# 

# 

***CSCI 530 COMPUTER SECURITY SYSTEMS***

***RESEARCH PAPER:***

***HOW TO MITIGATE SOME THREATS THAT AFFECT CORPORATE BUSINESS AND PRIVATE SYSTEMS ON A COMMON GROUND.***

***NIRANJANAA MOHANBABU - 2584318921***

I have read the Guide to Avoiding Plagiarism published by the student affairs office. I understand what is expected of me with respect to properly citing sources, and how to avoid representing the work of others as my own. The material in this paper was written by me, except for such material that was quoted or indented and properly cited to indicate the sources of the material. I understand that using the words of others, and simply tagging the sentence, paragraph, or section with a tag to the copied source does not constitute proper citation and that if such material is used verbatim or paraphrased it must be specifically conveyed (such as through the use of quotation marks or indentation) together with the citation. I further understand that overuse of properly cited quotations to avoid conveying the information in my own words, while it will not subject me to disciplinary action, does convey to the instructor that I do not understand the material enough to explain it in my own words, and will likely result in a lesser grade on the paper.  
Signed:\_\_Niranjanaa Mohanbabu\_\_\_\_\_\_\_\_

***ABSTRACT- In recent times, the potentiality of a cyber-crime has increased tremendously with respect to the increase in usage of the internet which increased the amount of cyber crimes hugely. Most affected by these crimes are either individuals when their private systems are hacked and then business organizations such as universities and companies where data is leaked and losses are incurred in multiple ways such as financially, customer’s trust and infidelity etc. The aim of this paper is to discuss in depth about the variety of these crimes and also compare and contrast between these crimes and find out how they affect not only a private system but also huge networks of devices which are interconnected in an organization.***

***Keywords : Threats, Risks, Corporates, Private systems, Devices, Vulnerabilities***

1. **INTRODUCTION**

When a system malfunctions, either fully destroying its purpose of installation or performing suspicious actions, it is considered to be hacked or under assault. A task is labeled suspicious when it is either abnormal or breaches system policy. The repercussions of an assault can be as severe as a vital information leak or a catastrophic system breakdown beyond recovery. This hacking can be of multiple types such as phishing, denial of service(DoS), Viruses, Worms, Trojan Attacks and much more. We will mainly be discussing the following :

i.Malware,

ii.Phishing

iii.CATO(type of phishing),

iv. Weak Passwords

v. Database Exposure



1. **LITERATURE SURVEY**

Threats that have been a technical issue for many years now. Most of this research is obtained from [3] where they discuss different types of cyber securities and threats. Other resources include wikipedia and from common knowledge that has been referenced to in the

Final section of this paper.

1. Malware

Malware is a combination of two words for malicious software, which is meant to harm a computer system without the user's knowledge. Being one of the most serious dangers to computers, tablets, phones, and other device’s security, malware encompasses viruses, spyware, ransomware, and other undesirable software that is deployed discreetly on any system. Spam attacks with malicious attachments or drive-by downloading that happens when an employee accesses an infected website inadvertently, and malware is subsequently installed and run without the person's insights are easy techniques for malware to propagate.[2] Once malware is installed, criminals may use it to steal important information, send customers unwanted or inappropriate adverts, demand money to unlock data locked by ransomware, and render the device vulnerable to other infections.

2.Phishing

According to MalwareBytes[1], phishing is an action in which the malicious attacker disguises himself as a reputable person or organization in order to dupe potential victims into revealing sensitive information or paying money. There are several ways to lure in a prey, much like in actual fishing: Three popular varieties include email phishing, smishing, and vishing. The three main stages of how phishing works :

* In a phishing operation, the attacker creates a fake (or "spoofs") identity that can be trusted that the receiver is probably familiar with. Depending on the sort of phishing operation, it might be a person, such as a recipient's family member, the CEO of the firm they work for, or even someone prominent who is presumably giving something for free. Phishing emails frequently imitate communications from huge corporations such as PayPal, Amazon, or Microsoft, as well as banks or government offices.
* The message: The attacker will ask the receiver to click a link, download a file, or give money under the pretext of someone trustworthy. When the victim reads the message, they receive a disturbing message designed to overwhelm their common sense by instilling anxiety in them. The message may urge the individual to visit a website and take quick action or face repercussions.
* Users who fall for the lure and click the link are sent to a spoof of a real website. They are then prompted to sign in using their username and password. If they are tricked enough to comply, the attacker receives the sign-on credentials and uses it to steal identities, hijack bank accounts, and create losses in the stock market in corporations .[]

3. WEAK PASSWORDS

Password-based security has become increasingly difficult. It is nearly hard to create and remember a complicated password for each account and website on your own. Using weak and basic passwords, on the other hand, is a strategy for data theft, account invasions, and other types of threats.

