THE CENTRE FOR internet & society

Roundtable on 'Enhancing Indian Cyber Security through Multi-Stakeholder' Cooperation

November 4, 2017 | New Delhi, India

EVENT REPORT

Designed by **Saumyaa Naidu**

Introduction

The Roundtable on 'Enhancing Indian Cyber Security through Multi-Stakeholder' Cooperation (hereinafter 'Roundtable') was held on the 4th November 2017 at the Indian Islamic Centre, New Delhi. This event was organised by the Centre for Internet and Society (CIS), and was attended by various cyber security and policy experts.

Given the proliferation of digital technologies and the central role they play in national infrastructure and governance, the security of systems and services is fundamental to the economic, political, and social development of a nation. Digital India, the National Payments Corporation of India, IndiaStack, and the Aadhaar ecosystem are only a few examples of such digital infrastructure. Yet the digital realm is increasingly becoming more complex, and difficult to secure, and monitor for vulnerabilities, threats, breaches, and attacks. The responsibility of identifying and monitoring such vulnerabilities is spearheaded by designated governmental bodies like CERT-IN and NCIIPC, but for effective identification of threats and vulnerabilities, collaboration is needed across stakeholder groups including security researchers, industry, and government bodies. Transparency in breaches and attacks is also key in enabling consumer awareness and building trust with the public. Examples of such mechanisms include bug bounty programs and breach notification frameworks.

This closed door Roundtable sought to bring together government, industry, civil society, academia, and security researchers to identify different areas for and tools of collaboration between stakeholders towards enhancing Indian cyber security. It broadly focussed on vulnerability identification and reporting and vulnerability/breach notification.

The Roundtable consisted of three sessions that dealt with Government Disclosure of Security Breaches, Incident Reporting, and Direct Interactions between the Government and the Cybersecurity Industry. This was followed by a final session that discussed questions from participants.

Session 1

The first session of the meeting was centred around the **vulnerability disclosure policies of the government and its departments**, as well as mechanisms to disclose or report vulnerabilities.

The first part of the session dealt with the system in place for individuals to report bugs/vulnerabilities to the respective authorities. Among the attendees, there were many suggestions on how the government's reporting mechanisms could be improved, primarily comparing them to jurisdictions where comprehensive vulnerability reporting processes are in place. For example, the reporting mechanism of the National Critical Information Infrastructure Protection Centre (NCIIPC) comprises of a static pdf form for the reporting of vulnerabilities, requiring reporters to print out the form, fill it manually, then scan the form, and finally email the scanned form back to NCIIPC. Kerala's Cyberdome on the other hand uses a free text field for reports, which creates a lack of consistency in inputs due to there being no compulsory fields. These mechanisms were compared to United States' CERT website which offers a web-form with conditional logic, which allows for the fields in each form to dynamically modify themselves according to previous responses. It was noted that having standardized forms with detailed fields for reporting vulnerabilities would be useful as many people who discover vulnerabilities are rarely experienced in reporting them and do not have a clear picture on the type of information that would be useful to the government for rectifying the vulnerability.

The second part of this session concerned the disclosure of incidents of security breaches by the government. The roundtable discussed two categories of vulnerability disclosure: Voluntary and Mandated. In India, it was noted that there is slow development of the latter category, where some departments/organisations are becoming subject to regulation that requires them to report vulnerabilities. However, voluntary disclosure is still very rare.

Another issue concerning disclosure dealt with different levels of disclosure. This discussion focused on the global debate between the historically contentious concept of responsible disclosure, and the more recent practice of full disclosure. Responsible disclosure involved limited disclosure, in the interest of security, but left too many loopholes that could be taken advantage of, defeating the purpose of disclosure. Full disclosure was later conceptualised to fix these problems, but does not address the security concerns. To date, there is no consensus on the most effective disclosure mechanism in the security industry, although some models have been developed where multiple kinds of disclosure (from only to a government regulator to a full fledged public release) are utilised according to the breadth and depth of the breach.

Session 2

The second session of the Roundtable dealt with the **motivations of security researchers**, and how the government could utilise this perspective to better engage with the security community.

