long periods of time from months to years.

Snowden's disclosures also highlight some of the tools which can be used to carry out targeted attacks. Some of the tools are listed below:

7.1. Computer Implants

1) **Sparrow II**: A small device that could be implanted at a strategic location to spy on the wireless networks and collect data.

2) **Firewalk**: It is capable of filtering and regressing (outputting) network traffic over a custom RF link and can inject traffic into the network as commanded.

3) **SWAP**: Can be used to exploit motherboard BIOS before the operating system loads

4) **CottonMouth I, II, III**: USB Implant that provides a wireless bridge into a target network and also the capability to load exploit software on target PCs in the target network.

Likewise, there are about 18 hardware/software tools listed as part of the disclosure which can be used as computer implants to spy on the network/data. It is possible that other organizations may be able to develop such tools. Hence it is important to be aware of their presence and take action to prevent their use in spying on the network.

Since all the above equipment is a computer implant, it would need to be physically implanted at a strategic location within the company premises. It cannot be done remotely and thus needs an insider to plant the devices. Refer the section on insider threats on strategies to mitigate them.

7.2. Server Implants and Firewall Implants

The Snowden disclosure lists seven tools which include *Ironchef*, *DeityBounce*, *JetPlow*, *Halluxwater*, *FeedTrough*, *GourmetTrough* and *SouffleTrough*.

Many such software implants can be used to install backdoors in servers and firewalls, which can be used to leak data from the networks. This highlights the importance of protecting servers and firewalls from such tools. There should be a policy to protect the firewalls themselves, especially when updating their operating system, software, changing the firewall rules, or in general carrying out any management tasks on the devices.

7.3. Covert Listening Devices

Another set of devices listed in the disclosures are the covert listening devices

like *LoudAuto*, *NightWatch*, *CTX*4000, *PhotoAnglo*, *Tawdryyard*. These devices can be used to listen to wireless data. There may be many similar devices which could be used to pry on the wireless networks within *our company*. Hence it is important to use wireless routers whose range is limited to the company premises and don't have very high ranges beyond the premises which cannot be monitored. It is better to use multiple wireless routers with small ranges rather than using high range routers which may have sufficient range making it possible to listen to their traffic beyond the company premises.

7.4. Mobile Phone Implants

Mobile Phone implants like *Picasso*, *Genesis*, *Crossbeam*, *Candygram*, *DropoutJeep*, *GopherSet* highlight that mobile phones can be compromised either during manufacturing phase or during their operation. It is also possible that certain employees might bring in modified hardware devices to help in spying on the networks. Otherwise, a mobile phone user could be a target of an attack which may lead to software like *DropoutJeep* getting installed in their phone. This will compromise the privacy of the user and may also leak company information exchanged through conference calls, emails, SMS messages through the phone. It is worth noting that such devices are used at multiple networks (public hot-spot) and thus more susceptible to attacks unless the user is careful in using them. Hence it is important for the company to highlight best-practices to employees regularly, so that they are careful in using their devices, and opening links in emails etc. Also, it is important to restrict the data access which is available through these wireless devices on the company's wireless network.

8. Measures to Avoid Sophisticated Attacks like Stuxnet

Our recommendations are as follows:

- **Isolate the network** of the manufacturing units from the internal LAN of the company. This would not have prevented *Stuxnet* from spreading (it used USB to inject itself initially). However, it is still an important practice to follow
- The computer systems connected to the manufacturing units and machines should have very limited connectivity to the outside world. Security measures should be built in to provide additional credentials for connecting USB drives/CD-ROM etc. to the systems. This will prevent anyone who has operational access to the systems from trying to modify it.
- Modifying the firmware on the manufacturing units should not be easy. It should have multiple levels of security. Even after downloading the firmware on the computer systems from (say) USB drive, there should be additional privileges required to upgrade the firmware. This should be through a specific set of computers placed in a high security zone which are NOT used for the operational activities of the units.
- There should be mandatory integrity checks carried out on the new version

of firmware before it is passed for installation. If the integrity checks fail, the systems used for upgrading should lock out. The integrity checks should be carried out on a separate system/network than the one used for upgrading. Some experts recommend using cloud services to carry out the integrity checks which can be considered too.

