International Cooperation to Enhance Website Security

Mannomhan Chaturvedi  
Director, Curriculum and Pedagogy  
CISO Academy  
Gurgaon, India  
m.chaturvedi@cisoacademy.com

Srishti Gupta  
MS, Software Engineering  
VIT University  
Chennai, India  
srishti.iitd@gmail.com

Abstract—Websites are critical for any organization whether in public or private domain to reach out to the consumers of e-governance or e-commerce. The privacy of the consumer data and security of the online transaction has been an area of concern. Web based attacks and web application attacks are on the rise. In this paper we analyze the international context and options to minimize cybercrime.

Keywords—Website security, Secure online transactions, Privacy & security of consumer data, International cooperation

I. INTRODUCTION

Digital infrastructure is the substrate of the modern society. The networked society would achieve the potential efficiency gains only if this infrastructure is reliable and secure. As the internet and web technologies have advanced from the pure information-sharing phase to interactive, transactional, and intelligent or integration phases, many states and nations, like business corporations, see opportunities of offering web-based government (e-government) services for improving government efficiency, transparency, and competitiveness in the global economy [1].

The sharp uptake of e-government services on the internet has also brought with it security threats. Certain government websites have been observed to post citizens' names, social security numbers, property tax records, or other private information on the web without requiring user login ID and password. Cyber attackers have matured from nuisance and destructive attacks towards activities motivated by financial gains.

II. WEB BASED THREATS TO THE PRIVACY AND SECURITY OF USER DATA

A. Privacy Policy

In the current times when there are growing discussions globally regarding the privacy of users and safety of his/her details, it is important to have a privacy policy in place so as to make the citizen user confident about the safety of his/her personal information as well as keep informed about the conditions when such information can be shared with the relevant authorities.

A privacy policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data. Personal information can be anything that can be used to identify an individual, not limited to but including; name, address, date of birth, marital status, contact information, ID issue and expiry date, financial records, credit information, medical history, where one travels, and intentions to acquire goods and services. In the case of a business, it is often a statement that declares a party's policy on how it collects, stores, and releases personal information it collects. It informs the client what specific information is collected, and whether it is kept confidential, shared with partners, or sold to other firms or enterprises.

Privacy policy is important to the modern state, because grounded in it is the individual's physical and moral autonomy. For this reason, it is worthy of constitutional protection. The exact contents of a privacy policy will depend upon the applicable law and may need to address requirements across geographical boundaries and legal jurisdictions. Most countries have their own legislation and guidelines of who is covered, what information can be collected, and what it can be used for.

In general, a privacy policy is a statement of several paragraphs long explaining to the site users and customers exactly how their information will be used. It also details what information is tracked and how it is tabulated. In today's world of trying to be anonymous and expecting privacy from outsiders, the privacy policy is that much more important to many website users and online customers.

One of the main reasons a website needs a privacy policy page is to disclose the owner's intent. People have a right to know what information is being traced behind the scenes, and what the owner plans to do with that private information. For example, does the site owner collect IP addresses to establish a database of user habits to sell to other organizations? Does the site owner request addresses with the express purpose of selling the list, or are the email address provided for a legitimate purpose, such as sending existing customers relevant information about product issues and upgrades?

Policy statement pages are particularly useful and are actually required by law in many jurisdictions for sites that operate businesses for catalogues and online shopping. Users must be made aware that when they purchase goods and services, that their purchases are conducted in a secure and safe environment. Further, they must be assured that their personal data such as home addresses, telephone numbers, and credit card information will not be used in any way other than to ship
goods and bill for the products. Companies are not permitted to sell private information and must always disclose any mailing lists upon which customers will be placed as a result of purchasing.

Another reason for a policy statement is to notify users that some pages may take them away from the existing website. If users choose to follow links to other resources or to outside pages, then they must understand that the privacy policy from the original site is no longer in force, and that they should read the terms of use of the website where they landed. In addition, users should know that any banners or third party advertisements will take them away from the originating site.

