# India's TOP 5 Information Security Concerns: 2013

The country's first ever independent assessment of InfoSec concerns identified by the professional community

ClubHACK

India Watch

# COPYRIGHT AND DISCLAIMER

# PREAMBLE

It's time we identified what ails the information security efforts in India. It's time we used India-centric information and localized knowledge and intelligence to counter the threats and risks that keep growing alongside advances in technology.

This report, jointly prepared by *IndiaWatch* and *ClubHack*, is about India and is based on submissions to an online survey of hundreds of information security professionals from India and abroad. *IndiaWatch* is an India centric research and knowledge organization in the Information / Data management and security domain with a mission to seek opportunities to work and contribute to enhancing the national security posture. *ClubHack* is the first Indian Hacker's conference and monthly magazine. Synonymous with the information security profession in the country today, *ClubHack* is largely responsible for popularizing free and open learning in the technical InfoSec domain.

**Why a new study?**

Numerous annual threat and risk predictions are published globally–some are relevant to India, some are not. While some of these reports are reliable, many are vendor-driven or influenced by vested interests. Although these reports help in focusing on security issues, none, surprisingly, help to look at missing perspectives or perceptions, or at issues arising out of behavior or work culture–the weaknesses that contribute to the 'insecurity' of information security.

We intend to highlight these concerns for *India the Nation*, the *Indian Business*, and the *Indian Netizen*. This report offers a straightforward presentation of systemic concerns as expressed by our survey's respondents. Our respondents want you to look within–engage in an internal debate, light up your *Dimaag Ki Batti* [1] and experience your *Eureka* moment. Rather than worrying about risks and threats, one should work to address these InfoSec concerns or issues.

We present **India's Top 5 Information Security Concerns: 2013.**

[1] **Dimaag Ki Batti:** A Hindi phrase that literally means 'light a lamp in your mind'.

# CONTENTS

# EXECUTIVE SUMMARY

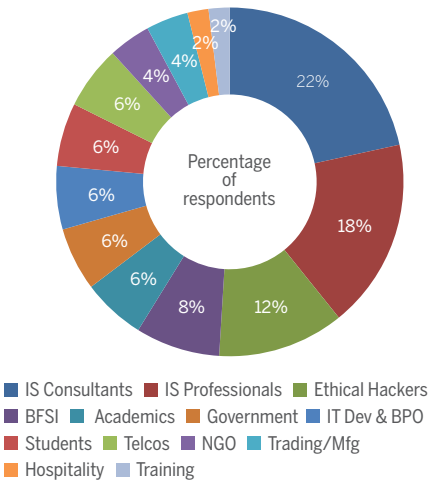
India is recognized as a global leader in the technology domain. The prevalence of technology in every aspect of life in the country is growing exponentially, keeping pace with global trends. Gigantic projects like UIDAI-Aadhaar, CCTNS, NatGrid, NPR and state/ national eGovernance initiatives are leveraging technology to reach out to the remotest parts of India. One by-product of this spread of technology is the rise in electronic crimes and frauds.

Much has been done at various levels to deal with cybercrimes and security incidents, but something seems to be missing still. To identify the missing factor, we surveyed a large number of professionals in IT, IS and other domains, requesting them to share their **top five India-specific concerns** in three segments:

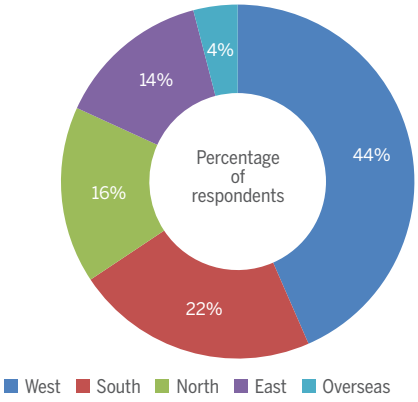
- The Nation
- The Corporation or Business
- The Citizen

Respondents were asked not to list out the risks and threats usually found in security reports but to think of the missing strategic, operational, tactical, behavioral and cultural weakness. This report presents the views and observations of the informed Indian professionals who face systemic shortcomings and a general lack of awareness of impending threats on a daily basis. Data for the survey was collected through an online form: http://goo.gl/VFNqm

Respondent Profile




Geographic Distribution of Respondent Sample




The unstructured survey responses were segregated and thoroughly analyzed to arrive at the Top 5 concerns in each category. Some interesting survey highlights are given below:

- 89% of the total respondents expressed grave concerns about the lack of awareness and the need for more security knowledge.
- Leadership at the government and corporate level must step up to learn and understand technology and lead by example. Although it has been 13 years since the IT Act was promulgated, the technological illiteracy in government and business is appalling. Trouble will not disappear by ignoring it; we have to wake up to critical issues such as poor infrastructure, espionage, counter-productive policies, and capacity and skill shortages.
- Government, corporations and people have to change the way they think and act about issues related to technology and internet. The virtual world is a new frontier where the assumptions of the 'real' world do not always hold true.