- To ensure tightest security, firmware upgrades for mechanical units should be locked in hardware through jumpers. Only when upgrades are mandated, they should be unlocked and upgraded. Although this is difficult to implement on large scale manufacturing facilities with 1000 s of units for manufacturing, it must be noted that firmware upgrades are not carried out frequently and the equipment run for many months or years without the need for any change in operational logic. The risks of damage that can be caused are way higher than the lack of convenience in upgrading the firmware. Hence, we strongly recommend this method.
- Any change in software of the systems (besides firmware) should use the same level of security. Consider the extent of damage that can be caused by printing wrong labels on the medicines and sending them out in the hospitals/ stores.

9. Proactive Threat Protection

Besides a reactive strategy for security threats *i.e.* taking action once an attack occurs or is attempted, as most organizational measures deploy, we recommend pro-active threat prevention strategies along-with the strategies discussed till now. In this section we see what kind of innovative measures can be used to not only prevent attacks but also to catch the attackers and identify their intentions by monitoring their activities on the *company* network. Although at first glance, the recommendations might appear to be costly to implement, the cost is certainly less than the risks involved in security breaches. *Our company*, as a pharmaceutical company has the functions of manufacturing and delivering medicines promptly which help in saving lives. Any delays in these procedures or errors in these procedures could affect human lives and lawsuits could potentially lead to closure of the company. Considering this aspect, our recommendations in this section must be seriously considered by *our company*.

Our first recommendation is to deploy multiple *HoneyPots* at significant locations at all the facilities of *our company*. A honeypot is a system that's put on a network, so it can be probed and attacked. Because the honeypot has no production value, there is no "legitimate" use for it. This means that any interaction with the honeypot, such as a probe or a scan, is by definition suspicious [27]. Computer systems which may appear to contain confidential data like research information, payroll information, financial bills etc. which are fake could be placed at strategic locations within the company. They could be setup to monitor any network activity on them. A legitimate employee would not access these systems as they don't need to. However, an insider trying to steal data may find

these systems online while scanning the network and could get caught easily by the monitoring of the system. This would counter insider threats. A masquerader or an outsider accessing the network through an insider's credential or in general posing as an insider may try to access the resources on honeypots too and get caught by their activities on them. Honeypots may be used to fingerprint the activity of attackers and identify what they are looking for, why they are attacking the network, and also perhaps who they are. Recognizing the identity of attackers would help *our company* in catching them and thus help in reducing the threats they pose to the company.

Honeypots can help prevent attacks in several ways. The first is against automated attacks, such as worms or auto-rooters. These attacks are based on tools that randomly scan entire networks looking for vulnerable systems. If vulnerable systems are found, these automated tools will then attack and take over the system (with worms self-replicating, copying themselves to the victim). One way that honeypots can help defend against such attacks is slowing their scanning down, potentially even stopping them. Called sticky honeypots, these solutions monitor unused IP space. When probed by such scanning activity, these honeypots interact with and slow the attacker down. They do this using a variety of TCP tricks, such as a Windows size of zero, putting the attacker into a holding pattern. This is excellent for slowing down or preventing the spread of a worm that has penetrated your internal organization [28].

Our recommendation is to deploy multiple *HoneyPots* throughout all the facilities of *our company* and at strategic locations in the network. This network of *HoneyPots* is usually termed as *HoneyNet*. A *honeynet* is a type of honeypot. Specifically, it is a high-interaction honeypot designed to capture extensive information on threats. High-interaction means a *honeynet* provides real systems, applications, and services for attackers to interact with, as opposed to low-interaction honeypots which provide emulated services and operating systems. It is through this extensive interaction we gain information on threats, both external and internal to an organization. What makes a *honeynet* different from most honeypots is that it is a network of real computers for attackers to interact with. These victim systems (honeypots within the *honeynet*) can be any type of system, service, or information the company wants to provide [29].

