Cyber Security & the CERT-In

A Report on the Indian Computer Emergency Response Team's Proactive Mandate in the Indian Cyber Security Ecosystem

Udbhav Tiwari

Table of Contents

Introduction

The Indian Computer Emergency Response Team (CERT-In) is India's nodal agency under Section 70B of the Information Technology Act, 2000, as amended in 2008[1] (IT Act, 2000). CERT-In's operational scope extends from being the first responder for cyber security incidents to spreading awareness among the various stakeholders on best practices to secure the nation's cyber infrastructure. This article will be the first in a series of articles that analyse the proactive, reactive and training mandates of CERT-In respectively, while highlighting key areas that can be improved and suggesting normative measures using which such improvements can be carried out. It shall primarily rely on CERT-In's website and verified media coverage as its primary sources of information for CERT-In's past actions. The article will exclude coverage of the National Critical Information Infrastructure Protection Centre and its operations, which are governed by separate legislation,[2] have a far more specific mandate and in turn will be the subject of a separate series of papers/blog posts to be published at a future date.

Legal Background

CERT-IN's proactive mandate is defined in the IT Act, 2000 as well as in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Function and Duties) Rules, 2013[3] (CERT-In Rules, 2013) both of which postdate the existence of the organisation itself, which has been operational since 2004. Regarding the proactive mandate, the IT Act and CERT-In Rules include the following areas where CERT-In is required to carry out proactive measures in the interests of cyber security:

1. Forecast and alert cyber security incidents (IT Act, 2000) & Predict and prevent cyber security incidents (CERT-In Rules, 2013)
2. Issue guidelines, advisories and vulnerability notes etc. relating to information security practices, procedures, prevention, response and reporting (IT Act, 2000)
3. Information Security Assurance (CERT-In Rules, 2013)

[1] http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf
[2] http://meity.gov.in/sites/upload_files/dit/files/GSR_19(E).pdf
[3] http://meity.gov.in/sites/upload_files/dit/files/GSR_19(E).pdf

This article will track and analyse the CERT-In's operations in each of these areas over the past twelve years, by analysing the information available on CERT-In's website as well as other media in the public domain.

The analysis will be carried out using a mixed methodology. The basic quantitative analysis of the information available on the CERT-In' website will be carried out in the form of simple comparatives of updates, bulletins and other forms of publicly available interaction and critical information dispersal on CERT-In's website. The qualitative sections, on the other hand, will contain a comparative analysis of the content present in the technical documents of the CERT-In with the equivalent documentation (where present) of similar bodies in the USA and EU. Each section will then illustrate normative suggestions as to how CERT-In's performance of that respective obligation can be improved to better serve its cyber security mandate.

Forecast & Alert of Cyber Security Incidents - Section 70A(4)(b) of the IT Act, 2000

CERT-In's mandate to forecast and alert cyber security incidents is arguably one of its most important, public mandates that has a tangible impact on the various stakeholders in the cyber security industry. The various resources and privileges uniquely available to a government sanctioned cyber security outfit make this mandate a possibly exclusive one in terms of impact on the nation's cyber security. These resources and privileges include the ability to carry out normative research on fringe fields, ensure rigorous analysis of previous cyber security incidents, collaboration with other security agencies from the public and private sector, etc.

The CERT-In's website contains a 'knowledge base' section that has been codifying its action with regard to this mandate since its inception in 2004. This knowledge base section has four subcategories: Guidelines, White Papers, a Monthly Security Bulletin and an Annual Report. This post will analyse each of these subcategories, from a critical and normative perspective.

Guidelines[4]

The 'Guidelines' subsection was last updated in 2011, with 23 guidelines issued between 2003 to 2011.[5] Some of the guidelines that were issued, are targeted towards the layman public and contain little to no technical research or knowledge that can be used by stakeholders to prevent cyber attacks from a proactive perspective[6]. The guidelines that do analyse cyber threats from a technical perspective are all over a decade old and are thus technologically outdated.[7] The guideline linked to the previous footnote which was issued in 2005, for example, deals with RedHat Server 3, which lost extended life support in 2010, over six years ago[8]. Similar archaic standards are seen in the ISS 7 Server from Microsoft[9] (the current version being ISS 10), web server security guidelines from 2004[10] and even the latest IT Security Policy recommendations on the page date from 2003[11]. The absence of any new guidelines since 2011, even if they were to be attuned to the general public, means that CERT-In has not publicly issued guidelines on any of the relatively new cyber developments since 2011 such as ransomware, botnets, exploits relating to the internet of things, etc. by CERT-In. Consequently, the public knowledge base created by CERT-In is very dated and leaves the stakeholders relying on it for being informed about threats ill equipped to handle modern cyber security challenges.