# NATIONAL ISSUES

## AWARENESS

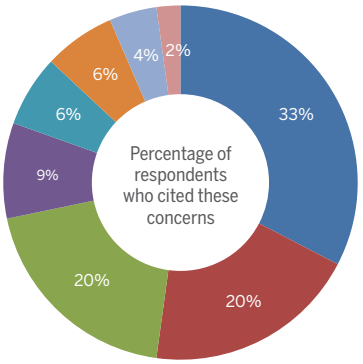
Awareness is the most abused word in the InfoSec lexicon. Every 'expert' swears this as the best and most effective antidote for InfoSec ill, but a few have walked the talk or done something constructive. Awareness remains a pipe dream – to be smoked in public, lamented in private.

This was the one common area of concern in all submissions, and it appears in many variations: lack of training, lack of informed policy makers, apathy, indifference, ignorance, arrogance, lack of acceptance of criticism, the perception of a lack of willingness. Amongst those who cited Awareness as a concern, close to 32% mention 'Lack of Training' as the key concern. 'Absence of informed policy makers' and 'Perception of lack of willingness' (20%) followed as two other main concerns. A lot of attention is given to the shortage of information security professionals in the country – but little is done to solve the problem. Aging technology assets are widespread, and planned policies greatly lacking across the establishment. Compounding this concern is the indifference to cyber security risks, technical naiveté, ignorance, and the lack of willingness to take action. When the government lacks expertise and knowledge, it should be open to invite contributions from civil society. High levels of arrogance in the establishment and the total lack of acceptance of any form of criticism is of grave concern on this front. Demonstration of demonic reactions by government, bureaucrats and (politically connected) individuals and the continued lack of empathy provide ample evidence of this attitude.

AWARENESS REMAINS A **PIPE DREAM TO BE SMOKED IN PUBLIC**, LAMENTED IN PRIVATE

India is suffering from internal strife, cross-border aggression and illegal immigration. It is critically important to address cyber security concerns on all fronts at one go. There are too many wrongs happening. For all we know, there may be a security tsunami rising quietly.

Awareness related concerns



## OBSESSION WITH CONTROL AND POWER

Obsession with control and power is the hallmark of politicians and bureaucrats. Every effort is made to suppress dissent. In this context, the national executive must reexamine issues like:

- Central control
- Inter-department rivalry
- Turf wars and jurisdiction issues
- Outdated laws and lack of knowledge (or understanding) in the law enforcement agencies
- Counter-productive policy measures
- Delayed response to disclosures
- A discouraging attitude

Central control is proven to be good for cyber security control, but unfortunately, it is in often in the hands of an officer with no interest in technology.

Archaic laws and the law making process need a reality check. While technology and life have changed over the past decade, we continue to live under the yoke of century-old laws. Even newer laws such as the IT Act continue to disappoint in enforcement. Lawmakers have to understand the medium (the internet) for which laws are enacted, and the legislation must include a vision for the future. Inspiration is not far away if we look at the Constitution – farsightedness and public good are enshrined in the document.

A discouraging attitude towards the citizens' needs and counter-productive policy measures demonstrate arrogance and should be curbed with good governance and policies. Technology risks, threats, and incidents require quick attention. A solution to this can be a National Security Organization as an additional constitutional wing apart from the Legislature, Executive and Judiciary.

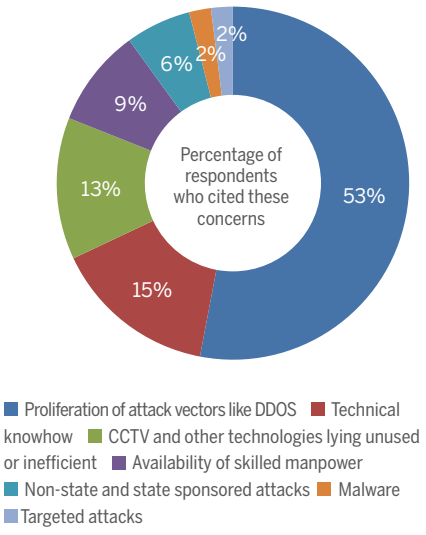
INSPIRATION IS NOT FAR AWAY IF WE LOOK AT THE CONSTITUTION — **FARSIGHTEDNESS AND PUBLIC GOOD** ARE ENSHRINED IN THE DOCUMENT

As a nation, we have successfully reinvented ourselves throughout the centuries under different rulers, religions, and languages. In the present day and age, internet technology demands a change of mindset and this has to first happen at the national executive level, setting the tone at the top.

