Bangalore Cyber Security Summit 2009
NIMHANS Convention Center
October 8th and 9th, 2009
Organized by

Department of IT and BT, Government of Karnataka
KEONICS

Supported by
NASSCOM, DSCI, Mandamus, Cyber Law College, CSI, DSFI and Karnataka Police

Summary of the Recommendations made at the Summit

Prepared by a Committee which included the following persons

Naavi
Pavan Duggal
Sateesh Kannegala
Iqbal Ahmed
Kishan
Pratap Reddy

The Bangalore Cyber Security Summit 2009, held at NIMHANS Convention Center on October 8th and 9th deliberated on various issues related to Cyber Security in India and several eminent speakers from India and abroad presented their views through Panel discussions and lectures.

Some of the views expressed in the summit resulted in certain suggestions on the improvements that can be brought into the ITA 2000 and Security measures indicated there in. Several other suggestions having relevance to Cyber Security and Privacy issues were also made by the participants.

These recommendations have been briefly collated in this recommendatory note into two categories namely

a) Cyber Law Issues
b) Others

Cyber Law Issues

The summit recognizes that the amendment to Information Technology Act 2000 has been effected with the Information Technology Amendment Act 2008 passed on December 22 and 23, in the Parliament and assent of the Indian President granted on 5th February 2009. The rules and regulations under the Act are now being drafted by the relevant departments of GOI and on finalization of the same the Act will be notified for its date of effect.

The Summit was of the view that the amendments (ITA 2008) had many positive features and the delay has held back important changes such as the definition of "Cyber Terrorism" and hence it needs to be expeditiously notified.

Some of the positive features of the ITA 2008 which the Summit took note of were,

i. Enabling non PKI based Authentication methods (Electronic Signatures) in addition to the current form of Digital Signatures.
ii. Increase of offence sections from 10 to 22 and Recognition of new Offences including Cyber Terrorism, Sending of Offensive Messages etc
iii. Removal of the upper limit on Civil liabilities that can be claimed under Section 43.
iv. Introduction of Civil Courts into the system of providing compensation for damages where the claim is more than RS 5 crores
v. Adding of "Diminishing the Value of Information" under Sec 43 and widening the scope of Section 43
vi. Integration of Section 66 with Sec 43 to provide better clarity.
vii. Introduction of e-auditing as per Section 7A
viii. Introduction of Data Protection provisions under Section 43A and Sec 72A
ix. Introduction of Government Digital Evidence Examiner
x. Clarification on Compounding and Cognizability.
xi. CAT being made a multi member body so that a technically qualified person can be part of the tribunal.
xii. Introduction of a responsibility for Retention of Data
xiii. Making Police investigations possible at Inspector Level.

The Summit also had a few concerns which it wanted to record. The Concerns

1. Responsibility of Controller of Certifying Authority as a Repository of Digital Certificates removed and shifted to the Certifying Authorities (Deletion of Sec 20)
2. All Offences being made "Bailable" as per Section 77B makes it easy for the offender to erase evidence and reduces the deterrence value of the penal provisions. The need to satisfy pre conditions such as "Dishonesty" and "Fraudulently" for invoking Sec 66 also makes it difficult for the law enforcement to file cases.
3. Inclusion of "Browsing" and "Seeking" in Sec 67B where the offence is cognizable and the term of imprisonment is 5 years is amenable for abuse.
4. Powers vested with the CERT-In amenable for abuse if not balanced with appropriate protection of the rights of Netizens.
5. The Intermediaries donot have adequate responsibility for security and in the emerging practice of using of Proxy IP addresses in e-mail and other http communications, can cause hurdles for investigation.

The Summit has taken note that the Bill has been already passed and only notification of rules is now pending. Hence any changes are now considered possible only to the extent the power to make rules permits. It is understood that the rules cannot be ultra-vires the act and hence the changes if any can only relate to the procedures for application of the provisions.

In view of the above, the following suggestions are being made:

1. Though the Controller of Certifying Authority is now not required to maintain the repository of Digital Certificates, as a part of the "Reasonable Security Practices" for the Certifying Authorities, it is suggested that the Certifying Authorities archive their repository and revocation list on a real time basis with CCA and the same shall be made available for the public for cross verification with the lists maintained by the individual Certifying Authorities.