White Papers[12]

This section documents on original cyber security research as well as technical reports of certain activities such as website defacements, etc. carried out by CERT-In. The documents are not entirely technical and only contain basic statistics about such cyber security breaches. The 'white paper' section of the website was last updated in 2010 and contains a net total of 17 'whitepapers' between 2003 and 2010, most of which are explanatory and statistical in nature as opposed to analytical (i.e. highlighting the source of the attack and illustrating possible solutions) in nature.[13] The reports that are in fact

[4] http://cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW01#

[5] http://hp.ipviking.com/

[6] http://www.cert-in.org.in/Downloader?pageid=6&type=2&fileName=CIGU-2011-0154.pdf

[7] http://www.cert-in.org.in/Downloader?pageid=6&type=2&fileName=cisg-2005-02.pdf

[8] https://rhn.redhat.com/errata/RHSA-2010-0817.html

[9] http://www.cert-in.org.in/Downloader?pageid=6&type=2&fileName=CIGU-2010-01.pdf

[10] http://www.cert-in.org.in/Downloader?pageid=6&type=2&fileName=CISG-2004-04.pdf

[11] http://www.cert-in.org.in/Downloader?pageid=6&type=2&fileName=CISG-2003-02.pdf

[12] http://cert-in.org.in/s2cMainServlet?pageid=WHTPIEW01

[13] http://www.cert-in.org.in/Downloader?pageid=7&type=2&fileName=CIWP-2004-01.pdf

technical are very outdated with the last Whitepaper being released in 2010, over 6 years ago. An example would be the report that studies the 'MyDoom' virus, which was last considered an active threat in 2008 and has since been widely patched against in most modern operating systems.[14] Other examples include Botnets from 2010[15] (which have since evolved to even include home thermostats as a part of their attack vectors), iFrame injection[16], while iFrames have become all but redundant since the advent of HTML5 and Mobile Viruses[17] that deal with neither Android nor iOS, but Symbian, an almost defunct platform. If similar analysis were to be carried out for more modern contemporary malware, it would enable the various stakeholders in the cyber security space to benefit from more comprehensive measures for future attacks as well as increase CERT-In's ability to respond to such attacks in the future.

Monthly Bulletins[18]

The Monthly Bulletins are supposed to be the most proactive and relevant component of CERT-In's mandate as they analyse previous attack trends, highlight key factors common to such attacks, suggest measures to overcome and prevent such attacks in the future on a monthly basis This section is the most up to date section of the CERT-In website with regard to its 'knowledge base' section, with the last bulletin being posted in October, 2015. There have been no bulletins issued since then and the 2016 page, at the time of writing this post, was empty.[19] The bulletins that do exist for the previous years also largely contain statistical information about open proxy servers[20], website defacements[21], etc. without going into the causes of cyber security issues nor providing solutions of how to mitigate their harmful effects. The last issued bulletin from October, 2015 is indicative of this, with few technical details or suggested preventive measures in the entire document.[22] Any forewarnings or normative news items it contains are also mere reiterations of other international cybersecurity websites such as Threatpost[23] or Sophos

[14] http://www.cert-in.org.in/Downloader?pageid=7&type=2&fileName=mydoomanalysis.pdf
[15] http://www.cert-in.org.in/Downloader?pageid=7&type=2&fileName=CIWP-2014-2334.pdf
[16] http://www.cert-in.org.in/Downloader?pageid=7&type=2&fileName=CIWP-2014-2333.pdf
[17] http://www.cert-in.org.in/Downloader?pageid=7&type=2&fileName=CIWP-2005-04.pdf
[18] http://cert-in.org.in/s2cMainServlet?pageid=MNTBLTN
[19] http://cert-in.org.in/s2cMainServlet?pageid=MNTBLTN&year=2016
[20] http://www.cert-in.org.in/Downloader?pageid=10&type=1&fileName=MBULL-2015-0008.pdf
[21] http://www.cert-in.org.in/Downloader?pageid=10&type=1&fileName=MBULL-2015-0001.pdf
[22] http://www.cert-in.org.in/Downloader?pageid=10&type=1&fileName=MBULL-2015-0009.pdf
[23] https://threatpost.com/

