A brief Survey: Current Trends in Cyber Security and the its challenges in India

Mehak
School of Computer Science & Engineering,
Lovely Professional University,
Phagwara, Punjab, India.

Abstract—Cyber Security plays an important role in IT growth, as well as Internet services. Generally, our attention is drawn to "cyber security" when we hear about "cyber-crimes." So our first thinking on "National Cyber Security" starts on how effective our "Cyber Crimes" handling system is [1]. This paper recognition on cyber safety emerging trends even as adopting new technology such as mobile computing, cloud computing, e-commerce, and social networking. The paper also describes the challenges because of loss of coordination among Security agencies and the Critical IT Infrastructure.

Keywords—Cyber security, Cybercrime, Cloud Computing, CERT, Mobile computing, social networking

1. INTRODUCTION

Internet is the major developing areas for development of technical infrastructure [2]. In today’s organizational environment, technologies including cloud computing, and next-generation cellular computing are changing the fact that how groups make use of data generation for sharing facts and undertaking business online [3]. Today, more than 80 percentage of total industrial transactions are carried out online, so this discipline requires a vast amount of safety for obvious and exceptional transactions. The application of Cyber Security covers the protection of IT systems in the enterprise not most effectively, however also to the broader virtual networks upon which they depend. It includes the cyber area itself and essential infrastructures to implement the security aspects [4]. Cyber security performs a vital role within the ongoing improvement of records era, in addition to Internet services [5]. Improving cyber security and shielding essential data infrastructures are crucial to protection for every nation and financial wellbeing. Keeping the Internet safer and more secure ends up being an important part of the development of the new services besides government policy [6]. Impending cybercrime is a crucial element of a countrywide cyber protection and critical records protection strategy.

For this purpose, the development and execution of a national cyber security policy and strategy needs a systematic approach [7]. For example, cyber-security techniques, implementing technological protection systems or educating users in order to avoid the situation where they are prone to become victims of cyber-attacks or cyber-crimes. This will help in reducing the risk of cybercrime at personal and organizational level as well [8]. Developing and promoting cyber-security policies is a necessary element in fighting against illegal cyber activities [9]. Only technical interventions alone cannot prevent any crime from occurring. It is critical that law enforcement agencies should be allowed to investigate and prosecute cybercrime effectively [10].

2. LATEST ISSUES ON CYBER SECURITY

Privacy and stealing information are be the topmost issues related to cyber security that all organizations want to focus upon. We are into an era where all of the information is in digital form. Social networking websites provide a secure space for users as they communicate with family and friends. In the case of domestic users, cyber-criminals would proceed to aim social media websites to abduct one’s personal information.

There are some malicious incidents which are happening on Android devices, but it will no longer be on a huge scale. The hand palm devices such as, tablets share the same operating device as that of cellular phones’ capacity. They will be quickly affected with the equal malware. The number of occurrences of malware will continue to grow for Macs, though it will be much less as compared to Personal Computers or laptops. Windows 8 permits the customers to improve applications for simply any system strolling Windows 8, so it will be viable to create malicious applications like these for Android softwares[11]. Figure 1 shows the rate of cyber crimes in India in last 5 years and Figure 2 shows the statistics of government sites being hacked in last 4 years.
According to a national survey of U.S. technology, Silicon Valley Bank encountered that cyber-attacks are a dangerous threat both to data of the organization and to every organization’s continued business.

- 98% of businesses retain or raise their cyber security capabilities, and half of them increase their resources this year for online attacks
- Most people of companies are gearing themselves to fight against the cyber-attacks, if situation arise.
- One-third of the companies have confidence in the security of the information of business partners but less confidence in their organization’s security measures. Table 1 show the analysis of increase/decrease of crime in 2 years.