The second recommendation is to deploy decoy documents. These decoy documents are usually also referred to as *HoneyFiles*. These are documents that look enticing *i.e.* appear to contain important information but actually contain bogus information. They won't be accessed by regular employees either because of their permissions and/or because they are not useful for them. However, an insider or a masquerader trying to steal information would try to look at them. These documents can be embedded with a beacon code through the Decoy Document Distributor system so that whenever they are accessed they trigger (say) an email alert, alerting the administrators of a suspected malicious activity [30] [31]. This way they can be caught.

Since the deployment of *HoneyFiles*, *HoneyPots* and *HoneyNets* may require some level of advanced security knowledge, *our company* may consider hiring security experts full-time to manage their security or they could consult them for recommendations on a regular basis.

10. Counter Measures for Future Threats

We looked at several aspects of security which are based on the current state of technology, both software & hardware, and which may change in the near future. These are certain areas which may need to be addressed separately in the future. Here's our view of it and a few examples:

- **Legacy systems, hardware and code**: There are many systems which use legacy code or software, e.g. Windows XP, or software written in languages like C/C++, which may be outdated in the future, or lose its support. Care should be taken to keep them to their latest patched versions, or to replace them with a secure version. This process may be difficult because in order to keep the network homogenous, the same changes may have to be done on a large number of machines, which may cause delay or downtimes, or may not be feasible immediately in cases like email server.
- **IPv6**: As the IPv4 address space is slowly expiring [32], the networking world is switching over to IPv6. Many contemporary security features may not work with IPv6 without some form of modification. The company should look into making itself IPv6 compliant in terms of security software as soon as possible. With the advent of IPv6, there is a possibility of using stronger security features like encryption, key-passing and signatures.
- **Cryptographic capabilities**: A lot of protection depends on the security capabilities provided by the present state of security algorithms like RSA. Day by day, attackers are coming up with newer attacks and also newer hardware is coming closer to crossing the computational barrier on which many secure algorithms rely. In the future, the security experts should look at methods which are based on multiple factors rather than computational difficulty. Also, older, insecure protocols should be replaced by newer, more secure ones as they arrive. The difficulty obviously lies in the scale of the transition and the fact that all machines may not be able to support all kinds of newer cryptographic operations and may require replacement as well.
- **Bypassing of learning methods by "wrong training" of IDS systems**: This is another trick used by attackers and takes place over a really long time, so it is not immediately noticed by monitoring systems. This is in the form of a particular attack which is consistent, and over a long period of time it makes the behavior engine in the IDS system raise its score much higher in comparison to other attacks. Later, the attackers launch an attack which is not much different in nature and is classified by the IDS as low severity. The company's IDS should have features that watch out against this type of "wrong" learning. Periodic evaluation/audit of threat scores of various types can help the

company in finding these types of anomalies.

- **Biometrics**: The state of biometrics has evolved in the past few years leading to technologies like facial recognition, retina scans and fingerprint readers starting to get used in devices like smartphones for authentication. They are accurate in reading the biometric input, however, the technology being fairly new is prone to spoofing. As biometrics starts getting used at a wide scale, attackers would try to come up with new ways to spoof the input. The technology may work well for a single user-based phone, but altogether replacing password authentication and certificate signing on large networks may take a while. Nevertheless, the company should be aware of this technology and prepared to adopt it in its systems where evaluations prove it to be better than conventional methods.