[24], with no original research or highlights in most of the bulletins for any year. This trend is true for all bulletins going back to the year 2012, when they were first issued. Even in the years in which they have been issued, there are at least two to three months in a year in which there were no bulletins at all, leaving those months undocumented. This continues to apply even if it were to be presumed that CERT-In was engaging in non public channels of communication for security reasons. It would be beneficial for research carried out by CERT-In & the methodology followed to neutralise such threats to be released into the public domain after the threat being neutralised, like CERT-In's equivalent agencies abroad.[25] Finally, the fact that no such bulletin has been issued since October, 2015 means that there is no current and contemporary documented knowledge of the cyber security scenarios in India for the for any of the stakeholders to analyse, react and protect themselves against.

Annual Reports[26]

These Annual reports are a collation of the data present in the Monthly Bulletins, with aggregated statistics and some scattering of news reports and other coverage of CERT-In actions, both reactive and proactive. These reports, which can have a key and focused impact on the cyber security ecosystem by highlighting key trends and suggesting countermeasures, appear to be limited to mapping trends. Of all the sections in the knowledge base, such statistical trends probably find their place the most in these reports. However, the absence of any normative measures or suggestions on how to combat these trends nor any effort to highlight measures to prevent such trends from occurring in the future significantly reduce their impact in the reports. For example, the 2015 report is a 11 page document that provides statistics, reiterates training programmes and devotes half a page to future plans and actions, without going into any technical details, resources or measures whatsoever.[27] While meeting the standard of being regularly produced every year since 2006, the reports leave a lot to be desired in terms of their relevance to the proactive aspects of the cyber security ecosystem due to their focus on rehashing prior actions with little to no technical detail which may help the audience learn from CERT-In's actions.

[24] https://nakedsecurity.sophos.com/
[25] https://www.us-cert.gov/security-publications
[26] http://cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT
[27] http://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2016-0063.pdf

Normative Suggestions for Improvement of the Knowledge Base

The following measures and practices, applied uniformly to all subsections of the knowledge base, will go a long way in making it a valuable tool to cyber community for both documenting current threats as well as proactively reacting to future ones. The suggestions are largely based on studying similar practices in other jurisdictions, such as the EU and USA, comparing the effectiveness of these practices with CERT-In's mandate and then choosing the ones that are the easiest to implement with minimal infrastructural costs :

1. Creating systems (both technical and process-driven) to generate necessary rapid situational awareness of existing and potential cyber security threats across the cyber security ecosystem. This would then allow for timely sharing of critical information that would allow both preventive and protective actions by selective relevant stakeholders in a well documented, publicly accessible format. Selective relevant stakeholders in this case would be industries (based on hardware & software used) at particular risk of being targeted to certain kinds of cyber attacks, where public disclosure would only make them more vulnerable to such attacks until they are patched. An example could be the recent Internet Of Things based Dyn Inc. DDOS attack that targeted the IoT industry[28]. An automated, systemic infrastructure, maintained by CERT-In, that allows for such situational awareness (in the form of warnings, patches, audit recommendations, etc) to be dispersed to the relevant parties in a very short amount time will be a game changer. It will allow institutional responses to cyber attacks with a scale and timing that can significantly reduce the harm that arises out of them regardless of their source or intensity. Examples of such systems already operating in other nations include the National Cybersecurity and Communications Integration Center[29] in the USA, the European Cybercrime Centre in the European Union[30] and the Automated

[28] https://www.us-cert.gov/security-publications

[29] https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

[30] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Indicator Sharing (AIS) at the US-CERT[31]. All of these initiatives can be studied for practices, tools and standards that will ensure increased capability to deal with modern threats.

