Name - Manish Arora **Mis - 111803036** **Btech Comp Div1**

1) IT Risk and Resilience - Cybersecurity response to Covid-19

DOI: MITP.2020.2988330

Introduction:
COVID-19's global spread has had a major impact on practically everything. Businesses and educational institutions have shuttered, people have been forced to work from home, supply chains have been interrupted, social gatherings have been prohibited, and so on. However, these activities must continue, and Information Technology has assumed a vital role in the majority of them by converting them to an online format. All of this has benefited IT, but it has also presented some issues. Above all, there are new and heightened cybersecurity dangers and vulnerabilities.

Increased Threats and Vulnerabilities Examples:
a. Zoom Bombing: Trolling hackers can steal authentication credentials and inject unwanted content into supposedly secure collaborative online meetings thanks to security and privacy flaws in teleconferencing software.

b. COVID-19 Phishing Attacks: There were bogus, malicious emails that seemed to be from the Centres for Disease Control and Prevention, according to FBI advisories (CDC). They either had malware attachments or were attempting to steal user credentials.

c. Malware: A Corona Trojan is an example of malware that overwrites the master boot record and disables hard disc storage. During the pandemic, ransomware assaults on healthcare systems have increased.

d. Network Availability: Despite a significant increase in traffic, the performance of essential communication networks and clouds remained good, however several collaborative applications saw spikes in service failures.

Industry Response:

- Remote access security
- Defending against rising fraud and virus threats.
- Evaluating the security posture of new suppliers (as well as changes to the security posture of current suppliers).
- Ensuring the availability and security of critical information systems.
- Managing staff morale; e. Refactoring security programme priorities, architectures, and budgets.
- Alignment with corporate leadership.

Planning For Future:

- Epidemics of infectious diseases and other types of crises are unavoidable and unpredictable. Their response, on the other hand, can be reduced by improved preparedness and effective response.
- IT will continue to play an important role in the post-COVID future. IT and other industries must continue to plan ahead of time, focus on research and development in practical areas, and revisit and modify their policies.
- Lessons learned from the current crisis should be used to examine and change necessary crisis management rules, as well as IT and business risk management policies, strategies, and practises.

2) Pegasus Spyware – A Privacy Killer

DOI: http://dx.doi.org/10.2139/ssrn.3890657

Introduction:

Pegasus is a type of spyware (Trojan/Script) that can be remotely deployed on Apple's iOS and Google's Android operating systems. NSO Group, an Israeli technology company, created and commercialised it. The NSO Group provides Pegasus to "vetted nations" for "lawful interception," which is widely assumed to imply battling terrorism and organised crime, as the company claims, but there are concerns that it is used for other purposes.

The latest Pegasus Project discoveries of about 50,000 persons being targeted for cyber-surveillance around the world, including some in India, has firmly placed the emphasis on the Pegasus spyware, largely regarded as the most advanced smartphone attack weapon.

The latest Pegasus malware uses "zero-link" technology, which means the user does not have to click on any links. Since the vulnerability is still in its "day zero", there are no patches or updates that can secure a user.

Working:

A. Target: A trap link is sent to a smartphone that convinces the victim to tap and activate or activates itself without any input, like in the most sophisticated "zero-click" hacks.
B. Infect: According to NSO marketing materials, the spyware captures and duplicates the phone's most basic functionalities, including recording from the cameras and microphone and gathering location data, call logs, and contacts.
C. Track: The implant sends this information to an operative in secret, who can use it to map out sensitive facts of the victim's life.

What can Pegasus do?

A. **Intercept calls:** Real-time monitoring of voice and VoIP calls.
B. Gather unusual and novel sorts of data (e.g., contacts, files, environmental wiretaps, passwords, and so on).
C. **Handle encrypted content and devices:** Overcome encryption, SSL, proprietary protocols, and any other obstacles that the complicated communications world throws at you.
D. **Pinpoint targets:** Use GPS to track targets and obtain precise positional information.
E. **Service provider autonomy:** There is no requirement for collaboration with local Mobile Network Operators (MNOs).
F. Allows the controller to access the phone's microphone and camera, although it makes no mention of how this would effect other apps.

G. The controller can access files, photos, and even read encrypted messages and emails, but it's unclear whether they can control other applications on the phone.

How to avoid such attacks?