The participants concluded that most people who report to the government are not interested in monetary rewards, since if they were, they would have simply report to the private sector which has an established practice of providing monetary rewards to bug reports. It was agreed that people who do report to the government do so with two goals. The primary goal is a genuine desire to get the bug fixed, often being driven by a patriotic mindset. The secondary goal for some of these people is to gain/receive recognition or acknowledgement for having reported a vulnerability. This is usually expected in the form of an acknowledgement of the report by government officials, on a public or private forum, or in the form of a "Hall of Fame" for individuals who have contributed to improving the government's cybersecurity infrastructure.

In India however, the government is yet to implement such a practice. Additionally, several times in the past the opposite effect has been felt, when the researchers are met with disincentives or demotivation to report vulnerabilities. For example, reporters of vulnerabilities have been issued show-cause notices, which has often resulted in them becoming fearful or reluctant to report vulnerabilities in the future, instead of being encouraged to do so.

The roundtable arrived at several solutions to this problem. First was for government departments to implement "Issue Trackers" through which a vulnerability reporter would be able to view the status of the report, in addition to the department's response to it and the action being taken. It is possible that such a system already exists internally, in which case it can now be made accessible to reporters.

The second solution was to effectively implement bug bounties. Bug bounties however, are difficult to run without external assistance. One successful bug bounty of note is "Hack the Pentagon", which the US government organised in collaboration with a privately owned vulnerability coordination and bug bounty program. Collaborating with a private organisation that is more experienced in organising bug bounties is a common practice internationally, to run an effective bug bounty.

A problem with bug bounties however, is the amount of misinformation that could potentially be perpetuated. Several past events across the world have shown that bug bounty events are can be either ineffectively conducted or conducted incorrectly. For example, a bug bounty organised by a former telecom provider, was done in collaboration with a private organisation. However, the event itself was marketed as a generic cybersecurity event, and instead of identifying bugs, the event had attendees give security recommendations, which failed to satisfy the goal of a bug bounty ie., identification and reporting of vulnerabilities. This also highlights the need to carry out checks on the expertise and competence of the participants and the collaborating private organisations, given that they are all likely to be privy to information on various security vulnerabilities.

Further, it was discussed that the government is allegedly apprehensive of vulnerability reporters. The lack of an official response on this issue, it was opined, could be attributed to the fear that a reporter would act maliciously subsequent to an official response. In this regard, the government, however, is seemingly more receptive to, and engaging with the reporters who have reported multiple times.

Furthermore, a policy system similar to the Netherlands could be implemented, where non-mandatory guidelines exist for security professionals. Professionals who abide by these guidelines get immunity from specific types of criminal prosecution. A system similar to this would create incentives for reporting by removing disincentives.

Even though the value of reporting is clear, some ineffective reporting mechanisms do more harm than good. In 2016, the RBI came up with a cybersecurity framework for banks, under which banks were compelled to submit a report within 2 to 6 hours. Subsequent to a security breach, the bank's Chief Information Security Officer had to prioritise between the drafting of the report to be sent to the RBI, or actually dealing with the security breach. The time constraint within which both actions had to be taken was a great hurdle in this case. Additionally, the banking personnel are not informed of the purpose of preparing such reports. In the absence of such information, many assume such a process to be mere formality, thereby reducing quality of the report and in turn reducing the effectiveness of the reporting mechanism. Sensitising the personnel on the importance of the mechanism would greatly increase their motivation to prepare diligent reports.

The recommendations to resolve this issue dealt with correcting the system on several levels. First, a more pragmatic mechanism should replace the existing one, where the compulsion to report does not

negatively affect remedying the breach itself. Second, the reporting authority should correctly utilise the data in the report. In this case, the suggestion was to replace RBI with a more appropriate forum like the CISO forum. One of the points brought up in favour of the superiority of the CISO forum was the uniformity in its process of notifying different vendors about security breaches, in that the CISO treated all vendors on an equal level. As an additional safeguard, the guidelines or regulations could outline what the forum does with these reports, and establish deadlines for the same.

Another recommendation came in the form of a discussion on the liability of the departments or organisations to compensate the users in the event of a breach. In these cases, giving entities an immunity from liability in case of a security breach, as long as the entity abides by the disclosure standard would create incentives for departments/organisations to disclose vulnerabilities, by removing disincentives.

The final discussion of the session dealt with recommendations to set up a parliamentary committee that all government entities would report to. This committee would handle all cases of disclosure and decide, on a case by case basis, the specific nature/extent of appropriate disclosure as well as when and to whom the disclosure is to be made. Though this system would be very effective under ideal conditions, it is also very difficult to set up a committee that is experienced in matters of cybersecurity.

