CYBER SECURITY AND PRIVACY

Ms. Priyanka
(Student)
Shri Jai Ram Mahila College of Education Research and Development,
Lohar Majra, (KKR)
Email: priyanka.6213.arora@gmail.com
Ms. Rashmi
Assist. Professor of English
SNRL Jai Ram Girls College
Lohar Majra (KKR)
Mrs. Rajneesh
Assist. Professor of Commerce
SNRL Jai Ram Girls College
Lohar Majra (KKR)

Abstract

"It takes 20 years to construct a reputation and few minutes of cyber-incident to ruin it." Computer security or Cyber Security is blend of processes, technologies and practices. The objective of cyber Security is to defend programs, application, networks, computers and data from attack. The five most proficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do make in mind: "Cyber Security is on a large amount other than an IT topic." Cyber security contains controlling physical access of the hardware, application, networks and protecting against harm that may come via networks. We also give various security aspects associated with cyber security. Cyber Security plays an essential role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. Various Governments and companies are taking many procedures in order to prevent these cyber crimes. This paper over all focuses on challenges face by cyber security on the latest technologies .It also focuses on latest cyber security techniques, ethics and the trends shifting the face of cyber security. It explore how challenges for cyber security are also challenge for retreat and data security, considers how cyber security policy can affect privacy, and notes how cyberspace governance and security is a global concern. Finally, it sets out key policy directions with a view to generating dialogue on cyber security as a crucial element of online privacy protection.

Keywords: Cyber Security, Cyber Attacks, cyber ethics, social media, cloud computing, android apps.

INTRODUCTION

Concept of Cyber security: Cyber security, referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. In recent years, governments and corporations have increasingly relied on cyber-security sys-Terms to protect against increasing threats on networks, devices, and organizational and personalInformation. These systems prevent adversaries from breaking into networks and devices, fromsabotaging digital activity, and from accessing private information. At the same time, by monitor-ing networks and computing devices, cyber-security systems ultimately a ■ ect individuals' privacy.

Being one of the most rapidly expanding sectors, internet has become one of the most essential parts of our life from work to entertainment there's no other option now but it comes with a price of our privacy. Cyber-security systems, which defend networks and computers against cyber attacks, are becoming common due to increasing threats and government regulation. At the same time, the significant amount of information gathered by cyber-security systems poses a serious threat to the privacy of the people protected by those systems. Cyber Security combined form involving to information and technology, the internet, and virtual reality. The term cyber security is used to referto the security existing through on-line services to protect your online information. Itadditionally refers to the technologies andplans designed to secure computer systems,computer networks and information fromunauthorized access, susceptibilities andattacks delivered though the internet. Cybersecurity is an all-encompassing domain ofinformation technology it comprises the whole set of security-related technologies.Cyber Security crime includes: Internet Fraud, Spam, Cyber bullying, Gathering Information illegally, Identity theft, Phishing scams and hate Crimes. In many cases, the monitoring system can draw the identities of users and access sensitive information. For instance, many enterprise cyber-security systems monitor IP addresses that can be easily traced back to a particular personality. Moreover, the user's device identification on mobile devices is often accessed by cyber-security applications. Therefore, while cyber-security mechanisms protect individuals from attacks from hackers and other third-party adversaries, they also create new vulnerabilities for privacy disobedience from the entity that runs the cyber-security system.

CYBER SECURITY CHALLENGES

A report from the World Economic Forum released in January 2014 examines the need for new approaches to increase resilience against cyber attacks and suggests that the failure to effectively secure cyberspace could result in an aggregate impact of approximately US$ 3 trillion by 2020.18 However, many of the challenges for cyber security are also challenges for privacy and data protection. Cyber security is by no means a static issue with a permanent solution. Threats to information in cyberspace evolve quickly and, more recently, have expanded into new channels such as social media and mobile technologies. As organizations strive to keep pace with the changing landscape created by innovative technologies, social practices and ever-changing threats, data produced, collected and collated on a massive scale can be left vulnerable to those cyber threats. The following are some of the emerging challenges for data protection and cyber security

a) Complexity of the connected environment The continuing evolution of cyberspace, as a fully electronic world created by interconnected networks in parallel with our physical environment, is characterized by an enormous amount of data. The modern economy increasingly depends on vast quantities of digital data that are generated through financial transactions, communications, entertainment, travel, shopping, online browsing, and hundreds of other routine activities. Data elements are continually being combined, connected, compared and linked to other information as organizations try to capitalize on its value and to offer new and improved services to their users. The electronic systems and digital networks that facilitate these transactions and communications also capture our preferences and other personal details, and track our online and, increasingly, physical movements. The volume of data generated in cyberspace can only increase exponentially once the "Internet of things" becomes a reality, and sensors within devices autonomously report on location, status, and surrounding environment, provide real-time updates or help monitor and control devices remotely.