2. Reactivating the guidelines and whitepapers section of the knowledge base, along with focusing on an overall increase of funding (which has been noticed as a problem before[32]) and focusing on Research & Development activities in the areas of attack & malware detection, threat prevention and information sharing. This will allow CERT-In to augment its already present in house expertise to combat technical threats as well as disseminate critical knowledge into the Indian cyber security ecosystem. It will also allow CERT-In to better fulfil its mandate regarding publishing and engaging with the public & other stakeholders. CSD Projects at the Department of Homeland Security in the USA[33] is an excellent case study for how funding cybersecurity research and development projects can result in transforming an idea into a deployable solution accessible to the community at large.
3. Initiate and increase active collaborations with reputed international agencies to allow for information and tool sharing, resource (both human and technical) development and reduction of redundancy. Currently, such collaborations are limited to on paper MoUs with approximately nine countries (Korea, Canada, Australia, Malaysia, Singapore, Japan, USA, UK and Uzbekistan)[34] with very little public information about the tangible outcome of these MoUs. A large percentage of cyber threats have little to no concern with national borders, meaning they would affect systems equally across jurisdictions. Collaboration with international and national partners would ensure that solutions are shared quickly and efficiently across agencies to proactively block the attacks they protect systems against from spreading across global networks, preventing them from becoming even more dangerous. The US-EU Cyber Security Collaboration[35] initiated earlier

[31] https://www.us-cert.gov/ais

[32] http://articles.economictimes.indiatimes.com/2015-01-28/news/58546771_1_cyber-security-cert-in-national-cyber-coordination-centre
http://articles.economictimes.indiatimes.com/2015-01-28/news/58546771_1_cyber-security-cert-in-national-cyber-coordination-centre

[33] https://www.dhs.gov/science-and-technology/csd-projects

[34] http://meity.gov.in/content/mouagreementprotocol [Lists MoUs prior to 2015]

[35] http://europa.eu/rapid/press-release_MEMO-11-246_en.htm

this year is a model that India should inspire towards recreating with as many international and regional entities as possible. Salient aspects of the MoU that should be initiated with other countries include specifically allowing for exchange technical information on Cyber attacks, combined response to cyber security incidents and incentivising joint R&D efforts to find solutions to counter the cyber attacks

Vulnerability Issuance & Damage Control- Section 70B(4)(e) of the IT Act, 2000

CERT-In's proactive mandate in terms of real world practice is best exemplified from its Advisories[36] and Vulnerabilities Notes[37] subsections on its website. These two subsections contain information on exploits and vulnerabilities in commonly used software and hardware. This information aims to enable stakeholders to contain harm to live systems either by patching them or by preventing scenarios that allow for the exploits to be carried out until patched. CERT-In does not issue fixes or provide solutions apart from linking to the vendor's website, which may or may not contain possible solutions or fixes for the corresponding exploits.

CVE & Advisory Issuance

There are various issues with the CERT-In's Advisories and Vulnerabilities Notes procedures which are highlighted below. Normative suggestions on how these highlighted problems can be fixed will follow after this section. The most pressing problems with CERT-In's current Advisories and Vulnerabilities Notes procedures are as follows:

- The Advisories and Vulnerabilities Notes on the CERT-In website are not products of original research or outputs but mere reiterations of either vendor disclosures or other internationally respected cyber security analysis outfits. One of the most commonly used source for CERT-In's advisories is the United States Computer

[36] http://cert-in.org.in/s2cMainServlet?pageid=PUBADVLIST
[37] http://cert-in.org.in/s2cMainServlet?pageid=VLNLIST

Emergency Readiness Team[38] (US-CERT) which is the based out of Carnegie Mellon University and is funded by the Federal Government to carry out cutting edge research into major incidents, analyzing threats and ensuring information dissemination. Other resources used include the CVE Database[39], which is the internationally recognised standard for disclosing and divulging vulnerabilities, the National Vulnerabilities Database[40] from USA and the CERT-EU[41] from Europe. The lack of original research and outputs is deeply problematic for two main reasons. The first being the large quantity of domestically produced and used software & hardware that doesn't enjoy an external, international market is largely ignored. Exploits from these systems, therefore, go undocumented and are left wide open for exploitation. Systems that suffer from this issue include all the software produced by C-DAC, software that powers critical national infrastructure[42] as well as various key components of the recent Make In India drive[43] including defence and aerospace systems. These critical components of India's cyber infrastructure are left unanalysed and open to exploitation due to neglect by CERT-In or a similar organisation from a software security auditing perspective. The second problem that arises from the lack of new and original research for issuing security advisories is that it prevents CERT-In from developing the in house skills and expertise it needs to be able proactively research, highlight and patch exploits as a part of its mandate. Both of these factors conspire to make the Advisories and Vulnerabilities Notes little more than a mere compilation of software and hardware exploits.