## TECHNOLOGY

Technology, surprisingly, was not a grave concern area for our respondents! Its blind acceptance is what troubled them more. If the world is deploying some new technology, it is quickly and blindly included in our system without thought about the need, capability or localization.

Technology Concerns




The rapid growth of technology itself is responsible for the rising risks and threats. The scenario is not pleasant when there are obvious weaknesses in technical knowhow, availability of skilled manpower, proliferation of attack vectors (like DDOS , botnets, malware, etc.), non-state and state sponsored attacks, and targeted attacks.

Amongst those who cited technology concerns, 53% expressed 'Proliferation of attack vectors like DDOS' as a major issue. '(Absence of) technical knowhow' (15%) and 'CCTV and other technologies lying unused or inefficient' (13%) were the other major technology-related concerns expressed by respondents.

Though India has a vast pool of IT talent, when we get down to the brass tacks, there seems to be a lack of technical knowhow. Time and again, teams have to depend on overseas experts for specialist skills! The problem is evident when departments blindly implement technologies having been sold on the features or just because some other governments have purchased them or because the world is talking about them. There are numerous instances of compromise and national loss due to unused or defunct systems.

Although the shortfall of skilled InfoSec professionals has been highlighted at the highest levels of the government, nobody seems to be serious. Even though hiring is based on need, these departments are usually short of funds or are not given hiring plans. How is anyone expected to close the capacity gap with a hiring freeze and lack of executive / budgetary support is anyone's guess.

THE RAPID **GROWTH OF TECHNOLOGY ITSELF IS RESPONSIBLE** FOR THE RISING RISKS AND THREATS

While technology provides tremendous computing power it also brings new risks to one's doorsteps. As a nation, we must wake up to the realities of the damage that can be wrought by various threat vectors as mentioned earlier.

## IGNORANCE, CAPABILITY AND LEADERSHIP

The speed of change in the world of internet and technology has to be matched in thought and action. Else, we will soon see a steep decline in preparedness and spend a lifetime playing catch-up.

Espionage is real, played subtly, using tools like social engineering, APTs, malware and botnets. There is also the high level of dependency on foreign equipment and technology knowhow; so how does one know how safe one is? Cloak-and-dagger is passé; now is the age of 'cloak and keyboard'.

**Urgent action needed**

International research groups have exposed espionage networks operating on Indian national infrastructure on multiple occasions. Lack of significant reaction demonstrates the missing large-scale counterattack capability, infrastructure and leadership weakness.

We are surrounded by hostile neighbors in cyberspace too. Large-scale destruction from cyber attacks has been seen all over the Middle East – there is no way we can say that we are not vulnerable.

### CLOAK-AND-DAGGER IS PASSÉ; NOW IS THE AGE OF CLOAK AND KEYBOARD

We often see knee jerk statements from government sources, showing the reactive nature that governs national security thought leadership. This has to change to a mature planning process.

In the absence of cyber security capabilities, we stick our head into the sand wishing the problem will go away. This is evidently demonstrated in the slow pace of action (or inaction), the lack of funds for hiring and capacity creation, and the low levels of preparedness or urgency.

## DATA OBSESSION

We once lived in a 'license raj' where we had to provide data to the government for all types of things. The more files and papers we had, the greater our importance. And the more information we gave, the more the establishment demanded – it was like the mythical *Bakasura* [2] – never satiated and not under control till the day good triumphs over evil.

Our respondents are concerned about the lack of control over the private data collection entities, the obsession with data, and multiple data stores being created by all. The national obsession with data is well known – we have lived and grown up with ration cards, voter cards, domicile certificates, caste certificates, BPL [3] cards, KYC [4], UID [5] and NPR [6]. Every scheme requires citizens to submit new forms filled with the same data.

### DATA COLLECTION ENTITIES FOLLOW THE EXAMPLE OF LAXITY DISPLAYED BY THE GOVERNMENT

Extensive data resides in systems at the state and the national level. This can be merged and mined to create joint resources at the national level and be channeled into creating resilient and secure databases and policies – the resulting resource savings will be colossal. In developed countries, a single number is allotted to an individual at birth and remains valid through the lifetime of the individual – with safeguards that have matured over the decades.

The government has demonstrated its lack of control over citizen data with the absence of a firm policy statement related to handling of data and its purpose of use. As an example, Aadhaar was announced as a voluntary scheme, but every day there is a new announcement where Aadhaar is declared to be compulsory for one or the other basic service, such as bank accounts and cooking gas connections.