b) Growing sophistication of the threat online threats may be invisible but their effects are very real, and interconnected systems that are globally accessible are inherently vulnerable. As the scale of information flowing through cyberspace has expanded, so too has its value to corporations, government, and those with malicious intent. Our data trails now leave a larger footprint across cyberspace, leaving us more exposed to threats. Wherever there is an opportunity to profit there is usually a market for criminal activity, but as Gabriella Coleman notes, there has also been a "professionalization" of hacking and cyber-crime, making these activities much more sophisticated. State sponsored threats, conducted or condoned by a nation state, are also becoming increasingly common. These are sometimes referred to as Advanced Persistent Threats (APTs) and are usually well educated, well-resourced adversaries who focus on the theft of secrets including intellectual property.

c) Threats are moving to the mobile sphere in the next three years, the number of cellphones in use will exceed the global population. Our mobile devices can contain a goldmine of personal information. People routinely carry their mobile devices everywhere and use them for almost anything imaginable; people communicate with friends, access email, take photos and video and upload it to the web, play games, track distances, locate nearby stores and restaurants, find directions to specific locations, access their bank accounts, surf the web, monitor their health/physical activity, keep track of appointments or log to-do lists. Organizations are all striving to reach consumers and clients on the devices they use every day, but alongside all of these conveniences for the consumer is the possibility for new vulnerabilities or opportunities for cyber threats

d) Compliance vs. risk-management Organizations are required to comply with various laws and regulations in order to operate in particular jurisdictions or across various jurisdictions. When it comes to security, however, a mechanical approach to compliance does not necessarily mean that the organization is secure. In fact, blindly pursuing compliance may actually put an organization at increased risk specifically because it is focused on a "check-the-box" compliance model leading to a false sense of security, whereas performing proper risk management requires organizations to scour and identify areas where additional safeguards are needed. A risk management approach naturally complements compliance obligations. The challenge for organizations is to understand that security is not simply a matter of meeting minimal compliance standards, but rather, a question of engaging in effective risk management and dynamic implementation of security.

CYBERSECURITY INTERETS

To succeed with the implementation of efficient IoT security, we must be aware of the primary security goals as follows Cybersecurity Interests

a) Consumer Cybersecurity Interest

Online consumers have been victimized by cyber-threats in the form of spyware; malicious computer viruses, worms, or malware; and fraud or abusive sales tactics that lure consumers to invest in bogus products or services. Online consumers routinely fall victim to identity theft, as well as spam, phishing or harming attacks.

Consumers are also facing the challenge of determining which products or services to trust to provide goods and services as advertised.

b) Political Advocacy and Academic Cyber security Interest

For individuals and organizations that rely on the Internet for research, access to information, collaboration, political participation, fundraising, coalition building, campaigns, advocacy, organized dissent, political speech, watchdog actions against government and businesses, freedom of expression, dissemination of information or for outreach to constituencies--cyber security does matter a great deal.

Threats posed to political activity include deceptive campaign tactics that deface Websites, target donations for theft, create denial of service attacks on Websites, or send messages that are deceptive or misleading regarding the rules for voter participation on Election Day. If responses to cyber-attacks deny advocates access to the Internet and/or advanced communications networks, this would deny them the means to engage in a wide range of activities that could include election protection efforts during public elections, mobilize supporters for public protests, educate consumers, or empower constituencies to know and understand policy that impacts their lives. Academics and researchers must have a trustworthy and reliable means of exchanging ideas, participating in discussions, and collaborating on projects that advance their areas of research interest.

c) Business Cyber security Interest

Large and small companies have cyber-threats within and outside of their control such as data breaches, theft of company secrets, spying, attacks on computer networks, and damage to critical systems. Many companies are considering the challenges of cyber security and looking to new business applications such as cloud computing to secure data. However, cloud computing has enormous security and privacy risks relating to dependence on untrustworthy or unevaluated third parties.