<table>
<thead>
<tr>
<th>Incidents</th>
<th>Jan-June 2018</th>
<th>Jan-June 2019</th>
<th>% Increase/Decrease</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td>2439</td>
<td>2490</td>
<td>2</td>
</tr>
<tr>
<td>Intrusion</td>
<td>2203</td>
<td>1726</td>
<td>(22)</td>
</tr>
<tr>
<td>Spam</td>
<td>291</td>
<td>614</td>
<td>111</td>
</tr>
<tr>
<td>Malicious code</td>
<td>353</td>
<td>442</td>
<td>25</td>
</tr>
<tr>
<td>Cyber Harassment</td>
<td>173</td>
<td>233</td>
<td>35</td>
</tr>
<tr>
<td>Content related</td>
<td>10</td>
<td>42</td>
<td>320</td>
</tr>
<tr>
<td>Intrusion Attempts</td>
<td>55</td>
<td>24</td>
<td>(56)</td>
</tr>
<tr>
<td>Denial of services</td>
<td>12</td>
<td>10</td>
<td>(17)</td>
</tr>
<tr>
<td>Vulnerability reports</td>
<td>45</td>
<td>11</td>
<td>(76)</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>5581</td>
<td>5592</td>
<td></td>
</tr>
</tbody>
</table>

The following list was drawn up from study and survey on cyber security [13] [14] [15].
2.1 Artificial intelligence (AI) will play an increasing role in both cyber-attack and defense [18]

AI is the new arms race, but unlike earlier arms races, anyone can get involved – there’s no need for the sort of resources that were previously only available to governments. This means that while AI is undoubtedly being researched and developed as a means of crippling an enemy state’s civil and defense infrastructure during war, it’s also easily deployable by criminal gangs and terrorist organizations.

So rather than between nations, today’s race is between hackers, crackers, phishers and data thieves, and the experts in cybersecurity whose job it is to tackle those threats before they cause us harm. Just as AI can “learn” to spot patterns of coincidence or behavior that can signal an attempted attack, it can learn to adapt in order to disguise the same behavior and trick its way past our defenses.

This parallel development of offensive and defensive capabilities will become an increasingly present theme as AI systems become more complex and, importantly, more available and simpler to deploy. Everything from spam email attempts to trick us into revealing our credit card details to denial-of-service attacks designed to disable critical infrastructure will grow in frequency and sophistication. On the other hand, the technologies available to help us escape victimization, such as profound learning security algorithms, automation of processes vulnerable to human error, and defense of biometric identity, are also improving. The most common and current network threats are depicted in Figure 3 below.

![Fig.3: Top network threats to an organization](image)

2.2 Political and economic divisions between east and west lead to increased security threats [18]

As it appears to most people, the internet and the online world is an international entity – relatively free of borders or restriction on the free movement of information and ideas. It’s been built that way because its architects understand the importance of international cooperation when it comes to accessing talent and resources. But that’s really all just an illusion. The corporations, networks, and associations which provide the infrastructure behind the scenes are legal entities obliged to comply with national laws and regulations.

With no end in sight to the “trade war” between the world’s superpowers, talk of fracturing among international organizations like the UN or EU, and an ongoing tech-driven arms race among nations that are economic competitors, that illusory veneer is being stretched thinner and thinner. And that could have very scary consequences. Russia announced that it had tested an 'unplugged' internet, basically a country-wide alternative to the global internet, which could give their Government control over what citizens can access on the web. Countries like Iran and China are already censoring content and block access to external information.

In 2019, we also saw the US government effectively embargoing partnerships between US tech firms and the Chinese mobile giant Huawei, due to fears over the close links between Huawei and the Chinese state. If more barriers like these go up, it could easily have the effect of preventing international cooperation on both the technological and regulatory challenges of cybersecurity, and that’s only likely to benefit the bad guys.
2.3 Vehicle hacking and data theft increases [18]

Even before we get into the subject of self-driving cars, vehicles today are basically moving data factories. Modern cars are fitted with an array of GPS devices, sensors, and in-car communication and entertainment platforms that make them an increasingly profitable target for hackers and data thieves.

Criminals have learned to piggyback into private networks through connected home appliances and smart devices, thanks to the lack of security standards among the thousands of device manufacturers and service providers. Likewise, the automobile is likely to increasingly become the backdoor of choice in the coming years thanks to the growing amount of data they collect and store about our day-to-day lives. Attackers will have the choice of targeting either the vehicles themselves, perhaps using them to access email accounts and then personal information, or the cloud services where our data is routinely sent for storage and analysis. Large scale harvesting and resale of this data on the black market is highly lucrative for cybercriminals.