A. When using your device, only open links from known and trustworthy contacts and sources.
B. Ensure that any relevant fixes and upgrades are installed on your device. While having a standardised operating system provides a steady platform for attackers to target, it is still your best defence.
C. When accessing sensitive material, avoid using public or free WiFi connections (including hotels). When you need to use such networks, using a VPN is a fantastic alternative.
D. Enable pin, finger, or face-locking on your phone to restrict physical access to it.

3) A Technical Review Report on Cyber Crimes in India

DOI: 10.1109/ESCI48226.2020.9167567

Introduction:

Thousands of people utilise the internet, which is a global network of interconnected frameworks. The number of people using smart phones is steadily increasing, raising concerns about security and privacy.

Banks are critical in arranging money and channelling it for the financial advantage of the nation. However, the banking industry has recently been hit by a crisis as the number of fraud cases has risen dramatically. Similarly, cyber-crime among children and women is on the rise in India, thanks to chat rooms. Corporate researchers are mostly working on Security Analytics to combat cyber-crime threats. Network managers can use analytics to keep an eye on real-time detection and network streams for both suspicious and malicious patterns.

Case Studies:

➢ **Extortion case experienced at Greater Hyderabad MunicipalCorporation (GHMC)**

- ☐ Cyber-crime cops in Hyderabad apprehended a GHMC data entry operator and his sibling for fraudulently issuing a Property Tax Identification Number (PTIN) for a plot in Rajendra nagar.
- ☐ Jay Chand Velaga, an outsourcing worker, had previously entered into the GHMS website and dishonestly modified the data, issuing door numbers and PTINs for property for some advantage, and his brother assisted him in this illicit transaction.

➢ **Digital Fraud instances of 2017**

- ☐ A Rs 3700 crore online scam was registered against a so-called entrepreneur who defrauded over 7 lakh people under the guise of "Social Trade."
- ☐ Due to the fear of associating aadhar with a bank account, an ICICI Bank aadhar scam involving Rs 1.3 lakh was reported. Unauthorized individuals pretended to be bank officials and deceived bank clients by stealing their OTP.
- ☐ The LIC has been warned about the aadhar fraud. Fraudsters are establishing bogus websites to deceive LIC customers and steal their money.

Why cyber-crime instances are growing rapidly ?

Due to lack of awareness regarding cyber-crimes and cyber security.
Presence of cyber-crime cells are yet not known to numerous people.

Cyber culprits are very difficult to trace by cops since crime is not happening physically rather it is happening logically.
Hence cyber culprits are left uncaught by cops, which lead to the rise of cyber-crimes.

Various Types of Online Scams

A. **Phishing email scams:** Cybercriminals used to send victims emails or messages including various tricks in order to persuade them to submit sensitive and important data such as banking passwords.
B. **The Nigerian scam:** A scammer sends an emotional message asking for help in reclaiming a large sum of money from banks by paying a little amount of money for legal and paper matters in exchange for which they promise to return a large sum of money.
C. **Scams involving greeting cards:** If such emails are read and the card is activated, harmful software is downloaded and installed on the operating system.
D. **Credit card or bank loan scams:** People receive messages claiming to have won a lottery jackpot or a substantial sum of money.
E. Scammers demand mandatory fees in order to obtain that money, and people who pay the cost become victims.
F. **Hitman scams:** Scammers tell victims via email that unless they pay a sum of money via online banking, they will kidnap or injure the victim's family members.
G. **Online romance scams:** Scammers can simply deceive their online partner by telling them that they are truly in love. They begin collecting useful and lucrative banking information when they have been persuaded. They quickly end the relationship after defrauding the victim because there is no proof because everything is done digitally.
H. **Bitcoin scams:** Digital wallets can be easily hacked.
Cyber-criminals are stealing precious data of the victim’s from this new technology.

Conclusion:

The problem is that the perpetrators of these scams are difficult to identify, which is why they are becoming more common by the day. Women between the ages of 16 and 35 are also more vulnerable to cyber-crime, according to research.
Cyber-attacks on banking systems are extremely common. Currently, each district in India has a cyber cell, yet many people are unaware of its presence. As a result, more secure and efficient technology and networking systems for securing persons' essential data must be devised and implemented to reduce cyber-crime. At the same time, awareness workshops should be held to educate individuals, particularly women, children, and senior people, about various types of cybercrime and how cyber security measures can be applied to protect their data.