* A weak password[4] could allow an attacker the ability that would otherwise be denied. As a result, additional possible attack avenues are available.
* A weak password, for example, might allow an attacker to get access to your bank accounts using the email/password reset option on your bank/insurance company website (assuming you use the same email address/password combination).
* It may also allow an attacker to access your emails or social media accounts if you use the same email/password combination as the attacker (this is where hackers will try different common passwords with varying success rates also known as brute force attacks).

4. CATO

CATO,[3] also known as Corporate Account Takeover arises when cyber hackers obtain valuable employee credentials and information and seize control of networks. Criminals can then conduct fraudulent wire transfers and transactions to any account using the ACH. Hackers usually gain access to a system by harmful software (malware), which can infect a laptop via e-mail, websites, or malware masquerading as software. It is critical to completely know the gravity of these attacks, their influence on consumer trust, and the possible consequences for the institution's image.

If strong authentication is not implemented and a user's credentials are taken, the culprit can get access to the business's fund. The credentials appear to be the authorized user to the banking institution.

The attacker has accessibility to the company's accounts and may review them. Account activity and trends are provided, as well as ACH and wire transfer origination criteria such as file size and frequency constraints and SEC codes.

With awareness of the account's rights and limitations, the attacker can transfer funds out of the account using wire transfers via ACH files.

For example, the Patco Construction Company sued Ocean Bank after Patco’s computers became infected with malware, allowing fraudsters to make six wire transfers amounting to more than $588,000 using the Automated Clearing House (ACH) transfer system. Only $243,000 of the stolen money was recovered.

5. DATABASE EXPOSURE

This is the type of threat that every business and individual is worried about. Most devices have sensitive information that no one wants to be revealed. When such information gets leaked either intentionally or unintentionally, it leads to database exposure. Sensitive data exposure flaws can occur when a web application fails to adequately protect the data from being accessible to attackers. There are 3 types of sensitive data[5]:

* Personal/Private Data of an individual, such as medical records, laboratory tests, and insurance information Enrollment records and transcripts, as well as financial documents such as credit card numbers, banking information, tax forms, and credit reports.
* High-risk businesses that contain confidential intellectual property, trade secrets, or merger plans that may all be detrimental to the firm if they came into the hands of a competitor.
* Classified Data that has been purposely kept hidden at the governmental level. It is usually classified as restricted, confidential, secret, or top secret, which restricts who has access to the material.

Data that has been leaked due to negligence of security is also considered as an exposure as that information is now accessible by the hacker from which he can get other details. The following diagram shows how a attacked infiltrates his way into a company’s server[6]:



**How these threats affect businesses:**

As corporate businesses have a larger scale of finances involved, hackers have higher chances of getting a higher ransom once they hack into their data.

But organizations are prone to have large numbers of interconnected devices which are exponentially harder to crack through. This requires the hacker to use different combinations of attack vectors to bypass the network security. It includes a series of steps that is followed to breach through where the first step into a network typically involves some sort of phishing, social engineering or web application attack. They can begin deploying ransomware to all targets they can reach as soon as they establish a hold in the network.

Another factor that has to be kept in mind is that no two companies are the same. A hacker has to keep in mind the size, type, number of devices, consequences if anything fails and other minute details. In order to compromise the confidentiality, availability and integrity of data, the attacker just has to place worms, viruses or trojans(malware software). Secondly, he can also use Phishing techniques to steal private information from users through masquerading as a trustful source (e.g. website or identity theft) as explained before. [7]

Cato is usually done by brute force attack where they get the credentials of employees in their system and then apply phishing as an employee to perform discrepancies. Every business should perform a risk assessment and establish the required security with respect to their assessment. The purpose of risk assessment is to develop policies that can resolve the security factor in a company. The picture below that is surveyed by Pamden depicts the types of risk assessment. [2]



**How Companies Protect Themselves:**

Companies usually protect themselves by having multiple layers of firewalls and encrypted protocols. Another method is by having a controlled database of who is having access to what kind of information. This is an extremely important step as sometimes threats come through employees and competitors. Those staff who were fired can expose trade secrets to earn money from the rivalry company or for other purposes. Lastly most businesses hire specialized IT security systems who provide solutions after the risk assessment[8].



