

Computer Security

Computer sceince

Rashid Al-Mahmud | 21269650

Table of Contents

[Investigation on current threats 2](#_Toc463385120)

[Types of threats 2](#_Toc463385121)

[Computer virus 2](#_Toc463385122)

[Spyware threats 2](#_Toc463385123)

[Hackers and predators 2](#_Toc463385124)

[Phishing threats 3](#_Toc463385125)

[Protective Measures 4](#_Toc463385126)

[Threats prioritized 6](#_Toc463385127)

[Vulnerabilities 7](#_Toc463385128)

[Policies 8](#_Toc463385129)

[standards/guidelines 9](#_Toc463385130)

## orignisation

We need to understand what we will be analyzing and possibly protecting first to be affective. In this case what it is that I will be studying is a gas station, there needs to be a break down in the structure or security, this is the where the system will require the security.

## Investigation on current threats

### Types of threats

First we need to understand the amount of current threats and how many different types of threats there are. A threat can come in the form of hacker hacking into your system to retrieve all of your information and your customer information cleaning out your company and them loosing the customer information. Another way could be that someone find s a way to watch you company and then just watching what you do and always keeping a step ahead of you. Another threat could be be as simple of getting a malicious virus into your system and them it deleting various information crippling your company until you have been fixed. We will first be filtering and speaking about the many threats and circling down to the most current and imposing threats that we have in this day and age. We will also be talking on how to prevent this and way to always to stay in front of the threats.

### Computer virus

This is probably the most well known threat to people and it something most people do not like to hear when it comes to there computer because what the virus can do to the computer. What this is a program that is written to alter the way the computer performs, loosing control of a computer system especially in a big company can be disastrous even more so now because of how heavily reliant modern companies rely on computers. The virus became such a threat due its regards to permissions and security penetration capabilities it can do what it wants, once it is in your system, but this can be solved by having a good firewall and anti-virus system, but in big company loosing a couple seconds could cost billions. What it does basically in the computer system is it replicates and executes its instructions.

### Spyware threats

This is a potentially devastating threat, this is something that can bring down some of the largest companies, what spyware does can be guessed by its name. The spyware and tracks and records what you do on the internet, this could include private information credit card details or customer information etc. and again like the previous threat this doesn’t need you permission to do this. In a one off account where it happens only to one person it can terrible for a large scale company the consequences can be disastrous and a company recovering from an attack like this is minimal.

### Hackers and predators

This threat that is directly from the humans, there are people that create malware and hack in systems for there own benefits, this can be for information they want or entering system to make them work however they want to work. This threat is very dangerous, some of the most secure systems in the world have been hacked in the military systems. This is known as cyber terrorism, the information taken will used for their own gain, but the criminals can be caught and can face lengthy prison sentences.

### Phishing threats

This threat is probably one of the most direct and out right evil threats there are just of the nice front that will be presented to you. This could come a nice phone call telling you give your computer system details; this might seem to be easily avoidable but it has affected millions because of the how much information the general public has on computer security.

Top five external threats to corporate IT systems and suggests that a layered approach to defense can help companies become more prepared for attacks  
  
**1.** In terms of sheer frequency, the top spot on the list of security threats must go to viruses. According to a DTI survey, 72% of all companies received infected e-mails or files last year and for larger companies this rose to 83%. Worms and Trojan horses share the first prize in malignancy: the internet experienced three worms in only 12 days last summer, causing £1.8bn in damages, according to Symantec's Internet Security Threat Report.  
  
**2.** The after-effects of viruses are so dangerous that they take second place. The vulnerability here is the back doors viruses leave in their wake, or the chinks in the corporate armour that later generations of code can exploit. For example, in January, MyDoom left a back door that was subsequently exploited by Doomjuice and Deadhat. Companies that failed to close the back door, as well as rid themselves of the primary attack, remained exposed.  
  
Another related threat is the worms that turn PCs into remote mail servers and send cascading volumes of e-mails that cause denial of service attacks. These attacks are becoming more sophisticated.  
  