Ironically, a citizen has no choice but to submit to the establishment when it comes to their data collection exercises. If a person does not want to enroll for UID, she / he will be excluded from the banking system despite the government's assurance that UID is not compulsory for a bank account. On the other hand, passports are not accepted in courts where the authorities demand a ration card for personal identification. Even at this nascent stage, there are regular reports of fraudulent registrations and lax handling.

Private data collection entities follow the example of laxity displayed by the government. In the absence of privacy legislation, the banks, telecommunications and insurance companies show scant respect for personal identifiable information (PII), and blatantly share or sell it. Their nuisance value was demonstrated when even the Commerce Minister received spam calls during a Cabinet meeting. During our survey, more than 60% respondents cited fraud, identity theft, and data security as significant national concerns.

[2] **Bakasura:** A demon described in the Hindu epic, *The Mahabharata*. He forced the kings in the vicinity to send him food and provisions which he devoured along with the men who carried them. Was killed by Bhima in a fight.

[3] **BPL:** Below poverty line

[4] **KYC:** Know your customer

[5] **UID:** Unique Identification

[6] **National Population Register** (NPR) is an initiative of the Government for registration of citizens.

# CORPORATE CONCERNS

## AWARENESS

The problem with this area in Information Security is that everyone knows that it should be done. Everyone talks about it, but does nothing about it, except–talk!

Every respondent who participated in the survey mentioned lack of adequate awareness about Information Security as a critical issue with India's corporations. Close to 7% respondents attributed lack of awareness to the attitude that:

- Information security is more about compliance than risk containment
- Awareness programs are clubbed with training
- Awareness is not really built into corporate culture

In corporations, 'security awareness' is reduced to running a program rather than deriving value from it. A shift in mindset is needed here. This relates to people, process, technology, continuity, availability, and confidentiality, and should not be considered only for compliance.

### TRAINING AND AWARENESS HAVE DIFFERENT OBJECTIVES **AND MUST BE TREATED DIFFERENTLY**

The organizations' CXOs should delink awareness from training. It is critical to make the move towards building a culture of safe computing (safe information management and security) in the same manner as executive management works to build an aggressive culture for growth through sales, innovation, and customer satisfaction.

Training and awareness have different objectives and must be treated differently. Metrics for each has to be different, but it is not so currently. Awareness as a (soft) control suffers, and delivers no value.

## INFORMATION SECURITY MANAGEMENT

Information security management is of great concern to respondents. It appears that the essential tenets of an InfoSec management system are themselves a source of weakness, exposing the organization to threats and risks.

The areas of highest concern are poor policies, weak audits and compliance, L-1 purchasing, certification for the sake of certification, lack of monitoring, rogue and privileged accounts, and more. The general consensus is that corporations must responsibly ensure strong processes for IS management.

IT IS EASY TO SET UP AN ISMS AND GET CERTIFIED BUT INFORMATION SECURITY MANAGEMENT IS **HARDLY ABOUT GETTING CERTIFICATES**

A number of IS consultants and professionals wrote about lack of effective policies in corporations. Shoddy cut-paste jobs provide poor policy documents and when this is combined with weak audits, compliance, and enforcement, we have the ingredients for an IS disaster in the making.

**Throw peanuts, get monkeys**

The private sector is inspired by the public sector and has etched the L-1 mindset into their procurement processes. The lowest bidder who walks away with the contract may be the least capable or the most corrupt. The buyer suffers because of this L-1 purchase, but lives with the pain and is even found lobbying for a security award to cover up the failures. Hiring and purchase revolve around 'negotiation skills', a politically correct term for bringing in the lowest bidder without thought about quality.

Along with awards, organizations seek certificates for the sake of certificates. Many certifying bodies will oblige too with low fees and weak audits. The result is a framed certificate to hang on the wall, having less value than toilet paper in terms of effectiveness or usefulness.

A cliché in InfoSec conversations is that the insider is the biggest threat but our respondents caution readers against privileged users and senior management. Other vulnerabilities are the convenience user accounts created by the tech team(s), and the accounts which are 'orphan' or those that remain undeleted even after the users leave the organization. All these are easy pathways into the system and very few companies have a grip on the problem. Logs are usually not enabled because of additional hardware investment requirements, but even when logs are available, no one seems to be looking at them!

It is easy to set up an information security management system (ISMS) and get certified but information security management is hardly about getting certificates. If one starts from the bottom and builds up, it will work. Unfortunately, everyone is looking for shortcuts and often overlook the essentials.

## WEAKNESSES DURING IMPLEMENTATION

The implementation of any asset or process must be a properly planned activity entrusted to qualified teams. While there is evidence that procedures are followed for security implementations, something or the other is often missing, creating a weakness in the security ecosystem.