Most of the latest laptops and mobile phones have a front-camera. The company could mandate using ONLY devices with a front camera. The VPN software could ask for permissions to the front camera, and if permissions were not granted, the software could be disabled. The VPN software while logging into the official network could take a picture of the user trying to log-in and use it as an additional validation. Further, the camera could be accessed randomly during the user's session, ESPECIALLY when dubious activity is detected. This would help catch insiders attacking the system, remotely, which would otherwise get evaded by traditional systems. A similar approach may be adopted for fingerprint scanners. With the (remote) use of biometric hardware on the user's device, the security of access from remote locations would be similar to access on-site.

11. Conclusions

As part of this case study, we have tried to cover all aspects of computer networks that would typically be found in a large scale global organization with offices spread in different geographies. We defined a fictitious company and chose a network profile for the organization. The network profile was carefully chosen so that it is relevant, generic and nearest to the actual profile of most global organizations. However, any real organization may have some deviations from profile we have chosen. Hence, we advice that while taking the suggested recommendations, they should also be tweaked based on the actual profile of the organization being considered. We have tried to address each aspect of the network independently, with suggestions to ensure security of that part of the network. We have studied and discussed some of the recent threats that have been in the news relevant to the profile of our fictitious organization, and how those threats can be dealt with. We also tried to suggest parameters that should be used while selecting a security product from the available vendors, which would best meet the needs of the organization. By listing the different features that most security products offer and the types of appliances that are available, working at different levels of the network (ranging from host devices to network

devices), we have tried to help any organization make an informed decision, in order to ensure the security of their systems, in the best possible manner.

It must be noted that just following best practices and ensuring compliance with the security certifications are not sufficient for an organization. The personnel involved in defining the security measures must understand the organization's computer systems and how to best provide security in the current threat scenario. Hence, as part of this document, we have not looked at solutions from compliance perspective. Instead our focus has been based on the design of the networks.

References

[1] Cyber Intelligence for Pharmaceuticals.
https://www.cyveillance.com/web/solutions/industries/pharmaceutical.php

[2] AlertEnterprise Security Solutions for Life Sciences and Pharmaceuticals Industry.
http://web.archive.org/web/20140404224526/http://alertenterprise.com/solutions_ind_pharmaceuticals.html

[3] Utilizing CipherShare within Pharmaceutical and Biotechnology Industries (2006) Proven Security Solutions.
http://www.provensecuritysolutions.com/resources/CiphershareBiotechnology.pdf

[4] SANS Institute (2002) Designing Secure IT Environments for Pharmaceutical Clinical Trial Data Systems.
http://www.sans.org/reading-room/whitepapers/casestudies/designing-secure-environments-pharmaceutical-clinical-trial-data-systems-708

[5] SANS Institute (2001) Developing Security Policies for Protecting Corporate Assets.
http://www.sans.org/reading-room/whitepapers/policyissues/developing-security-policies-protecting-corporate-assets-490

[6] Damage due to Stolen Laptops.
http://web.archive.org/web/20150222152411/http://newsroom.intel.com/servlet/JiveServlet/download/1544-16-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf

[7] Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V. and Iftode, L. (2010) Rootkits on Smart Phones: Attacks, Implications and Opportunities. *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, Annapolis, Maryland, 22-23 February 2010, 49-54. http://dl.acm.org/citation.cfm?id=1734596
https://doi.org/10.1145/1734583.1734596

[8] Refrigerators Attacked and Used for Sending Spam Email.
http://www.foxnews.com/tech/2014/01/20/hackers-use-refrigerator-in-cyber-attack/

[9] Li, X.W. and Xue, Y. (2011) A Survey on Web Application Security. Vanderbilt University, Nashville, TN.
http://www.isis.vanderbilt.edu/sites/default/files/main_0.pdf

[10] Report on Sony PlayStation Attack.
https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage
http://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today

[11] Stolfo, S.J., Bellovin, S.M., Hershkop, S., Keromytis, A.D., Sinclair, S. and Smith, S.W. (2008) Insider Attack and Cyber Security beyond the Hacker. A Survey on Insider Attack Detection Research. Springer Science & Business Media, LLC.
http://www.cs.columbia.edu/~angelos/Papers/2008/24024663-0387773215-Springer

