# Study of Cyber Security Challenges Its Emerging Trends: Current Technologies

**Veenoo Upadhyay, Dr. Suryakant Yadav**

*Abstract*— **Cyber Security plays a vital role within the field of knowledge technology. Securing the data became one in every of the largest challenges within the gift day. Once ever we expect concerning the cyber security the primary factor that involves our mind is 'cyber crimes' that area unit increasing vastly day by day. Numerous Governments and corporations area unit taking several measures so as to forestall these cyber-crimes besides numerous measures cyber security continues to be a awfully huge concern to several. This paper primarily focuses on challenges visage by cyber security on the newest technologies. It conjointly focuses on latest concerning the cyber security techniques, ethics and therefore the trends dynamical the face of cyber security.**

*Index Terms*— **cyber security, cyber-crime, social media, cyber ethics, android, cloud computing apps**

## I. Introduction

Today man is ready to send associated receive associate sort of knowledge is also an e-mail or an audio or video simply by the clicking of a how ever ton but did he ever suppose however firmly his knowledge id being transmitted or sent to the opposite person safely with none discharge of information? The solution lies in cyber security. These days web is that the quickest growing infrastructure in on a daily basis life. In today's technical setting several latest technologies area unit ever-changing the face of the person kind. However thanks to these rising technologies we have a tendency to area unit unable to safeguard our personal data in very effective method and therefore recently cyber-crimes area unit increasing day by day. These days over sixty % of total business transactions area unit done on-line, thus this field needed a prime quality of security for clear and best transactions. Therefore cyber security has become a modern issue. The scope of cyber security isn't simply restricted to securing the knowledge in IT business however additionally to numerous different fields like cyber house etc.

Even the most recent technologies like cloud computing, mobile computing, E-commerce, internet banking etc additionally desires high level of security. Since these technologies hold some vital info relating to an individual their security has become a requirement factor. Enhancing cyber security and protective essential info infrastructures are essential to every nation's security and economic. Creating the net safer (and protective net users) has become integral to the event of recent services additionally as governmental policy.

Manuscript received August 04, 2018

**Veenoo Upadhyay,** Department Of Computer, Noida International University, Greater Noida (U.P), India

**Dr. Suryakant Yadav,** Department Of Computer, Noida International University, Greater Noida (U.P), India

The fight against cyber crime desires a comprehensive and a safer approach. Providing technical measures alone cannot stop any crime, it's important that enforcement agencies are allowed to analyze and prosecute cyber crime effectively. These days several nations and governments are imposing strict laws on cyber securities so as to stop the loss of some vital info. each individual should even be trained on this cyber security and save themselves from these increasing cyber crimes.

## II. Objectives

1. Safeguard national critical information infrastructure (CII).
2. Respond to, resolve, and recover from **cyber** incidents and attacks through timely information sharing, collaboration, and action.
3. Establish a legal and regulatory framework to enable a safe and vibrant cyberspace
4. Foster a culture of cyber security that promotes safe and appropriate use of cyberspace
5. Develop and cultivate national cyber security capabilities

## III. Methodology And Tools

### 1) Cyber Crime

Cyber-crime may be a term for any criminality that uses a pc as its primary suggests that of commission and stealing. The U.S. Department of Justice expands the definition of cyber-crime to incorporate any criminality that uses a pc for the storage of proof. The growing list of cyber-crimes includes crimes that are created potential by computers, like network intrusions and also the dissemination of pc viruses, additionally as computer-based variations of existing crimes, like fraud, stalking, bullying and coercion that became as major drawback to folks and nations. Sometimes in common man's language cyber-crime could also be outlined as crime committed employing a pc and also the web to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is enjoying in major role in an exceedingly person's life the cyber-crimes additionally can increase at the side of the technological advances.