2. No bail shall be granted without a proper order of an appropriate Court where the amount of security deposit for the bail is less than the maximum fine prescribed under the relevant section.

3. The section 67B which makes "Browsing" and "Seeking" information which depicts children in obscene or indecent or sexually explicit manner an offence with an imprisonment of 5 years should be omitted from being notified for the time being since the Act permits non notification of certain provisions. A separate step can be taken subsequently to remove "Browsing" and "Seeking" from the section through a process of further amendments. In the meantime Section 67 A will cover the Child pornography issue to some extent.

4. To address concerns arising out of the powers under Sections 69, 69A, 69B, 70B the Summit recommends some measures which supplements the system of review presently suggested in the rules, with the formation of a "Netizen Rights Advisory Committee" with participation of NGOs and Private Persons of eminence to resolve conflicts that may arise in the implementation of the powers of interception, monitoring etc.

5. Cyber Law awareness should be made mandatory in all Intermediaries for the employees with a suitable system of audit and reporting for confirmation.

6. In Cyber Café regulations,
   - **a.** registration, licensing must be made mandatory and
   - **b.** conditional to
     - **i.** Cyber Law training of the owner,

ii. implementation of ID verification through a robust system,
iii. confirmation of ID verification each time a user is provided access along with the record there of,
iv. provision for recording select activities of the user which will be retained for a minimum period of 3 years, with appropriate back ups and DRP systems as well as privacy related protections.
v. Enabling of authorized law officer's access to stored data with appropriate permissions and activity logging.

7. Making all e-mail providers and Intermediaries provide IP address resolutions to authorized investigating officers without need for time consuming formalities while at the same time maintaining accountability of the investigating officers for the proper use of the authority.
8. Providing Reasonable Security in Internet based services including Banks should be the responsibility of the service provider and he should assume responsibilities for technical failures of the system and providing a security warranty.
9. The period for which data needs to be retained under Sec 67C has to be adequate to meet the requirements of law enforcement. It is suggested that the minimum retention period can be specified as 3 years for all intermediaries and 5 years for all Banks and Financial Organizations.

Others:

10. Summit recommends that the Government of India should record its opposition to ICANN which intends allowing registrars of domain names to allow "Privacy" and Proxy" registrations. Such a measure will seriously limit the legal rights of Indian Citizens to take action against owners of foreign websites who transgress Indian law and also seriously affect the investigative capabilities of the Police. Since ICANN has requested for public comments on the proposal which is to be provided before November 2nd, an immediate action on this is recommended to be initiated.
11. A serious concern has been exercised on the mobile companies protecting the data related to the customers. Some summit members expressed that the mobile companies may use the data of one customer to issue multiple connections which are then traded to others. To prevent this possibility, it is suggested that under the reasonable security practices for mobile companies, a provision should be made for adoption of OECD model of privacy protection which should provide a right for the data owner to ensure that no other account has been created by the mobile companies with his ID data. In order to ensure this, a name and address based search should be provided by all mobile companies so that a genuine citizen can check if his ID has been used only for his accounts and no body else.
12. Effective security at home computers using Internet should be ensured by increasing the responsibility of the ISPs providing internet connection to educate and obtain an undertaking from the account holder that he is aware of the Cyber Security implications of owning the Internet account.
13. In the reasonable security practices to be prescribed for ISPs, they should be made responsible to identify known spam and phishing mails and suitably tag them and or remove them before delivery to the recipient.

Rationale for the Recommendations
(Not submitted with the recommendations during the Summit)