- Even if the mere compilation of Advisories and Vulnerabilities Notes and other security bulletins from elsewhere on the Internet were to be looked at as a fulfillment of CERT-In's mandate and the harms highlighted above were to be ignored, they are lacking in terms of relevance, speed of issuance and comprehensiveness. They are more often than not available in a better format

[38] https://www.us-cert.gov/
[39] https://cve.mitre.org/about/
[40] https://nvd.nist.gov/
[41] https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.htmla
[42] http://cdac.in/index.aspx?id=products_services
[43] http://www.enterpriseinnovation.net/article/make-india-cyber-security-1433304887
http://www.mckinsey.com/~/media/mckinsey%20offices/india/pdfs/a_bright_future_for_indias_defense_industry.ashx

and at an earlier date on other publicly accessible websites on the internet run by other governments as well as other private organisations,[44] making the entire process carried out by CERT-In rather redundant if breadth of coverage and speed of issuance is considered a relevant factor in such security warnings. An example is the the MITRE CVE List website[45] interface. The MITRE CVE List is available in various formats (both online and offline), can be easily searched with various boolean operators and contains a detailed and well-defined FAQ on how to get included on the CVE database. The CERT-In website lacks a search function, with CVE's only available on an individual link by link basis, forcing users to trail through possibly hundreds of links to get to the designated CVE unless they know exactly which CVE they are looking for prior to coming onto the website.

- The narrower scope and delay in issuance of vulnerabilities by CERT-In can be seen comparing CERT-In's statistics from their Annual Report[46] to the National Vulnerability Database(NVD)[47] of the USA to see the total number of vulnerabilities that have been documented in these databases in 2015. CERT-In claims to have issues 420 security alerts, advisories and vulnerability notes in 2015. The NVD on the other hand, has issues over 6,488 such notices in 2015 alone. That is a difference of over 6, 000 security alerts, advisories and vulnerability notes in just one year, a staggering number considering the pervasive use of common software and hardware between both jurisdictions. A majority of the CVE's that are common between both of these systems appear 3 to 6 days[48] after their appearance on the NVD database in the USA, also proving the lack of proactiveness in terms of the time taken in releasing these vulnerabilities on the CERT-In website.

[44] https://www.first.org/global/sigs/vrdx/vdb-catalog

[45] https://cve.mitre.org/cve/cve.html

[46] http://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2016-0063.pdf

[47] https://nvd.nist.gov/
https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on&pub_date_start_month=0&pub_date_start_year=2015&pub_date_end_month=11&pub_date_end_year=2015&cvss_version=3

[48] http://cert-in.org.in/s2cMainServlet?pageid=PUBADVLIST &
http://cert-in.org.in/s2cMainServlet?pageid=VLNLIST

Normative Suggestions for Improvements in Alert & Guideline Issuance

The current model followed by CERT-In in issuing Advisories and Vulnerabilities Notes could benefit from the implementation of the following measures :

1. Actively leveraging the full membership CERT-In enjoys at the Forum of Incident Response and Security Teams (FIRST), an organisation created for information exchange and cooperation on issues such as security vulnerabilities and cyber attacks. FIRST provides access to up-to-date best practice documents[49], technical colloquia for security experts[50] and special interest groups[51] surrounding key security issues and even holds an annual incident response conference[52] almost none of which CERT-In chooses to actively utilise or contribute towards. For example, since the current CERT-In system merely compiles advisories from other jurisdictions, the FIRST Vulnerability Reporting and Data eXchange SIG[53] can replace the entirety of CERT-In's database and will serve the job far better than the current system and solve most of the problems highlighted above.
2. A clear focus on Research & Development activities rather than mere compilation and dissemination of the work of other security organisations. Since measures like the FIRST SIG eXchange are already available, a simple guide on how to utilise such systems is more than sufficient to fulfil the part of the mandate that requires dissemination of previously conducted security announcements and research. This will allow the necessary original resources to be focused on finding unique security flaws and exploits in indigenously developed and used software as well as allowing CERT-In to contribute to organisations such as FIRST. Resources that can help in adopting such measures include FIRST best practices guides[54] and actively participating in the special interest groups at organisations such as MITRE[55] and active collaborations with other cyber security agencies such as leveraging the recently signed US-India Cyber Security Collaboration pact.[56]