### 2) Cyber Security

Privacy and security of the info can continuously be prime security measures that any organization takes care. We have a tendency to square measure presently living in an exceedingly world wherever all the data is maintained in an exceedingly digital or a cyber kind. Social networking sites offer an area wherever users feel safe as they act with friends and family within the case of home users, cyber-criminals would still target social media sites to steal personal knowledge. Not

solely social networking however conjointly throughout bank transactions an individual should take all the desired security measures

| Categories of Incidents Case | Quarters | | Percentage (%) |
|---|---|---|---|
| | Q1 2017 | Q2 2017 | |
| Content Related | 16 | 13 | -18.75 |
| Cyber Harassment | 150 | 229 | 52.67 |
| DoS | 14 | 7 | -50 |
| Fraud | 803 | 909 | 13.2 |
| Intrusion | 447 | 523 | 17 |
| Intrusion Attempt | 90 | 71 | -21.11 |
| Malicious Codes | 227 | 225 | -0.88 |
| Spam | 88 | 93 | 5.68 |
| Vulnerabilities Report | 15 | 8 | -46.67 |
| **Total** | **1850** | **2078** | **12.32** |

Table 1: Comparison of number of incidents b/w Q1 2017 and Q2 2017

| Categories of Incidents Case | Apr | May | Jun |
|---|---|---|---|
| Content Related | 2 | 9 | 2 |
| Cyber Harassment | 71 | 119 | 39 |
| DoS | 3 | 1 | 3 |
| Fraud | 265 | 346 | 298 |
| Intrusion | 101 | 138 | 284 |
| Intrusion Attempt | 41 | 22 | 8 |
| Malicious Codes | 62 | 92 | 71 |
| Spam | 30 | 31 | 32 |
| Vulnerabilities Report | 3 | 1 | 4 |
| **Total** | **578** | **759** | **741** |

Table 2: Number of incidents reported in the months of Q2 2017

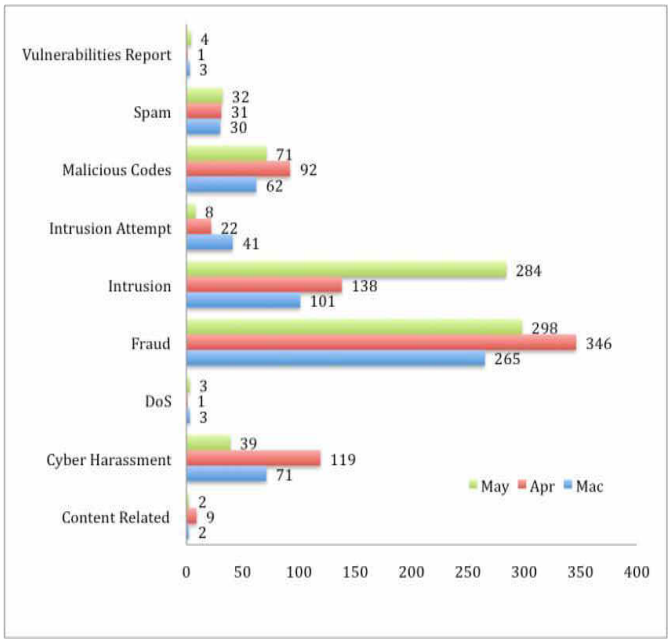


**Figure 1: Breakdown of reported incidents in Apr to Jun 2017**

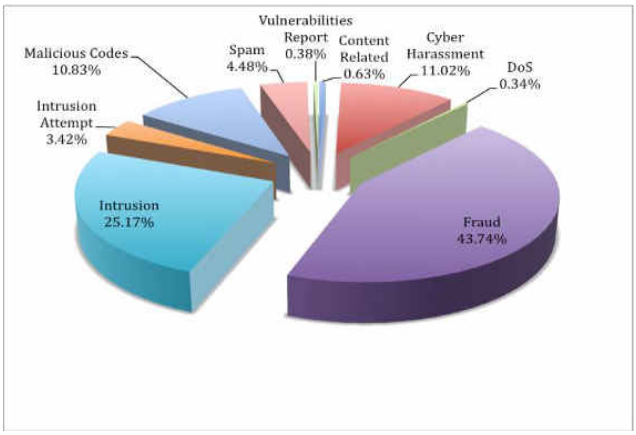


Figure 2: Percentage of reported incidents by classification

The higher than Comparison of Cyber Security Incidents reportable to MyCERT From Apr to Jun 2017, MyCERT from Q3 2017 to Q4 2017 clearly exhibits the cyber security threats. As crime is increasing even the protection measures also are increasing. Consistent with the survey of U.S. technology and care executives nationwide, Silicon Valleya geographic area geographical (region geographic region) Bank found that corporations believe cyber attacks are a significant threat to each their knowledge and their business continuity.