Another very real danger is that malicious actors could learn to compromise the digital controls and safety features of modern vehicles. The idea of hijacking autonomous cars and taking over their controls may seem far-fetched right now, but it’s a threat that’s being taken seriously by the automotive industry as well as lawmakers. During 2020, we’re likely to see more debate over this aspect of the safety of self-driving vehicles, as the regulatory framework that will allow them to operate on our roads continues to take shape.

3 CONCEREN AND BEST PRACTICES BY GOVERNMENT ORGANIZATIONS FOR MAINTAINING CYBER SECURITY

Ensure that country wide cyber security policies embody the demands of all the consumers and no longer just be central government facilities. Encourage the substantial authorization and use of the Cybercrime Convention with manageable worldwide treaties. There should be support for providing the training of end-users as it may benefits not solely the employee and device, however it further reduces the count of unprotected computers that are prone to hacking by black hat hackers and further used to launch attacks.

Using appropriate authority, setting definite security standards, and licensing to control suppliers in the computer industry to produce verified hardware and software properly. Expand the requirement of a specialist called Forensic Officer which does the investigating and forensic analysis tools. Supporting the International Computer Emergency Response Team (CERT) group, as the most possible means of decreasing or mitigating a large-scale cyber crisis. Fund research in areas such as: secured Internet Protocols, Analysis of risk, Contingency Planning and Analysis of Disaster Propagation and Human factors in Computer Systems [16].

4 APPLICATION OF MANDATORY CYBER SECURITY PRINCIPLES AND TECHNOLOGIES

4.1 Maintaining Access Control and Identity Management

Since the early 1960s the strong username and password combination has been central to computer access control.

4.2 Need for Authentication

Records must be authenticated as coming from a trust-worthy source, and not frequently changed.

4.3 Scanning of Malware

Software which scans for files and applications regularly for malicious code.

4.4 Installing Firewalls

A firewall software can track traffic flowing in and out from a device, and will alarm the user about the unauthorized access and usage.

4.5 Implementing Cryptography

It is widely used in the defense of information in two principal ways. It is best known for providing secrecy by encrypting the data concerning in storage space and in transit. Figure 4 depicts the topmost malware threats [19].
5 POSSIBLE CYBER SECURITY COUNTERMEASURES

Use verified cyber security strategies, customers or employees and organizations can build a strong preparation and response plan to help protect themselves from the vast scope and adverse effects of threats and minimize possible after effects of incidents: making sure that smartphones and other mobile devices have encryption and password features as allowed. Configure operating systems, plugins and other software programs correctly, and patch them. Using firewalls, anti-virus, anti-malware and anti-spyware applications, and update them periodically. Be vigilant with all communications; deliberate before clicking. One should not reveal too much of themselves on social media websites. One could become the object of an identity or property depending on the details they share. One should complain about unauthorized access and activities to Internet Service Providers (ISPs) and local law enforcement agencies.

6 CHALLENGES FACED BY SOCIETY

India’s important infrastructures consist of public and private institutions, which includes the sectors of public health, emergency offerings, management, IT and telecommunications, power, transportation area, banking sectors, and finance. Dependency nature of technology in India also mirrors the fact that India shifts towards a broader area of concern by incorporating aspects of e-governance. Sectors such as income tax, visas for passports are already bought by India so as to merge them into the field of e governance. It is to be practiced by industries like defense and judiciary. The travel industry is heavily dependent on that as well. All Indian banks are using digital way of handling operations and that too on full scale, which further brought in e-commerce and e-banking ideas, too.

7 CONCLUSION

Cybercrime is an extreme, pervasive, violent, rising and increasingly refined crime, and has major indication for national and economic health. Number of businesses, agencies, organizations of the public and private are at a major risk. To businesses and governments alike, to future growth, creativity and competitive advantage, having the Cyber Security policy across all its elements is mandatory. There is not any single technique to success, but corporations will be able to work in the direction of a future world that is both open and safe environment by operating through public and private quarter partnerships and improving safety measures to advancement, particularly in regards to essential systems which have a targeted mission, procedures and applications which might be linked to cyberspace.

REFERENCES

[4] [Online], Cyber Security Strategy of United Kingdom, 2009
[10] The most Important Instruments in fight against Cybercrime, Ch. 6.2
[17] Figure taken from Google images.