No	Recommendation	Rationale
1	Though the Controller of Certifying Authority is now not required to maintain the repository of Digital Certificates, as a part of the "Reasonable Security Practices" for the Certifying Authorities, it is suggested that the Certifying Authorities archive their repository and revocation list on a real time basis with CCA and the same shall be made available for the public for cross verification with the lists maintained by the individual Certifying Authorities.	Digital Certificate holders require a reference site from which the certificates issued and revoked can be verified for evidentiary purpose. CAs are private sector companies. In case of any errors or omissions, the public would be put to difficulty. Hence it is necessary for statutory authority to maintain the registers. This will also act as a back up.
2	No bail shall be granted without a proper order of an appropriate Court where the amount of security deposit for the bail is less than the maximum fine prescribed under the relevant section.	Some of the legal experts have suggested that availability of bail would reduce the deterrence effect of the penal provisions since the conviction rate is any way is expected to be low. Also if bail is granted immediately, the possibility of evidence being tampered with by the accused is also high since Police may not be able to secure all the evidence in a short time. Hence some experts have been critical of amendments and dubbed them as ineffective for prevention of Cyber Crimes. As a partial remedy, it has been suggested that the financial barrier for obtaining the bail may be raised.
3	The section 67B which makes "Browsing" and "Seeking" information which depicts children in obscene or indecent or sexually explicit manner an offence with an imprisonment of 5 years should be omitted from being notified for the time being since the Act permits non notification of certain provisions. A separate step can be taken subsequently to remove "Browsing" and "Seeking" from the section through a process of further amendments. In the meantime Section 67 A will cover the Child pornography issue to some extent.	Since the act has already been passed, it is not very practical to change the law at present. It can be attempted only in the next amendment. At the same time this provision is considered too threatening since many Viruses and Trojans can cause automatic display of child pornography in the computer operated by an innocent user. Hence the suggestion to withhold the notification of the specific section.
4	To address concerns arising out of the powers under Sections 69, 69A, 69B,	There is no denying the fact that these sections are a nightmare for those who

	70B the Summit recommends some measures which supplements the system of review presently suggested in the rules, with the formation of a "Netizen Rights Advisory Committee" with participation of NGOs and Private Persons of eminence to resolve conflicts that may arise in the implementation of the powers of interception, monitoring etc.	value Privacy and Freedom. At the same time the provision is considered necessary from the point of view of National security. Presently the review committee consists only of Government officials. It is therefore necessary to ensure that there is a participation of NGOs to prevent the possible misuse of the provisions and to provide confidence to the public that the powers are suitably balanced.
5	Cyber Law awareness should be made mandatory in all Intermediaries for the employees with a suitable system of audit and reporting for confirmation.	It is universally felt that lack of awareness of Cyber Laws is one of the reasons for widespread non compliance. It is considered that a legal mandate of creating awareness would be necessary to ensure better compliance.
6	In Cyber Café regulations, Registration, licensing must be made mandatory and conditional to **a.** Cyber Law training of the owner, **b.** implementation of ID verification through a robust system, **c.** confirmation of ID verification each time a user is provided access along with the record there of, **d.** provision for recording select activities of the user which will be retained for a minimum period of 3 years, with appropriate back ups and DRP systems as well as privacy related protections. **e.** Enabling of authorized law officer's access to stored data with appropriate permissions and activity logging.	Cyber Café regulation is considered a very important aspect of cyber space security. After a review of the existing regulations in some of the States it is felt that a uniform National regulation with implementation at the State level is essential. It is also felt that the browsing data would be a good source for intelligence purpose to monitor terrorist activities and it should be facilitated. However the privacy concerns of such a monitoring activity is also appreciated and appropriate safeguards in the form of de-identification of data and accountability of usage of the data as safeguards. The data retention period is presently 1 year in some States but considered inadequate considering the law enforcement requirements in India. Hence the period of three years is suggested.
7	Making all e-mail providers and Intermediaries provide IP address resolutions to authorized investigating officers without need for time consuming formalities while at the same time maintaining accountability of the investigating officers for the proper use of the authority.	The practice of providing proxy IP addresses in the e-mails by major e-mail providers such as Google and Yahoo create delays in investigations by the Police. Many of the smaller E-Mail providers in other countries may be completely out of