[49] https://www.first.org/resources/guides/
[50] https://www.first.org/events/colloquia/
[51] https://www.first.org/global/sigs/
[52] https://www.first.org/conference/
[53] http://jvnrss.ise.chuo-u.ac.jp/vrdx/vdb_catalog.html
[54] https://www.first.org/_assets/resources/guides/cert-in-a-box.zip
[55] https://cve.mitre.org/docs/cve-intro-handout.pdf
[56] http://thewire.in/42021/the-long-and-winding-road-to-us-india-cyber-cooperation/

3. Allowing the private sector, including private hackers and the public to submit security vulnerabilities and cyber attacks in a easy to find and detailed manner, without making the process too cumbersome or tedious. The current CERT-In can only be informed of such exploits via an email address, leaving the modalities of such as exploit completely open ended. In comparison, the US-CERT Incident Reporting System[57] contains a detailed, elaborate and privacy conscious form that makes an exploit far easier to report and follow up with in the future. Further, offering bug bounties will also incentivise security researchers to reach out to the government with their bugs and exploits instead of either utilising it themselves or selling it to the highest bidder on the dark web[58].

Information Security Assurance (Rule 9, CERT-In Rules, 2013)

Information security assurance (ISA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information and the systems used for these processes. There are various international standards that can be used to gauge best practices in ISA such as ISO 27001, [59] BS 7799-3:2006,[60] CISSP[61] etc. ISA and its relevant standards play the role of the first line of defence in cyber attacks and a well-designed, audited and resilient ISA policy process can significantly reduce or even nullify the harms arising out of a cyber attack. CERT-In's obligation to ensure the minimum required Information security related cyber security standards are followed by government organisations and key critical infrastructure is carried out under two main heads. The first is the role CERT-In itself plays in carrying out policy formation, advice

[57] https://www.us-cert.gov/forms/report & https://malware.us-cert.gov/MalwareSubmission/pages/submission.jsf

[58] https://iicybersecurity.wordpress.com/2015/06/10/famous-dark-net-marketplaces-to-buy-exploits-0-day-vulnerabilities-malwares-for-research/

[59] http://www.iso.org/iso/iso27001

[60] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/bs-7799-3
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/bs-7799-3

[61] https://www.isc2.org/cissp/default.aspx

gathering and empanelment of public & private sector organisations that are qualified to carry out information security audits & certifications. The second head is the role carried out by the Standardisation Testing and Quality Certification (STQC) Directorate[62] under the Ministry of Electronics and Information Technology, created in 1980 to provide minimum standards for the electronics industry but has since expanded its operational scope. The STQC Directorate is one of the premier organisations in the country involved in certifying organizations and products on their information security processes by auditing/testing them. It also provides training for auditors under certifications such as ISO 27001 to create a talent pool of qualified security auditing professionals in the country. This section will look exclusively at the role played by CERT-In, keeping in mind the original scope of the article, leaving out the STQC and critiques of its operations which may be covered in a separate piece at a later date.

The CERT-In's internal role on information security can be found on the Information Security Policy page[63] on its website which carries various documentation about the actions and recommendations carried out by CERT-In in furthering ISA in key government and critical infrastructure organisations. The CERT-In's website also contains a page on policy, procedure and eligible organisations that meet the criteria for empanelment with CERT-In as auditors for ISA audits in government organisations[64]. The section will look at ISA Policy largely, as Empanelment is solely concerned with procedural steps to verify ISO 27001 certification for auditing agencies to make them eligible for government organisation & company audits.

ISA Policy

The ISA Policy page at CERT-In's website contains the reccomended IT Security Policy for Government & Critical Infrastructure programmes as well as ISA Implementation guides that can be used by private and public entities alike to improve their cyber security profiles from both an infrastructure and processes perspective. The following observations about the content can be made:

[62] http://www.stqc.gov.in/
[63] http://cert-in.org.in/s2cMainServlet?pageid=PUBISP01
[64] http://cert-in.org.in/s2cMainServlet?pageid=CERTEMPANEL#