- 98% of corporations are maintaining or increasing their cyber security resources and of these, 0.5 are
- increasing resources dedicated to on-line attacks this year.
- The majority of corporations are getting ready for once, not if, cyber attacks occur.
- Only tierce are utterly assured within the security of their info and even less assured concerning the safety measures of their business partners

There will be new attacks on automaton software package primarily based devices, however it'll not get on huge scale. the very fact tablets share a similar software package as good phones suggests that they are going to be presently targeted by a similar malware as those platforms. the amount of malware specimens for Macs would still grow, though a lot of but within the case of PCs. Windows eight can permit users to develop applications for just about any device (PCs, tablets and good phones) running Windows eight, thus it'll be attainable to develop malicious applications like those for automaton, thence these square measure a number of the anticipated trends in cyber security.

Although external cyber attacks still become additional subtle, the first security threat still comes from insiders. to stay up with the evolving threat landscape, organizations could got to rethink their security methods and are available up with new approaches to attempt cyber security problems. Netwrix predicts that the subsequent trends can play a major role in 2017:

- **Blockchain for IT security:** Blockchain technology allows knowledge storage in a very localized and distributed manner, that eliminates one purpose of failure and prevents hackers from compromising

giant volumes of knowledge. Because of its ability to quickly determine the information that has been manipulated, blockchain could become the core technology for extremely regulated industries, like banking and law.

- **Focus on corporate executive threats:** Netwrix's 2017 IT Risks Survey found that the majority organizations lack visibility into user behavior, that makes them prone to corporate executive threats. the requirement to stay sensitive info secure and forestall corporate executive breaches can force organizations to form additional efforts to ascertain stricter management over user activity in their IT environments.
- **Continuous adaptative Risk and Trust Assessment:** Since protection against behind-the-perimeter attacks isn't decent these days, Gartner suggests an eternal Risk and Trust Assessment Approach (CARTA), that sees security as an eternal method that changes all the time and should be often reviewed. Time period assessment of risk and trust can modify organizations to create higher choices relating to their cyber security posture and mitigate the risks related to aberrant user activities.

### 3) Trends Changing Cyber Security

Here mentioned below square measure a number of the trends that square measure having an enormous impact on cyber security.

#### 3.1 Web servers:

The threat of attacks on net applications to extract information or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate net servers they have compromised. However data-stealing attacks, several of that get the eye of media, also are an enormous threat. Now, we want a larger stress on protective net servers and net applications. Net servers are particularly the most effective platform for these cyber criminals to steal the information. Thence one should always use a safer browser particularly throughout vital transactions so as to not fall as a prey for these crimes.

#### 3.2 Cloud computing and its services

These days all little, medium and enormous firms square measure slowly adopting cloud services. In different words the globe is slowly moving towards the clouds. This latest trend presents a giant challenge for cyber security, as traffic will go around ancient points of review. In addition, because the range of applications accessible within the cloud grows, policy controls for internet applications and cloud services will ought to evolve so as to stop the loss of valuable data. Although cloud services square measure developing their own models still plenty of problems square measure being spoken regarding their security. Cloud could offer Brobdingnagian opportunities however it must always be noted that because the cloud evolves therefore as its security considerations increase.

#### 3.3 APT's and targeted attacks

APT (Advanced Persistent Threat) may be a whole new level of cyber crime ware. For years network security capabilities like net filtering or IPS have contend a key half in characteristic such targeted attacks. As attackers grow bolder and use a lot of imprecise techniques, network security should integrate with different security services so as to sight attacks. Thus one should improve our security techniques so as to forestall a lot of threats coming back within the future.