Today, one of the biggest reasons for a policy statement is to acknowledge to users the fact that either the website owner or third party advertisers may drop cookies, which may track information about the users’ online habits. For many online businesses, cookies serve a legitimate purpose in that they save users time from logging into sites every time they visit them, and cookies allow information about their accounts to be stored for easy access. But, some advertising companies want to know more about the users. Either way, the use of cookies must be disclosed and the reason for the cookies must be apparent.

Finally, policy statements are mandated by some companies with which the website owner does business. Because privacy is a sensitive issue for many people, often companies will not do business with those that try to hide behind the cloak of the internet. Examples are affiliate programs. The program managers want to be sure that the affiliates are doing business in an open and honest environment. They do not want their customers deceived, and they do not want their reputations degraded. In order for affiliates to participate in certain programs, they must be upfront about the third party ads and the possible existence of cookies. They must explain that the cookies may track web traffic in an attempt to offer targeted advertisements to certain individuals. As a result, the users must have the option to decline the use of cookies, and may opt out of the activity altogether.

Government websites need to follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. Website should solicit only that information which is absolutely necessary. As per many government guidelines, in case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom. Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor’s system during the process and what shall be the purpose of the same.

In this era of cyber crimes and cyber threats it is very important to have certain procedures in place which are acknowledged by renowned certifying agencies. They are required to get audited by agencies empanelled by a government agency. Indian government guideline to Indian government websites enumerates that if a Department’s website allows E-Commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

Web Application security is of paramount concern to owners as well as consumers of the website. A lot of security threats are handled at data centres and server administrator level where the application is hosted. Application developers should however be sensitive about security aspects, as a lot of security threats arise due to vulnerability of application software code. These application driven attacks sometimes turn out to be quite fatal. Best Practices to follow while developing web applications using various technologies are available on CERT-IN website as well as in internet space. Some of the key features of the NIC guidelines include: security audit from empanelled agencies for each website/application; formulation of a security policy by Department to address various security risks/threats; etc.

III. INTERNATIONAL EFFORT TO CONTAIN CYBER CRIME

The past two decades has witnessed a number of initiatives by international bodies like; the Organization for Economic Cooperation and Development (OECD), Council of Europe (COE), G-8, European Union, United Nations [2], and the Interpol, which recognized the inherent cross border reaches of cybercrime, the limitations of unilateral approaches, and the need for international harmony in legal, technical, and other areas [3].

IV. CHALLENGES OF SECURITY IN CYBERSPACE

According to [4] the security issues raised by cyberspace pose special challenges to those wishing to bring it into a classic international security framework. These special features pertain to four aspects viz. actors, attribution, authority and activity.

A. Actors

A key challenge of cyberspace is that it is populated by both state and non-state actors. An additional problem is that these two categories of users are not readily identifiable. It is for the sovereign states to ensure that non-state actors within their jurisdiction respect the law, including international legal obligations that have been incorporated into national law. The cyber criminals or terrorists residing in a country A and targeting victims in another country B while insulated from direct action of law enforcement agencies of country B are still the responsibility of the country A in terms of any collaborative treaties signed between the two countries. To achieve effective implementation very close, proactive and flexible interaction between law enforcement agencies of the two signatories is essential. The matrix becomes more involved when the number of member states increases and the ecosystem should evolve to bring in transparency amongst all stakeholders.

B. Attribution

The verification tools of the International Monitoring System of the Comprehensive Test Ban Treaty Organization
(CTBTO) were easily able to detect the nuclear tests by North Korea in 2006 and 2009[5] and led to necessary international response. In cyberspace, however, a cyber attacker can hide himself readily, and even disguise his attack to appear to originate from a third party. The problem of attribution for a cyber-action is clearly one that will complicate any effort at security controls. Uncertainty about attribution will also constrain retaliatory action. The current level of research in reliable attribution is not adequate. The cyber crime treaties cannot be implemented unless trust exists between signatories that best efforts are being put to identify the criminals and therefore, transparency is first precondition for success.