Session 3

The final session of the roundtable dealt with improving the **government's capacity building**, as well as amending the provisions of the **Information Technology Act, 2000**. With respect to capacity building, there were three broad issues discussed. The first issue dealt with the government engaging with the cybersecurity community through events like conferences. The International Cyber Security and Policing Conference, or Co-con, is one such event that has proven to be an exemplary initiative where security researchers from across the world gather. This has served as a platform for Indian police officers to learn from their global counterparts. A major problem with conventional large scale events is that they are more focused on marketing and publicity, instead of technical research or development. This consequently results in a lower quality of participation, and attendees. As a result, several charlatans in the security industry utilise these events as a platform to build their own brand. However, in conferences like Cocon, though similar problems exist, the organisers are conscious of them and closely monitor the event to preserve the high quality standards. Nullcon, another cybersecurity conference, is also similarly high quality.

Other opportunities for the police to engage with the cybersecurity community come in the form of establishments like Kerala's Cyberdome, which is a public-private partnership created by the Kerala police department in collaboration with private cybersecurity entities. Cyberdome is involved in reactive and preventive cybersecurity work in Kerala. This initiative is in the process of being replicated in Assam, Maharashtra, Gujarat, and Tamil Nadu.

Another capacity building issue that was discussed was the value of security certifications. While most attendees did not believe in the inherent value of certifications exclusive, and preferred looking at the practical track record of the security researchers. Most certification courses are "checklist-driven", and often do not result in training qualified and/or competent professionals. Importantly, most certification courses fail to cover even a small aspect of hacker ethics.

Finally, the roundtable discussed various provisions of the IT Act that were problematic. These provisions due to inconsistency, create problems for security researchers. The issues in this regard arise primarily in Sections 43 ("Penalty and compensation for damage to computer, computer system, etc."), 65 ("Tampering with computer source documents"), and 66 ("Computer related offences").

Section 43, imposes penalties on "unauthorized access to computer systems". On plain interpretation, this would make mere browsing of a website an offence under section 43, since there is no "permission of the owner" of a website while browsing. Section 43 also imposes penalties on anyone who "introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network". However, this would include entities like CERT-In and NCIIPC who encourage the sharing of malware with them. Section 66 is the criminal equivalent of Section 43, and suffers from similar problems, but on a more severe scale, due to the criminal sanctions involved.

Section 65, which criminalises altering, destroying, or concealing computer "source code" that is required to be protected, is especially problematic since the definition of source code is "listing of programmes, computer commands, design and layout and programme analysis of computer resource in

any form". It was agreed that this definition does not conform to the technical definition of source code that is followed by most security researchers, and other professionals who are conversant with digital technology.

These issues in the interpretation of the law pose large obstacles to initiating development in the cybersecurity industry. Presently, judges who are sufficiently conversant with technology are few and far between. A large majority of judges do not understand the intent of these provisions, and often misinterpret them. It was agreed that there was an immediate need to clarify the meaning and intent of these provisions in the form of an amendment, before problematic legal precedent can be created.

To conclude, the Roundtable acknowledged the following solutions, and implementations for the Indian government that would greatly improve the state of cybersecurity in the country, as well as the relationship between the government, and professionals in the cybersecurity industry:

1. Implement logic based vulnerability reporting facilities on department websites, similar to the United States' CERT model.
2. Implement an acknowledgement feature for security researchers who report vulnerabilities, possibly in the form of a Hall of Fame.
3. Respond to vulnerability reports in an encouraging manner, without causing disincentivisation or demotivation.
4. Implement an Issue Tracker system for each department, and make it available to the public, to enable the tracking of responses and acknowledgements to vulnerability reports.
5. Implement effective bug bounty programs in collaboration with legitimate, and reliable organisations.
6. Provide specific immunity from liability to departments and organisations that follow effective breach disclosure practices.
7. Improve existing breach disclosure mechanisms (like the RBI's mechanism), by sensitising personnel to the importance of effective disclosure, and by proactively responding to disclosure reports.
8. Establish an effective authority to oversee disclosure reports, like the CISO, or a parliamentary committee.
9. Organise high quality cybersecurity events, like Nullcon and Co-con, and encourage the participation of government personnel, as well as police officers.
10. Give importance to the industry track record of security professionals, instead of focusing exclusively on the certifications they hold.
11. Amend unclear, and problematic provisions of the IT Act, before problematic precedent is created.