For instance, the University of Southern California(USC) has a huge data set of student details. These details consist of the financial documents, medical records, academic transcripts and bank information as well. USC has ensured security by getting 2–factor authorization by Duo for every login at every website they own for each student.

**How Private Systems are Affected:**

A private system in this generation can be any device that is owned by an individual. This includes a mobile phone, laptop, tablets etc. Considering the amount of devices that are used by people today with internet access, cybercrime increases massively. As compared to a large business, a person’s interconnection of devices is low but also relatively easier to break through. How each cyber crime affects an individual are explained below:

1. Malware: This is the main type of attack used on people as they fall for it easily. Most methods include malicious software that is installed on laptops or in the form of apps in mobile devices. For example, a highly modernized calculator app that has a hidden photo vault in a mobile phone might give access to the photos in them to anyone when downloaded. We also tend to download a lot of data from untrusted sources that contain viruses which are eligible to wipe off complete data on the device as well.
2. Phishing [9]: An identity theft can be done to get details of your credit card or such via a phone call or an email by impersonating a company. This is usually given in the mode of free gifts or raffle win vouchers to their customers. Some people tend to give out such crucial details on call without verifying who is on the other side and hence fall right into the trap of the phishers[10].
3. Weak Passwords: People choose the most common passwords such as ‘password’ or ‘12345678’ or ‘0000’ or ‘1234’ etc as they are easy to remember. These passwords take just a few seconds to be cracked by an attacker. Another way is that most of us use the same combination of credentials. For example, a student will use his username for multiple websites that belong to the school but he also tends to set the same password for every website so he can keep track of it. He does not understand that if an attacker tries to intrude his system, the hacker can get access to the student’s complete database. A student database has financial details of their parents who again have weak passwords so the hacker reaches them as well. This loop continues until the hacker is not able to break through the passcode or reaches to the point where the hacker has managed to manipulate all the details that he needs to.
4. CATO : This does not apply for individuals as it's meant only for corporations, huge organizations and businesses.
5. Database Exposure: Many private devices have their passwords saved for easier access, have private details, files that are all saved in their laptops which are not encrypted. Unsecured data exposed all over the net brings loss to billions of people.

**How to Mitigate these threats**

High usage of devices has made people extremely vulnerable. Social Media, being introduced for connection purposes has now become a network platform where all these issues happen at once. In order to protect ourselves, we have to detect the malware. Recently, third party anti-malware softwares has been installed, more firewalls are built and all documents encrypted with digital signatures are being implemented. Below is an example of how a risk is mitigated.[11]

**III. Conclusion**

This research paper explains the most important and common threats. We have also established how it differs from a huge business to small scale private devices. Thus concluding how to mitigate these risks as well has been discussed.

**IV. CITATIONS**

[1]M. Ozer, S. Varlioglu, B. Gonen and M. Bastug, "A Prevention and a Traction System for Ransomware Attacks," 2019 International Conference on Computational Science and Computational Intelligence (CSCI), 2019, pp. 150-154, doi: 10.1109/CSCI49370.2019.00032.

[2]<https://www.pamten.com/blog/why-you-need-a-cyber-security-risk-assessment/>

[3]K. Thakur, M. Qiu, K. Gai and M. L. Ali, "An Investigation on Cyber Security Threats and Security Models," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015, pp. 307-311, doi: 10.1109/CSCloud.2015.71.

**V. REFERENCES**

1. https://www.malwarebytes.com/phishing
2. https://www.researchgate.net/publication/267777154\_Malware\_Analysis
3. https://www.hypr.com/security-encyclopedia/corporate-account-takeover
4. https://www.cybersecurity-automation.com/what-are-the-risks-of-weak-passwords/
5. https://www.lawinsider.com/dictionary/data-exposure
6. https://www.zettaset.com/blog/what-is-sensitive-information/
7. https://www.sciencedirect.com/science/article/pii/S2212567115010771
8. https://www.zettaset.com/blog/what-is-sensitive-information/
9. trendmicro.com/en\_us/what-is/phishing/types-of-phishing.html#:~:text=Phishing
10. <https://resources.infosecinstitute.com/topic/who-is-being-targeted-by-phishers/>
11. https://en.wikipedia.org/wiki/Malware#Mitigation