C. Authority

The designation of a state agency that would lead the response to an international cyber-attack would depend on the nature of the attack. The vast majority of hostile cyber-activity originates with criminal elements, for which law enforcement agencies are normally responsible. A response to use of the Internet by terrorists might entail pooling resources from both the national security and law enforcement communities. The fact that hostile international cyber-activity is not exclusively or even predominantly a national security phenomenon adds a further complication to the development of internationally acceptable approaches for regulating or policing such activity. International collaborative initiative for countering cybercrime; the 2001 Budapest Convention on Cybercrime by the Council of Europe has run into road blocks in absence of mutual trust and attempts to erect barriers to the operational procedures (remote log in to the suspected computer systems)considered crucial for timely collection of the evidence, which is in any case very fragile.

D. Activity

Hostile international cyber-activity, as already noted, can be perpetrated by state or non-state actors. Within state actors too, the military and intelligence arms of nation states operate under different norms. Intelligence agencies of all countries with means and capacity will keep tabs on adversaries and on activities they perceive as threats. No international agreement or legislation will change that. When such attempts to spy are exposed, as by Snowden, there will be a degree of furor and then it will be business-as-usual [5].

V. THE POSSIBLE OPTIONS

A. Necessity for a review of the cyber space use

Considering the above four special feature of cyber domain that seem to discourage international treaties to combat cyber crime and terrorism, we conclude that bilateral and multilateral trust and transparency amongst signatories is a precondition for success. All nations have to realize that dual use of cyber space for commercial and military use is fraught with unacceptable risks. If we look at the international treaties[4]for Nuclear Weapons, Chemical Weapons Convention, Biological and Toxin Weapons Convention, Outer Space Treaty of 1967 prohibiting the placement of weapons of mass destruction in outer space and the militarization of the Moon and other celestial bodies and more recently, the Ottawa and Oslo treaties banning anti-personnel landmines and cluster munitions respectively, as precedence, there is hope for international cooperation in cyber space. The efficiency gains provided by the cyber domain are very valuable for mankind and using them for mutual destruction would be a serious folly.

Once all nation states share this common perception, combating cyber crime and terror would not be an impossible mission. The Budapest Convention(Council of Europe (COE) convention on cyber crime- 2001) was a good attempt to seek international cooperation to harmonize the law enforcement efforts of all nations against cyber crime. However, lack of trust and international political compulsions to use the cyber domain for projecting the state power have sabotaged this potential collective action against cyber crime. With the development of new technologies such as cloud computing, “smart” phones and social media, as well as the emergence of botnets and the expansion of encryption, the Budapest Convention requires updating [6] before being ratified by all nations.

We need to realize that the state actors particularly militaries and intelligence agencies would certainly be using the ICT networking technologies for achieving the efficiency gains in their core activities. It is important that their ICT networking infrastructure is protected from; non-state actors viz., criminals/ terrorists and competing state actors viz. militaries and intelligence agencies. Use of the commercial internet technologies for such segment is fraught with risk and therefore, there is a case to evolve hardened systems for such niche groups.

B. Role of deterrence in combating cyber crime and terrorism

Deterrence theory can be applied to all cyber crimes including cyber terrorism [7] [8]. The impact of deterrence (deterrence effect) is positively correlated with the identification probability, and it also may be positively correlated with punishment level. Keeping the potential punishment severity unchanged, the deterrence effect will be determined by the identification probability. The identification probability depends upon the capability to track cyber terrorists[9]. Thus, to increase the impact of deterrence on cyber terrorism, the identification probability must be increased. An inability to track cyber terrorists would make it difficult for local and international jurisdictions to track the entire network of cyber terrorists as well as to prosecute them due to the lack of proof of identification of these cyber terrorists. The potential adoption of a new variant of Cyber Crime and Terrorism convention by all nations would provide the eco-system that may put the criminals and terrorists under pressure and increases the success probabilities of the international law enforcement agencies.

VI. CONCLUSION REMARKS

This paper has attempted to unveil the underlying reasons for the rising cybercrime. Race for dominance has prevented the nation states to see the logic of unrestricted international collaboration to combat Cyber crime and terrorism. The peaceful use of cyber domain for the good of mankind offers unimagined opportunities. The common enemies for all nation states are cyber criminals and terrorists. The collaboration with adequate trust and unrestricted access to the law enforcement agencies across the national boundaries would certainly mitigate this transnational menace.
REFERENCES