**TIME AND AGAIN, CORPORATIONS HAVE BEEN VICTIMS** OF BREACHES THROUGH SYSTEMS THAT ARE NOT UPDATED OR PATCHED

Our respondents identified inefficient security implementation, weak process for patch management, piracy, pirated software resulting in malware, and encryption as major concerns. The first step must be firm and strong, but when this step itself is flawed, one can be assured of mayhem. Inefficient security implementations result from wrong first steps. Weak controls, workarounds, privilege mismanagement, lack of will to enforce policies, me-too technologies, and a lack of strong hiring practices are amongst the many wrong practices that result in weak information security management system (ISMS).

Patch management should be by habit but the real habit observed is procrastination. Time and again, corporations have been victims of breaches through systems that are not updated / patched.

It is common knowledge that there is large-scale acceptance of piracy across the country. Cracks, keygens, dubious license keys and installers are exchanged across networks without thought about IPR violations or the threat of malware entering corporate networks, or the risk of penalties arising out of non-compliance.

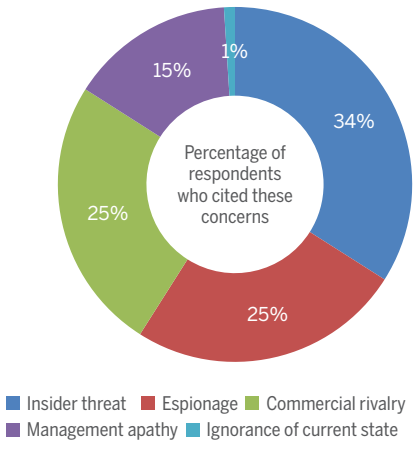
## 'IT CANNOT HAPPEN TO ME' SYNDROME

This is a common affliction across organizations — the small guy thinks he is too small to be of interest to a hacker, and the big guy thinks he is too strong to be attacked. Both fail to realize that the joke is on them and that a blackhat may already have them in his crosshairs waiting for the right time to pwn [7] them.

While we are aware of the dangers lurking around us, our sense of fatality prevents us from addressing concerns such as espionage, commercial rivalry, insider threats, management apathy, ignorance of the current state, etc.

'It cannot happen to me' syndrome was opined to be a significant concern by a whopping 51% of the total respondents. Within these, 34% cited 'Insider threats' as a major concern while 25% each cited 'Espionage' and 'Commercial rivalry' as other serious concerns.

'It Cannot Happen to me' syndrome




THE **SMALL GUY THINKS HE IS TOO SMALL** TO BE OF INTEREST TO A HACKER, AND THE BIG GUY THINKS HE IS TOO STRONG TO BE ATTACKED

Espionage has become easy for the smart and aggressive operator, and the key threat vectors to look out for are data theft, phone tapping, keyloggers and advanced malware. Executive management must realize that the results of successful espionage are felt by shareholders and the nation and that it is not merely a commercial loss for the company.

Taking care to harden systems and increase monitoring will help contain loss of IPR, contracts, and revenue. Survey respondents believe that little is being done about silent attacks on management assets in the form of espionage or downright damage, and this is due to management apathy – which is a manifestation of a different type of insider threat.

We have addressed insiders and senior management in a different context but apathy is a weakness in thought and leadership that leaves the organization open to pillage and plunder.

[7] **Pwn:** In information security, to pwn is to compromise or control another computer / application / site / gateway device.

## UNDERESTIMATION OF TECHNOLOGY

Underestimation of technology is another problem area driven by ignorance at the top due to the absence of professional threat / risk intelligence. Technology risks or benefits are usually intangible and claims of loss or success are always regarded with suspicion.

Risks and threats created by technology cannot be wished away or ignored, especially vectors of high concern like botnets, virus/APT, no logs, ransomware, rogue and unauthorized software installations, slow adoption of new technologies, etc.. The survey respondents feel that corporations are not paying attention to the risks they face and that there may be a heavy price to pay in the due course.

SURVEY RESPONDENTS OPINE THAT **WE SHALL SOON SEE RANSOM DEMANDS** AS IT IS A SIMPLE AND EASY VECTOR

Incidentally, of the total number of respondents, 12% cited 'Hacktivism' as a rising information security concern whose threat is underestimated by India's corporates.

From MMSes and morphed pictures, we are seeing criminals moving to identity theft and targeted financial crimes. Botnets, ready-to-use viruses, 0-days, APTs and such tools can be easily purchased online along with required support and help for successful use. This makes it easy for anyone to launch an attack against any corporation; unfortunately, most are unprepared for a technical onslaught.