New business and government services such as electronic health records and development and updating of critical infrastructure such as the Smart Grid each offer new cyber security privacy challenges for consumers.

d) National Security Cyber security Interest

The cyber-threats to any nation can range from disruption of an agency's networks or information services to the public to cyber-warfare. Depending on the agency, type of cyber-attack, its scope, duration, and effectiveness, the consequences for the online and offline operation of local, federal, or state government components can range from annoying delays in communications to serious damage to infrastructure threatening life or property.

Cyber-attacks or incidents that threaten the command and control structure of the national government or its assets including national defense, emergency response, and economic systems are of growing concern. The digital infrastructure of the nation must be treated as a strategic national asset. The new mission is to deter, detect, and defend against disruptions and attacks of all descriptions.

CONCLUSIONS

Emerging scenarios provide useful insights into the future of security and privacy. While previous predictions are diverse in their scopes and audiences, through constructing representative futures, we explored those developments most frequently-anticipated. Our study of the impact on individuals, organizations and nations highlights key considerations for these important stakeholders. We also analyzed existing frameworks and best practices, identifying guidelines which do not adequately translate to future predictions. Our findings suggest avenues for research and development, including privacy education for the general public, approaches to mitigate organizational insider threat, greater investigation of BYOD risk, and international legislation for cyber warfare. It is crucial that emerging scenarios are explored in anticipation of the security and privacy threats of the coming decade. We have considered a number of possibilities for future work. Firstly, we could conduct a technical analysis of why reputable guidelines fail to address the threats from emerging scenarios. In this work, we could rigorously examine individual sections in 'best practice' documents and identify which areas urgently require updating. Secondly, these emerging scenarios could be explored within the context of specific domains, such as healthcare. The pervasion of the Internet-of Things might be beneficial with the development of wireless sensors, but also threaten welfare when critical devices are compromised. Similarly, although advances in big data might revolutionize the detection of health conditions, these measures could unfairly increase insurance premiums for victims of profiling. Finally, we could expand our scope and explore future possibilities for technology as a whole. The coming decades promise to radically change how we perceive digital devices, and it is crucial we are prepared for these novel developments.

REFRENCES

a) World Economic Forum report on Risk and Responsibility in a Hyper connected World, released January 20, 2014

b) Center for Applied Cyber security Research, Indiana University. Roundtable on Cyber Threats, Objectives, and Responses: A Report. December 2012.

c) Business Insider "Everything You Need To Know About The New Internet—The 'Internet Of Things', Julie Bort, Published March 29, 2013. Accessed online October 7, 2013 at: http://www.businessinsider.com/what-you-need-to-know-aboutthe-internet-of-things-2013-3?op=1#ixzz2h3ge4p7R.

d) Discussed in an Interview with Ron Deibert, found at: http://ww3.tvo.org/video/193823/ron-deibert-surveillingcyberspace.

e) "Hacking" is the commonly used term, however the technically correct term is "cracking" - a shortened form of "criminal hacking". Hacking, in the original sense of the word, is figuring out how things work. Where the term "hacking" is used throughout the paper, it is meant to refer to criminal hacking activities, aka "cracking". For more on hacking, see the work of Gabriella Coleman; in particular, Politics and Publics http://gabriellacoleman.org/wpcontent/uploads/2012/08/Coleman-hacker-politics-publics.pdf or Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism at http://steinhardt.nyu.edu/scmsAdmin/uploads/003/679/255.pdf.

f) Google Big Tent Canada 2013, Google Demonstration: Cyber security in Action. May 30, 2013.

g) Ibid.

h) 'Study of the Impact of Cyber Crime on Businesses in Canada.' International Cyber Security Protection Alliance (May 2013) p. 33.

i) 'Canada and Cyberspace: Key Issues and Challenges' (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT).

j) Info Security "Gartner Says Risk-Based Approach will Solve the Compliance vs Security Issue," published August 8, 2013.

k) J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in IEEE Security and Privacy Workshops (SPW), 2014, pp. 214–228.

l) International Telecommunication Union, National Cyber security Strategy Guide, 2011.