Study of Latest Emerging Trends on Cyber Security and its challenges to Society

Ravi Sharma

Abstract— Cyber Security plays an important role in the development of information technology as well as Internet services. Our attention is usually drawn on "Cyber Security" when we hear about "Cyber Crimes". Our first thought on "National Cyber Security" therefore starts on how good is our infrastructure for handling "Cyber Crimes" [1]. This paper focus on cyber security emerging trends while adopting new technologies such as mobile computing, cloud computing, e-commerce, and social networking. The paper also describes the challenges due to lack of coordination between Security agencies and the Critical IT Infrastructure.

Index Terms— cyber security, cyber crime, cloud computing, e-commerce, mobile computing, social networking.

1 Introduction

THE Internet is one of the fastest-growing areas of technical infrastructure development [2]. In today's business environment, disruptive technologies such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online [3]. Today more than 80 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions.

The scope of Cyber Security extends not only to the security of IT systems within the enterprise, but also to the broader digital networks upon which they rely including cyber space itself and critical infrastructures [4]. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services [5]. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy [6]. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy.

The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach [7]. Cyber security strategies for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime can help to reduce the risk of cybercrime [8]. The development and support of cyber security strategies are a vital element in the fight against cybercrime [9]. The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively [10].

2 Latest on Cyber Security Issues

Privacy and data theft will be the top security issues that organizations need to focus. We live in a world where all information is in digital form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data.

There will be new attacks on Android operating system-based devices, but it will not be on a massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android [11].

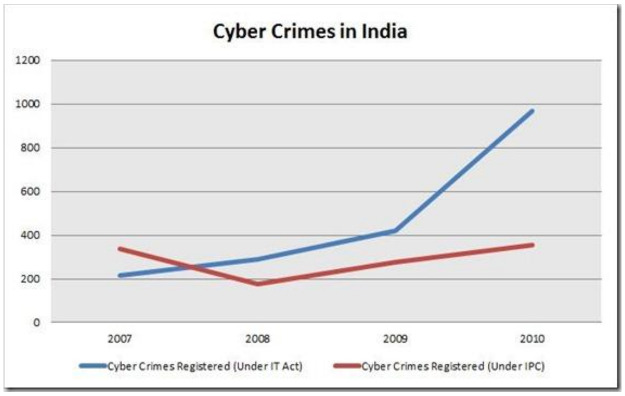

Fig. 1. Cyber Crime in India. (Indian Panel Code, Cyber Crime Registered are doubled from 420 to 966 between year 2009 and 2010) [12].

- ***Ravi Sharma***
  Bachelor of Engineering
  Department of Computer Science and Engineering
  Prestige Institute of Engineering and Science,
  Indore, M.P. INDIA
  PH-91 9926836093. E-mail: ravisharma.india@hotmail.com

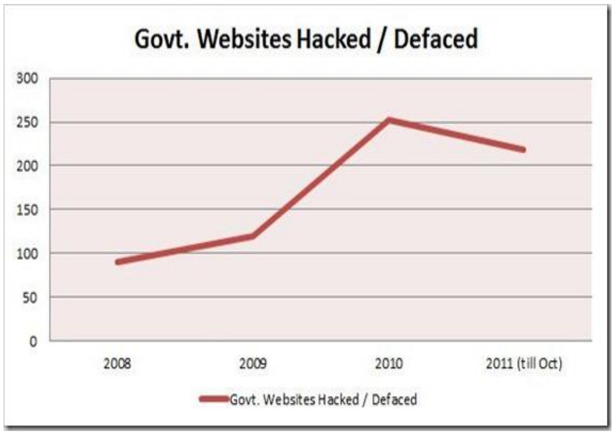

Fig. 2. Government Websites Hacked [12].

3 Recent Survey Issues on Cyber Security Trends

The following list was developed from cyber security research and survey [13] [14] [15].

3.1 Mobile Devices and Apps

The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber attack, as each creates another vulnerable access point to networks. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning.

3.2 Social Media Networking

Growing use of soc media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

3.3 Cloud Computing

More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

3.4 Protect systems rather Information

The emphasis will be on protecting information, not just systems. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house information, more granular control will be demanded - by users and by companies - to protect the data stored therein.

3.5 New Platforms and Devices

New platforms and new devices will create new opportunities for cybercriminals. Security threats have long been associated with personal computers running Windows. But the proliferation of new platforms and new devices - the iPhone, the iPad, Android, for example - will likely create new threats. The Android phone saw its first Trojan this summer, and reports continue with malicious apps and spyware, and not just on Android.

3.6 Everything Physical can be Digital

The written notes on a piece of paper, the report binder and even the pictures on the wall can be copied in digital format and gleaned for the tools to allow a activist-type of security violation, and increasingly this will be a problem.

4 Practices and concern by Governments for Cyber Security

Ensure that national cyber security policies encompass the needs of all citizens and not just central government facilities. Encourage the widespread ratification and use of the Cybercrime Convention and other potential international treaties. Support end-user education as this benefits not only the individual user and system but reduces the numbers of unprotected computers that are available for hijacking by criminals and then used to mount attacks.