The issue is with technology being taken for granted and with managements seeing it in the form and color that is comfortable to them. This is the big concern as managements often underestimate the resultant damage. Users freely install rogue or unauthorized software and thus provide backdoors into the corporate infrastructure. When logs are not collected and analyzed in real time, malicious network infiltration goes unidentified.

Survey respondents opine that we shall soon see ransom demands as it is a simple and easy vector. Crime gangs will find it a cakewalk to move from real life kidnappings to diginapping in the virtual world, which will be more lucrative and anonymous. Ransomware exists, is the message for the corporate head in the sand, and it is time to take immediate measures for protection against such threats.

Another culprit identified by our respondents is the slow adoption of new technologies. The pace of adoption is governed by the principle of denial – if the new technology is free, adoption is quick, but if money has to be spent then it is wished away until the world has adopted it.

Technical threats or risks are not visible and when the user feels that things are 'taken care of' or 'okay' once the machine is powered down! Managements must stay away from such delusions and make every effort to learn and understand the risks built into the operations fabric of the corporations. It's time corporations encouraged technology and security schooling for professionals who are not related to technology or InfoSec.

# THREATS TO INDIVIDUALS

## SOCIAL MEDIA

The great Indian joint family has been resurrected on the pages of Facebook, Google+, and others. Cousins far removed can see each other from birth and exchange their first words. Kids have accounts before they are born, forget walking, talking or burping.

With all this good happening in our social lives, our respondents (who are active on social media) say this is a huge concern area for the average Indian citizen – the Indinetizen. Users have yet to realize that there are risks to individual privacy arising from government monitoring, stalking, misinformation through social media, uninformed children activity, and much more. 'Misinformation through social media' was seen as the key issue by 14% of the total respondents.

Social media and online posts must be used intelligently and with a great deal of thought. We may guard our personal lives closely, but that privacy is easily breached when we or our friends post personal information and pictures.

Social media has brought everyone on the same platform – the government, the criminals, the gullible, the greedy, as well as the naïve and harmless good guys. The internet is called a level playing field but it is a virtual toy store for criminals and mischief mongers who can stalk, steal identities, run scams and damage reputations.

Our respondents are concerned about the well-being (financial, mental and physical) of the innocent user who is being targeted by criminals or the government machinery for their own purposes.

**MISINFORMATION THROUGH SOCIAL MEDIA** WAS SEEN AS THE KEY ISSUE BY 14% OF THE TOTAL RESPONDENTS

Children especially are high risk targets and a majority of parents are unaware of their children's internet activities. Parents take great pains to oversee their kids' playground activities, but overlook the cyberspace where kids are alone, befriend the strangers, accept gifts from them and inadvertently put their lives in danger.

The risk is not only for children who are snared with gifts, but teens and adults who post sensitive content (personal, family, or business related) that may be considered objectionable and illegal. Claiming ignorance of law will not help reverse or avoid damage.

## LACK OF SUPPORT

Lack of support is pervasive. Governments and corporations are struggling to understand and tame the phenomenon called the internet, and the so called know-it-alls provide quick fixes and remedies or snake oil. The individual struggles to make sense of right and wrong in the virtual world.

Law enforcement agencies are a critical component in the support system and must work with media and professionals to bridge perception gaps and provide the necessary skills and awareness to the police force and build trust through protection of the individual. Many state police departments have set up helplines and support groups for citizens; these activities need to be expanded. A common national helpline connected to a state network for local language services is the way to go.

LAW ENFORCEMENT AGENCIES MUST WORK WITH MEDIA AND PROFESSIONALS **TO BRIDGE PERCEPTION GAPS AND PROVIDE THE NECESSARY SKILLS AND AWARENESS TO THE POLICE FORCE** AND BUILD TRUST THROUGH PROTECTION OF THE INDIVIDUAL

It is essential to have correct information from media, proper guidance from the infosec professionals, elimination of the lack of trust and awareness in police by providing dependable and responsive system to report any crime or situation.

Support from the media is essential as even media is all pervasive. This is expected in the form of responsible reporting and reliable information about risks and threats. Media houses have to rise above TRP or circulation considerations and undertake this as a social cause. Assistance to this cause can be obtained from infosec professionals; a majority of whom are always willing to help.

The common citizen is forgotten in the chase for profit when ironically, it is the same common citizen upon whom business and politics are dependent. Without support, the citizens will be fleeced by criminals and it is critical to reach out to them at this nascent stage, while the going is good.

## UNSAFE SURFING

Unsafe surfing is like flying blind. In blissful ignorance, the individual glides through hyperlinks; believing every word to be true, trusting every pop-up that announces a virus attack, is easily sucked into porn sites, and does not believe in paying for software because cracks are easily available for download!