1. A majority of the documentation present on the page is very outdated with the latest document dating from 2009, which is training presentation that rehashed from CERT-In's yearly training programmes from that year[65]. The process and procedures described in this documentation are not only outdated but also incorrect in various instances. For example, the ISO 27001 standard was finalised in 2013, which would mean the ISO 27001 references in the document refer to draft instances of the standard and do not account for the changes in the ISA ecosystem that would have occurred in the four years between 2009 and 2013,[66] forget any of the newer developments that would have taken place since 2013.
2. The documents that do describe recommended policy and procedures are also incredibly brief, cursory and provide little to no details required to make them effective tools in ISA development and implementation. As an example, the "Implementation of Information Security Management System in Government & Critical Sectors as per ISO 27001 : Progressive Steps[67]" document is little more than half a page long, contains no technical details or knowledge to document the progressive steps been taken and refers to very broad and normative steps without detailing any real steps required to carry out these measures.
3. The templates and other reference documentation that are required documentation that need to be submitted to CERT-In by government agencies and critical infrastructure entities to CERT-In on the page are provided without any relevant sample documentation, guidelines or standards and neither are they present in any of the detail required to match up to international best practices. For example, the template for the "Progress in implementation of ISO27001 Information Security Compliance[68]" is a one page document that only contains one obtuse, hard to decipher table and contains no guidance on that any of the rows and columns means nor the processes that need to be followed to fill the required information.
4. The page contains limited documentation and guidance that is applicable to non-critical sector private organisations, who form the majority of the stakeholders in the national cyber security ecosystem. The available

[65] http://www.cert-in.org.in/Downloader?pageid=13&type=2&fileName=ISMS_STQC.pdf
[66] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
[67] http://www.cert-in.org.in/Downloader?pageid=13&type=2&fileName=ISO_27001.pdf
[68] http://www.cert-in.org.in/Downloader?pageid=13&type=2&fileName=InfoSecCompliance.pdf

documentation not only concentrates on government and critical infrastructure sector entities but actively ignores any applicable standards or advice that it could provide to industry associations[69] and ethical hackers,[70] making it fulfil (rather poorly) only a miniscule fragment of its mandate.

Normative Suggestions for Improvement of ISA Policy Initiatives

1. The suggestions on the page need to be significantly updated to reflect the current paradigm of threats that are affecting the Indian Cyber Security ecosystem, including modern standards, best practices & incident reporting procedures to deal with such threats. This is because all of the information on the CERT-In website on ISA pre-dates 2013 on the current website. An ideal role model for such a practice is the system followed by the US-CERT, which categorises all ISA information into four main categories,[71] namely, Industrial System Users, Government Users, Homes and Businesses. Each of these sections have detailed ISA policy recommendations, advisories, best practices and even user guides that are frequently updated to reflect new developments.
2. The information that is presented needs to contain far more technical detail, including defensive processes, investigative techniques and possible solutions than the current set of documents. This is so that the industry and even home users can actually use these documents in the field with as few edits or modifications as possible. The model followed by the CERT-EU[72], which is a combination of original news and aggregating technical content from all of the internet is a viable initial model that can be modified for the Indian scenario.

Conclusion

As the paper demonstrates with its analysis, CERT-In's mandate to proactively defend India's cyber security interest for the various stakeholders in the Indian Cyber Security ecosystem could benefit from a number of reforms. Studying (and even adopting) the

[69] https://www.dsci.in/taxonomypage/1182
[70] http://cmai.asia/cybersecurity/
[71] https://www.us-cert.gov/ncas
[72] https://cert.europa.eu/cert/alertedition/en/Malware.html

best practices from various similar organizations across the world, especially the European Union[73] and the USA[74] along with a focused increase on original research & development and targeted public outreach are the three main ways to bring the CERT-In up to par to not only its peers from all over the world but also capable of pre-empting the increasingly complex threats in cyber security. The various ways in which this can be done in the current operating spheres of CERT-In's proactive mandate have been illustrated in the paper but a truly contemporary CERT-In requires needs to restructure itself from the ground up to be able to be dynamic and consistent in its responses to cyber security threats, especially in matters concerning proactive security. While entities like the National Cyber Coordination Centre[75] (which is yet to be set up) can aid this process, only systemic technical skill development and real time engagement with concerned stakeholders can ensure CERT-In fulfils its mandate to both protect and defend against the wide spectrum of cyber threats faced by India.

[73] http://cert.europa.eu/

[74] https://www.us-cert.gov/

[75] http://pib.nic.in/newsite/PrintRelease.aspx?relid=133895