Use procurement power, standards-setting and licensing to influence computer industry suppliers to provide properly tested hardware and software. Extend the development of specialist police and forensic computing resources. Support the international Computer Emergency Response Team (CERT) community, including through funding, as the most likely means by which a large-scale Internet problem can be averted or mitigated. Fund research into such areas as: Strengthened Internet protocols, Risk Analysis, Contingency Planning and Disaster Propagation Analysis, Human Factors in the use of computer systems, Security Economics [16].

5 Specific Cyber Security Technologies

5.1 Access Control and Identity Management

The username/password combination has been a fundamental of computer access control since the early 1960s.

5.2 Authentication

Documents need to be authenticated as having originated from a trusted source and that they have not been subsequently altered.

5.3 Malware scanners

Software that is regularly scans files and messages for malicious code.

5.4 Firewalls

A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorized usage.

5.5 Cryptography

It is used in two main ways in information security. The better known is to provide confidentiality by encrypting stored data and data in transit.

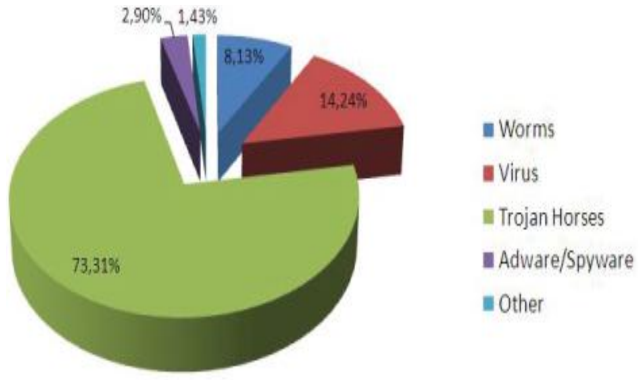

Fig. 3. Percentage of Malware Attacks [18].

6 Possible countermeasure techniques

By using sound cyber security practices, users and organizations can strengthen readiness and response to help defend against the myriad of challenges and mitigate potential impacts of incidents: Make sure that you have encryption and password features enabled on your smart phones and other mobile devices. Properly configure and patch operating systems, browsers, and other software programs. Use and regularly update firewalls, anti-virus, and anti-spyware programs. Be cautious about all communications; think before you click. Don't reveal too much information about yourself on social media websites. Depending on the information you reveal, you could become the target of identity or property. Complain about illegal communication and activities, if found to Internet service Providers and local law enforcement authorities.

7 Key challenges to Society

Our Nation's critical infrastructures are composed of public and private institutions in the sectors of public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance. India's reliance on technology also reflects from the fact that India is shifting gears by entering into facets of e-governance. India has already brought sectors like income tax, passports visa under the realm of e -governance. Sectors like police and judiciary are to follow. The travel sector is also heavily reliant on this. Most of the Indian banks have gone on full-scale computerization. This has also brought in concepts of e-commerce and e-banking. The stock markets have also not remained immune [1].

8 Conclusion

Cyber crime is now serious, widespread, aggressive, growing, and increasingly sophisticated, and poses major implications for national and economic security. Many industries, institutions, public- and private-sector organizations (particularly those within the critical infrastructure) are at significant risk. For businesses and governments alike, getting the Cyber Security posture right across all its elements will be vital for future growth, innovation and competitive advantage. There is no single answer for success, but by working across public and private sector partnerships and by advancing security measures particularly with regard to mission-critical systems, processes and applications that are connected into cyberspace, businesses will be able to work towards a future environment that is both open and secure and prosperous.

ACKNOWLEDGMENT

I thankfully acknowledges to Prof. Jaya Thomas, PhD Scholar, Department of Computer Science, Indian Institute of Technology, Indore. Prof. Rupali Pathak, HOD, Department of Computer Science, Prestige Institute of Engineering and Science, Indore, MP, INDIA.

REFERENCES

[1] Integrated Defense Staff, “National Informatics Center”, Ministry of Defense, India

[2] Yang, Miao, “ACM International Conference Proceeding Series”, vol. 113

[3] Unisys Corporation, “Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security” USA, 2011

[4] Cyber Security Strategy of United Kingdom, 2009

[5] ITU Cyber Security Work Program to Assist Development Countries, 2009

[6] Rev. Jonames Burg, TTU WTSA Resolution 50, 2008

[7] ITU Cyber Security Work Program to Assist Development Countries, 2008

[8] Kellermann, “Technology Risk Checklist, Cybercrime and Security”, IIB-2

[9] Schjolberg/Hubbard, “Harmonizing National Legal Approaches on Cybercrime”, 2005

[10] The most Important Instruments in fight against Cybercrime, Ch. 6.2

[11] Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012

[12] Arun Prabhudesai, “Cyber Attacks In India”, 2011

[13] Audry Watters, Read Write Cloud, RWW Solution Series, 2010

[14] Amichai Shulan, Application Defense Center (ADC), Amicha Regularly Lactures, Security, 2011

[15] Booz Allen and Hamilton, Reports, “Top Ten Cyber Security Trends for Financial Services”, 2012

[16] Peter Sommer, Ian Brown, OECO Project, “Reducing Systemic Cyber Security Risk”, 2011

[17] Figure taken from Google images.

[18] Ammal Security Report, Panda Labs, 2011