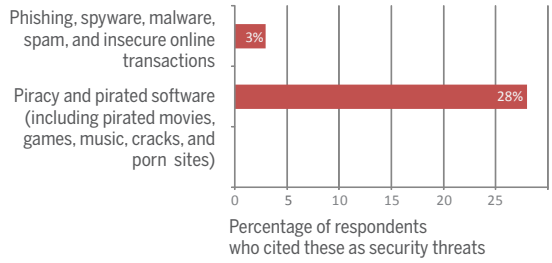
This is a cultural issue and calls for change from within. It has to do with the way individuals think, their moral values,level of ignorance, and awareness about piracy and pirated software, movies, games and music, software cracks, moral values, porn sites and about threat vectors like phishing, spyware, malware, spam, and insecure online transactions. During our survey, as much as 28% of the respondents thought 'piracy and pirated software (including pirated movies, games, music, cracks, and porn sites)' as major online threats. Phishing, spyware, malware, spam, and insecure online transactions were specified as the other important threats by 3% of the respondents.

IT WILL BE WRONG TO BLAME ONLY THE BELIEFS OR MORALS OF INDIVIDUALS AS **EVEN THE STRONG AND ETHICAL CAN BE TRAPPED**

The Indinetizen is her/ his own enemy. Pornography is as big as piracy on the internet and is in our face directly and indirectly through spam, phishing and other means. Our respondents urge surfers to stay safe. It is important that the individual stays away from bootleg stuff or porn sites because they are the carriers of dangerous infections or worse.

It will be wrong to blame only the beliefs or morals of individuals as even the strong and ethical can be trapped. The individual has to learn to recognize such attacks / threats and duck them.

Threats to Online Surfing



## AWARENESS

Lack of awareness is the root cause of the evils pervasive in the internet and technology environment. The survey respondents have highlighted issues like a lack of general awareness, legal issues, lack of knowledge about technology and gadgets for first level configuration, as key areas of concern.

Nearly 21% of respondents mentioned lack of general awareness as the primary cause behind security threats in the case of individual IT users. We can call it lack of general awareness or apathy or arrogance – and the botnets seem to thrive on apathetic systems that are mostly individual owned making India a fairly large contributor to the global botnet population.

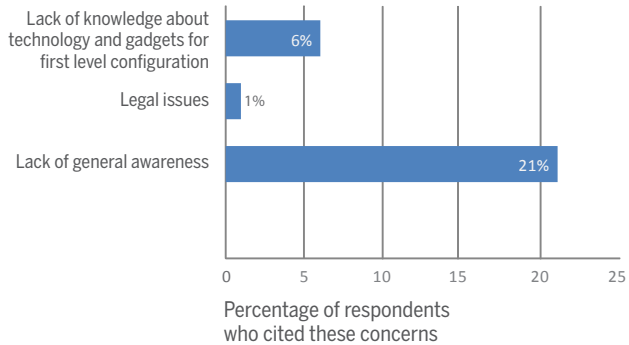
The concern is that individuals seem unwilling to learn the fundamentals of cyberspace, considering it beyond their understanding. This mindset has to change and individuals must realize that this is not about technology but about their own safety. On the one hand there is a lack of awareness and desire to learn and on the other hand the ignorance about illegal activities as defined by the IT Act.

ONE MUST USE THE INTERNET WITH ALL FACULTIES ON HIGH ALERT AS **THERE IS DANGER AT EVERY CORNER**

Many first timers caught engaging in cybercrime are surprised to learn that their 'minor' actions could land them in jail! It is essential for everyone to have basic knowledge about the technologies they use. Individuals purchase computers and software and then do not bother to patch, update or apply security fixes, as these are perceived only as irritants or 'nags'.

One must use the internet with all faculties on high alert as there is danger at every corner in the same manner as in real life where danger can be in the form of speeding cars, potholes, multistoried fire traps, falling bridges, and so on.

Lack of Awareness as a Concern



## INNOCENCE, GREED, AND AVARICE

Innocence, greed and avarice are human weaknesses that are easily exploited, and schemes and schemers abound on the internet to exploit them. The individual must exercise caution in online life, and be alert and quick to eliminate these weaknesses.

While it is easy to wish away one's innocence or greed it is difficult to execute the wish when faced with a perennial onslaught of attacks such as social engineering, spear phishing, financial frauds, hoax generation frauds, lottery, 419 frauds, and transnational crimes.