		reach of the law enforcement. Hence it is considered necessary that service providers are mandated to provide quick access to IP address resolutions.
8	Providing Reasonable Security in Internet based services including Banks should be the responsibility of the service provider and he should assume responsibilities for technical failures of the system and providing a security warranty.	In countries like Denmark and Germany the law/judicial view makes Banks liable for Phishing and Hacking of customer accounts. In India, Banks have been ignoring RBI instructions as well as law to use Digital Signatures for authentication. Hence there is a need to mandate use of digital signatures for communication for all Bank-Customer communications as well as Internet Banking log in. This can be achieved by the prescription of Reasonable Security Practices.
9	The period for which data needs to be retained under Sec 67C has to be adequate to meet the requirements of law enforcement. It is suggested that the minimum retention period can be specified as 3 years for all intermediaries and 5 years for all Banks and Financial Organizations.	Presently the thought is to make service providers liable to keep the data only for 6 months. This is considered insufficient. Most disputes arise after a lapse of time and investigations start much later. Hence 3 to 5 years is considered reasonable period for data retention.
10	Summit recommends that the Government of India should record its opposition to ICANN which intends allowing registrars of domain names to allow "Privacy" and Proxy" registrations. Such a measure will seriously limit the legal rights of Indian Citizens to take action against owners of foreign websites who transgress Indian law and also seriously affect the investigative capabilities of the Police. Since ICANN has requested for public comments on the proposal which is to be provided before November 6th , an immediate action on this is recommended to be initiated.	In case of any website which hosts anti national or criminal activities and content, it becomes necessary for filing cases against the registrars of domain names. If Privacy and Proxy registrations are permitted, neither Police nor any individual will know on whom the action has to be launched. Even though the system may assure that requests from Law Enforcement would be honoured, it is not possible to implement this since registrars are spread over hundreds of countries. If this provision becomes operational, "Rogue Websites" may mushroom. This will seriously hurt the interests of genuine web users. Since ICANN has asked for public comments, it has been suggested that the Government of India should itself formulate a response and state that Indian Government does not endorse the suggestion.

11	A serious concern has been exercised on the mobile companies protecting the data related to the customers. Some summit members expressed that the mobile companies may use the data of one customer to issue multiple connections which are then traded to others. To prevent this possibility, it is suggested that under the reasonable security practices for mobile companies, a provision should be made for adoption of OECD model of privacy protection which should provide a right for the data owner to ensure that no other account has been created by the mobile companies with his ID data. In order to ensure this, a name and address based search should be provided by all mobile companies so that a genuine citizen can check if his ID has been used only for his accounts and no body else.	The over aggressive nature of marketing in Mobile companies have resulted in many irregularities in the mobile registrations. Though measures are initiated on "ID verification" before new accounts are opened, this does not prevent multiple accounts to be opened with same ID documents. There have been reported incidents where customers have been requested to submit multiple documents for the same account and there is no accountability of how the ID documents have been used. Since the demand from anti social elements for SIM cards is eternal, there is a need to ensure that the ID proof of a person is used only for his account and not any body else. An appropriate procedure for this will involve recognition that the data of the customer has to be collected, used, protected and destroyed on OECD principles and the data owner should have an opportunity to verify if his data is being misused. This requires an online directory of mobile users with name and address with search facility like what BSNL provides. This is not a privacy invasion since mobile companies do share the data for marketing purpose unless the Donot Disturb registration is activated by a customer.
12	Effective security at home computers using Internet should be ensured by increasing the responsibility of the ISPs providing internet connection to educate and obtain an undertaking from the account holder that he is aware of the Cyber Security implications of owning the Internet account.	Security is never complete unless home computers are secured. As a first step to such security, every Internet user needs to be aware of certain basic security principles. The only agency which can effectively ensure this is the ISP. Hence it is suggested that before every new account is activated, a simple questionnaire is filled up and signed by the customer. This questionnaire should ensure that the customer is made aware of the basics of Internet security. Suitable checks should

		be instituted that this does not become a mere formality where the customer's signature is taken on a blank form and completed by the agency.
13	In the reasonable security practices to be prescribed for ISPs, they should be made responsible to identify known spam and phishing mails and suitably tag them and or remove them before delivery to the recipient.	Filtering Phishing and Spam should be the duty cast on ISPs. To avoid errors, every ISP should filter, tag e-mails as "Probable Spam" or "Probable Phishing Mail" before releasing it to the customer. The customers can then push such mails to separate folders and inspect them with care before relying on them. Hence this suggestion. Along with the earlier suggestion on Banks using digital signatures, this would reduce the impact of Phishing and Spam frauds.