"Most mass mail viruses require the recipient to open the attachment to run the malicious code," says Carole Theriault, security consultant at anti-virus company Sophos. "However, there are viruses that can take advantage of security flaws which means that only viewing or opening the e-mail is enough to launch the malicious code."  
  
**3.** Hacks, and application-specific hacks in particular, have become even smarter. Many companies are alert to the threat posed by so-called buffer overflows, the techniques by which web servers are overloaded causing a denial of service attack. But the new kid in this category, and the one the security industry is talking about, is the more advanced SQL injection.  
  
SQL injection forces a database to yield otherwise secure information by causing it to confuse classified data, such as passwords or blueprints, with information that is for public consumption, such as product details or contacts. It is hard to do but, according to the experts, there are plenty of hackers up to the task and plenty of customers ready to pay for the service.  
  
"We see it all the time," says David Litchfield, founder of NGSSoftware. "It is behind breaches such as the half a million credit card numbers stolen by Russian gangs or details from the Drug Enforcement Agency being sold onto drug runners. These are documented cases. SQL injection is not getting the respect it deserves."  
  
**4.** Phishing, or identity theft, is most commonly targeted at bank customers but everybody should be alert to it. The bank users receive an e-mail as if from the bank asking for their log-on and password and, according to risk specialist company mi2g, less than half of 1% of customers oblige, a significant figure if millions of e-mails are sent.  
  
A more sophisticated version of phishing, cross-site scripting, is on the rise, where users are driven to an identical but fake version of the bank's website and are lured into handing over confidential information unawares.  
  
**5.** Blended attacks are combinations of two or more of the above and are doubly alarming. The solution to protecting a company against these attacks is to combine the piecemeal security systems that protect against each kind of threat. But how secure are these security systems and who is winning, the attacker or the attacked?

Protective Measures  
  
Most of the measures companies can take to protect themselves are reactive, and anti-virus patches and firewalls are now, for the most part, implemented as standard. But these are responses to known attacks, rather than an anticipation of the unexpected. They do nothing to thwart the activities of worms that turn PCs into machines from which further attacks, such as mass e-mailing, can be launched. Nor can they deal with the more sophisticated hacks, such as SQL injection. To combat this level of threat, additional security must also be in place.  
  
This security can be grouped in three layers. The first layer scans IT systems for suspect activities by using intrusion prevention technology and by monitoring anomalous requests. For example, SQL injection often works by sending unusually long search strings to database query tools.  
  
"An intrusion prevention system that monitors traffic and watches for unexpected behaviour such as this should pick up the attempt," says Nick Garlick, sales director of Nebulas Security.  
  
Alternatively, a denial of service attack might be thwarted if the security system recognises high levels of a particular sort of traffic before they become so high the network falls over.  
  
Garlick also points out that testing new software adequately before it goes online is important. "The big issue is that coders tend to work to deadlines and do not think like security people," he says. "Build processes should also include penetration testing."  
  
A second layer is added when defences are integrated. For example, if a virus is known to open up a back door, the anti-virus system should not only search for the virus but also for the back door. Alternatively, it must prompt the firewall to stop entry through the back door. This is a complex process to carry out across enterprise-wide IT systems, and so experts advocate the installation of security management systems.  
  
"Suppliers are starting to develop the capabilities of systematic and effective patch management systems," says Jan Fundgren, a security analyst at Forrester. "When there is no 'all-in-one' solution, better enterprise security management is more likely to succeed." Compliance tools add another form of defence and can monitor how thoroughly systems have been patched against viruses.  
  
The third layer is good risk assessment. Online systems inevitably bring a degree of vulnerability along with excellent business opportunities, so internet security should be built into the company's calculations. If the business can understand which systems are most vulnerable, protective measures can be taken to cut the risk. That is the essence of dealing with external security threats.

## Threats prioritized

## Vulnerabilities

## Policies

## standards/guidelines