#### 3.4 Mobile Network

Today we tend to area unit able to connect with anyone in any a part of the planet. Except for these mobile networks security may be a terribly huge concern of late firewalls and different security measures have become porous as folks area unit exploitation devices like tablets, phones, PC's etc all of that once more need additional securities aside from those gift within the applications used. We tend to should always have confidence the safety problems with these mobile networks. More mobile networks area unit extremely at risk of these cyber crimes lots of care should be taken just in case of their security problems.

#### 3.5 IPv6: New internet protocol

IPv6 is that the new net protocol that is replacement IPv4 (the older version), that has been a backbone of our networks generally and also the net at giant. protective IPv6 isn't simply an issue of porting IPv4 capabilities. Whereas sciencev6 may be a wholesale replacement in creating a lot of IP addresses out there, there are unit some terribly basic changes to the protocol which require to be thought of in security policy. thus it's perpetually higher to change to IPv6 as presently as potential so as to scale back the risks relating to cyber crime.

#### 3.6 Encryption of the code

Encryption is that the method of secret writing messages (or information) in such some way that eavesdroppers or hackers cannot scan it. In associate degree secret writing theme, the message or data is encrypted mistreatment associate degree secret writing algorithmic program, turning it into associate degree indecipherable cipher text. This is often typically finished the utilization of associate degree secret writing key that specifies however the message is to be encoded. Secret writing at awfully starting level protects information privacy and its integrity. However a lot of use of secret writing brings a lot of challenges in cyber security. Secret writing is additionally wont to shield information in transit, for instance information being transferred via networks (e.g. the net, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. therefore by encrypting the code one will recognize if there's any discharge of data.

Hence the higher than are a number of the trends ever-changing the face of cyber security within the world.The highest network threats are mentioned in below.
The higher than chart shows concerning the key threats for networks and cyber security

### 4) Role of Social Media in Cyber Security

As we have a tendency to become a lot of social in associate in nursing progressively connected world, corporations should notice new ways in which to guard personal data. Social media plays an enormous role in cyber security and can contribute lots to non-public cyber threats. Social media

adoption among personnel is skyrocketing so is that the threat of attack. Since social media or social networking sites area unit nearly employed by most of them each day it's become an enormous platform for the cyber criminals for hacking non-public data and stealing valuable knowledge.

In a world wherever we're fast to present up our personal info, corporations need to guarantee they are even as fast in characteristic threats, responding in real time, and avoiding a breach of any kind. Since individuals area unit simply attracted by these social media the hackers use them as a bait to induce the knowledge and therefore the data they need. Thus individuals should take applicable measures particularly in handling social media so as to stop the loss of their info. The ability of people to share info with associate in nursing audience of millions is at the guts of the actual challenge that social media presents to businesses. Additionally to giving anyone the ability to spread commercially sensitive info, social media additionally offers a similar power to unfold false info, which may be simply being as damaging.

Though social media is used for cyber crimes these firms cannot afford to prevent victimization social media because it plays a vital role in substance of a corporation. Instead, they need to have solutions which will give notice them of the threat so as to mend it before any real injury is completed. But firms ought to perceive this and recognize the importance of analyzing the data particularly in social conversations and supply acceptable security solutions so as to remain aloof from risks. One should handle social media by victimization bound policies and right technologies.

## 5) Cyber Security Techniques

### 5.1 Access control and password security

The thought of user name and parole has been elementary means of protective our information. This might be one in all the primary measures relating to cyber security.

### 5.2 Authentication of data

The documents that we tend to receive should be attested be before downloading that's it ought to be checked if it's originated from a sure and a reliable supply which they're not altered. Authenticating of those documents is sometimes done by the opposing virus software package gift within the devices. Therefore an honest opposing virus software package is additionally essential to shield the devices from viruses.

### 5.3 Malware scanners

This is software system that sometimes scans all the files and documents gift within the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses area unit samples of malicious software system that area unit typically sorted along and remarked as malware.

### 5.4 Firewalls

A firewall could be a software package program or piece of hardware that helps separate hackers, viruses, and worms that try and reach your pc over the web. All messages coming into or going away the web withstand the firewall gift, that examines every message and blocks those who don't meet the required security criteria. Therefore firewalls play a very important role in detective work the malware.