-insider-attack-and-Cyber-security-beyond-the-Hacker-apr.pdf

[12] Zhao, Y., Zhou, F.F., Fan, X.P., Liang, X. and Liu, Y.G. (2013) IDSRadar: A Real-Time Visualization Framework for IDS Alerts. *Science China Information Sciences*, **56**, 1-12.
http://link.springer.com/content/pdf/10.1007%2Fs11432-013-4891-9.pdf
https://doi.org/10.1007/s11432-013-4891-9

[13] Biermann, E., Cloete, E. and Venter, L.M. (2001) A Comparison of Intrusion Detection Systems. *Computers and Security*, **20**, 676-683.
http://www.sciencedirect.com/science/article/pii/S0167404801008069
https://doi.org/10.1016/S0167-4048(01)00806-9

[14] Juniper Network IDS Specifications.
http://www.juniper.net/us/en/local/pdf/datasheets/1000254-en.pdf

[15] Cisco Network IDS Specifications.
http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/data_sheet_c78_459036.pdf

[16] McAfee Network IDS Specifications.
http://www.mcafee.com/us/resources/data-sheets/ds-network-security-platform-ns-series.pdf

[17] Palo Alto Networks Network IDS Specifications.
https://www.paloaltonetworks.com/resources/datasheets/pa-7050-specsheet.html

[18] The Best Free Antivirus for 2014.
http://web.archive.org/web/20140506075903/http://www.pcmag.com/article2/0,2817,2388652,00.asp

[19] SSL VPNs: Five Popular Products Compared.
http://searchitchannel.techtarget.com/tip/SSL-VPNs-Five-popular-products-compared

[20] OSSEC Host IDS Features.
http://web.archive.org/web/20140405095938/http://www.ossec.net/?page_id=165

[21] Barracuda Spam Firewall Features.
https://www.barracuda.com/products/spamfirewall

[22] Verwoerd, T. and Hunt, R. (2002) Intrusion Detection Techniques and Approaches. *Computer Communications*, **25**, 1356-1365.
http://www.sciencedirect.com/science/article/pii/S0140366402000373
https://doi.org/10.1016/S0140-3664(02)00037-3

[23] García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G. and Vázquez, E. (2009) Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges. *Computers and Security*, **28**, 18-28.
http://www.sciencedirect.com/science/article/pii/S0167404808000692
https://doi.org/10.1016/j.cose.2008.08.003

[24] Tech News on Future of Anti-Virus.
http://money.msn.com/top-stocks/post--symantec-says-antivirus-software-is-dead

[25] NSS Tests for IDS Evaluation.
https://www.nsslabs.com/reports/categories/test-reports/network-intrusion-prevention

[26] Snowden's Disclosures on NSA.
http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013–present)

[27] Harrison, J. (2003) Honey Pots. The Sweet Spot in Network Security.
http://www.computerworld.com/s/article/87288/Honeypots_The_sweet_spot_in_ne

twork_security

[28] Paper on HoneyPots. http://www.tracking-hackers.com/papers/honeypots.html

[29] Honeynet Project (2006) Know Your Enemy: Honeynets. http://web.archive.org/web/20140404155323/http://old.honeynet.org/papers/honeynet/

[30] Bowen, B.M., Hershkop, S., Keromytis, A.D. and Stolfo, S.J. (2009) Baiting inside Attackers Using Decoy Document. Columbia University, New York. http://www.cs.columbia.edu/~angelos/Papers/2009/DecoyDocumentsSECCOM09.pdf

[31] Salem, M.B. and Stolfo, S.J. (2011) Decoy Document Deployment for Effective Masquerade Attack Detection. Columbia University, New York. http://www.cs.columbia.edu/~Malek/Dimva_2011_final.pdf

[32] IPv4 Address Depletion. http://en.wikipedia.org/wiki/IPv4_address_exhaustion