THE INTERNET IS A POWERFUL MEDIUM THAT **MAKES IT EASY TO REACH OUT TO AND MOBILIZE** THE MASSES

Social Engineering is a trick as old as the world itself, from the time Eve was enticed into eating the Fruit of Knowledge to present-day internet crimes. Cyber criminals take advantage of the innocence and naïveté of human beings to extract information for attacks, and to further their own nefarious activities. Social engineering usually leads to the next level of attacks called spear phishing. In this case, the person who has been 'engineered' may become the recipient of targeted attacks designed for any particular objective – infiltrate an office network, steal data, steal personal information, compromise net banking credentials, etc. Or their contacts and friends are spammed for 'assistance' and money.

Greed and avarice are the evils as much in virtual world as in real life. Lottery fraud, Nigerian 419 scams, transnational crime, and Ponzi/ MLM schemes are everyday happenings designed to prey on the gullible and the greedy.

The internet is a powerful medium that makes it easy to reach out to and mobilize the masses. Governments have been overthrown by such movements. The same power can also be misused by antisocial or anti-national elements to spread terror and unrest; individuals have to be careful and proactive in reporting about and rooting out such elements.

# CONCLUSION

First off, we would like to thank all the people who helped spread the word about this report and those who have responded and supported this initiative. There also are many who encouraged and helped us in the analysis, and in crafting this report.

The scientist in you may opine this is qualitative, but then there is no other way to distill a huge database of submissions to extract a few lines or words of wisdom that will guide the Nation, the Corporation, or the Citizen. This is the result of hours and days of pouring over the submissions, extracting the important ones, fighting over choices or semantics, laughing at the funny opinions, crying over facts, and finally arriving at a few lines that pack the Indinetizen's potent message.

Through this report, we intend to help you assess your preparedness (or lack of it) to deal with the issues mentioned here or to face them. These are pieces of a whole at the bottom of the pyramid. If you have built your palace of information security management system (ISMS) on a foundation with missing blocks, you only need your child to tell you about the excitingly dark future that awaits you. While putting this report together, we did not want to pick up holes in one system or the other. Examples are quoted without any such intentions.

This report is about India and is derived from respondents who are working in the security domain. The observations, findings and pronouncements relate to the Indian work and establishment ecosystem – solutions may be typically Indian but are universal in their application. We welcome constructive feedback and will strive to improve upon our work. We also welcome volunteers who can help us in our work on the next report.

We hope that this report will provide you with the basics that need to be taken care of. Information Security is increasingly critical to keep us safe and we must make every effort to safeguard ourselves, our corporations and the nation.

INFOSEC IS CRITICAL TO KEEP US SAFE AND **WE MUST TAKE EFFORTS TO PROTECT** OURSELVES, OUR CORPORATIONS AND THE NATION

We also hope that this report will appeal to the practical CISO who is more concerned about functional and security effectiveness rather than crunching percentages and numbers about events in different companies, verticals or countries.

The good news is that enabling essential security practices is not rocket science. All it needs is a dollop of common sense over ethics and basic housekeeping practices, all the while taking care not to overlook small things when working on the big picture.

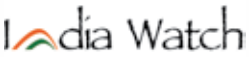
# ACKNOWLEDGEMENTS

This report would not have been complete without the valuable contribution of the established professionals in and out of the Information Security domain who reviewed it. We wish to thank these professionals, friends and associates who have contributed to the effort with advice and effort. A few people one must mention are Mrs. Sushma Ramchandran, an eminent journalist; Mr. Pavan Duggal, eminent Cyber Law Advocate; Mr. Vickram Crishna, a well known Privacy advocate and Mr. Hitesh Dixit, CISA, a Finance Professional employed in the BPO industry. We used resources public and private to reach out to the information security community through social media and mailing lists, notable among them were the Sysman-CCC News, Null, ClubHACK Mag, India InfoSec Group and LinkedIn.

Support has been extended for this report by the following organizations / individuals:

# NOTES

# CONTACT INFORMATION




www.indiawatch.in

Engaged in India centric research, we are a knowledge organization specializing in Management and Security of Information / Data and related People, Processes and Technology. We excel in providing strategic and tactical thought leadership to governments, public and private organizations. Our Body of Thought and Solution is the output of our conclave of cross functional professionals and industry leaders. We are continually working in areas to contribute in the interest of national security, public safety and business resilience.

**Email:** top5-2013@indiawatch.in

**Feedback:** www.indiawatch.in/top5-2013-feedback


www.clubhack.com

ClubHack is the first Indian Hacker's conference, which is now going international. ClubHack also started India's first monthly security journal. It is synonymous with the information security profession in the country. ClubHack is motivated by the spirit of community and is largely responsible for popularizing open learning in the technical InfoSec domain. Our events, articles, videos and presentations are popular across all sections of society and our audience is global. A truly Indian knowledge hack through the times!

**Email:** top5-2013@clubhack.com

**Feedback:** www.clubhack.org/top5-2013-feedback