### 5.5 Anti-virus software

Antivirus software package may be a bug that detects, prevents, and takes action to disarm or take away malicious software package programs, like viruses and worms. Most Antivirus programs embody an auto-update feature that permits the program to transfer profiles of recent viruses so it will check for the new viruses as presently as they're discovered. An opposing virus software package may be a should and basic necessity for each system.

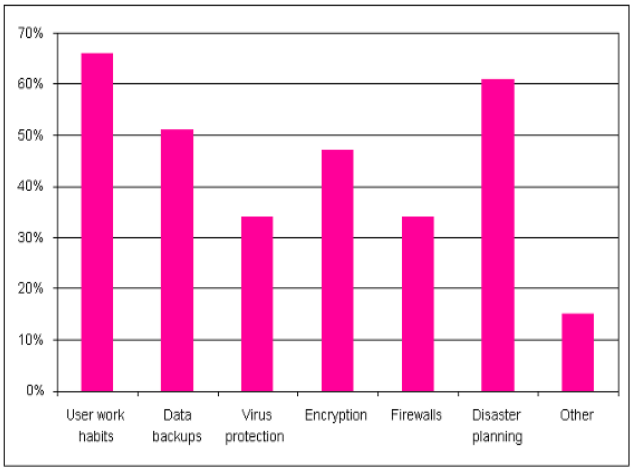


Table II: Techniques on cyber security

## 6) Cyber Ethics

Cyber ethics square measure nothing however the code of the net. Once we apply these cyber ethics there square measure sensible probabilities people victimization the net in a very correct and safer manner. The below square measure a couple of them:

- Do use the net to speak and move with people. E-mail and instant electronic communication create it straightforward to remain in-tuned with friends and relations, communicate with work colleagues, and share ideas and knowledge with folks across city or halfway round the world.
- Don't be a bully on the net. Don't decision folks names, laze them, send embarrassing footage of them, or do anything to undertake to harm them.
- Internet is taken into account as world's largest library with info on any topic in any discipline, therefore victimization this info in an exceedingly correct and legal method is often essential.
- Do not operate others accounts victimization their passwords.
- Never try and send any reasonably malware to other's systems and create them corrupt.
- Never share your personal information to anyone as there's an honest likelihood of others misusing it and eventually you'd find yourself in an exceedingly bother.
- Once you're on-line never fake to the opposite person, and never try and produce faux accounts on different person because it would land you similarly because the other person into bother.
- Always adhere to proprietary info and transfer games or videos providing they're permissible.
- The on top of square measure many cyber ethics one should follow whereas exploitation the web. we have

a tendency to square measure invariably thought correct rules from out terribly early stages constant here we have a tendency to apply in cyber area.

## CONCLUSION

Computer security could be a huge topic that's turning into additional vital as a result of the planet is turning into extremely interconnected, with networks getting used to hold out important transactions. Cyber-crime continues to diverge down completely different methods with every New Year that passes then will the protection of the data. The newest and tumultuous technologies, together with the new cyber tools and threats that return to light-weight on a daily basis, are difficult organizations with not solely however they secure their infrastructure, however they need new platforms and intelligence to try and do therefore. There's no good resolution for cyber-crimes however we must always attempt our maximum to attenuate them so as to possess a secure and secure future in cyber house.

## REFERENCES

[1] A Look back on Cyber Security 2016-17 by Luis coronus – Panda Labs.
*[2]* CIO Asia- Cyber Security MIS-Asia - H1 2017: Cyber security scene in Malaysia, *Dr. Amirudin Abdul Wahab.*
[3] My CERT Analysis of Report From Apr to Jun 2017, MyCERT via its Cyber999.
[4] Cyber Security: Understanding CyberCrimes- Sunit Belapure Nina Godbole.
[5] CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.
[6] https://www.sites.oas.org/cyber/Documents/OAS%20Cyber%20Security%20Journal %202014.pdf. RETRIVED ON: 2016.
[7] http://www.iosrjournals.org/iosr-jce/papers/Vol12-issue2/K01226775.pdf?id=15. RETRIVED ON: 201December 2016.