

# Cybersecurity vulnerability in Indian banks

Going beyond regulator compliance for effective operational risk management



# CYBERSECURITY FRAMEWORK IN BANKS

***“The number, frequency and impact of cyber incidents/attacks have increased manifold, underlining the urgent need to put in place a robust cyber security/resilience framework in banks and to ensure adequate cybersecurity preparedness among banks on a continuous basis”***

Reserve Bank of India’s [recent communication](#) to Banks in India.

Banks and financial institutions are seized with newer forms of threats to the safety and security of their data, a critical asset for any organization. In the age of Internet of Things, criminal activities and data theft have also gotten smarter and savvier, with criminals increasingly using technology to break technological barriers within the banking system.

In light of the low entry barriers to cybersecurity attacks in banks, it is incumbent upon them to invest in systems and technologies that go beyond merely pre-empting an attack.

This White Paper explores:

- ▶ The genesis of cybercrime in India.
- ▶ How it’s only grown over the recent years, especially 2011 onwards.
- ▶ How increasing reliance on technology makes it harder to detect and monitor financial crime taking place online.
- ▶ Recommends a few solutions that banks can and should invest in if they want their financial assets to stay safe and secure.

01  
CYBERCRIME:  
THE GROWING  
MALAISE

02  
CYBERCRIME  
ON THE  
UPSWING

03  
INDIA AND  
CYBERCRIME

04  
ERRING ON  
THE SIDE OF  
PRECAUTION

05  
RISK  
FORTIFICATION  
IS KEY

06  
WEAPONS OF  
CYBERCRIME  
DESTRUCTION

## 01 CYBERCRIME: THE GROWING MALAISE

**India had 42 million cybercrime victims, 52% of whom suffered financial or some other kind of loss due to hacking, scams, fraud and theft.**

Recently all banks in India were sent a [communication](#) by the RBI to upgrade their security standards and implement a novel cybersecurity system, along the governing lines of the RBI. This mandate is routine and it is a norm for the Central banking world's governing body to introduce new and improved laws for regulatory compliance.

While all of this may seem rudimentary on the surface, it gives one cause, to ponder and reflect on the underlying reasons for such a mandate. Is there a deeper malaise that affects the banking sector where banking safety norms and guidelines are concerned? If that is so, what is the prescription for such a growing malaise and how well are banks prepared, to tackle such malfeasance activities?

In fact after the first guideline for Cyber Fraud and Risk Management was released in 2011, the indications are clear as day, that cyber fraud across India is only increasing. As of June 2013, according to Norton reports, India had 42 million cybercrime victims, 52% of whom suffered financial or some other kind of loss due to hacking, scams, fraud and theft.

It automatically begs the questions:

- ▶ Can banks afford to turn a blind eye towards the RBI mandate?
- ▶ Is RBI's response harsh enough to tackle cybercrime?
- ▶ Should banks be more proactive in their approach to fraud?

The answers seem obvious, but surprisingly banks in India and elsewhere have depended on silo-based solutions that do not have the long-term view of an integrated, real time, cross-channel approach. More the merrier does not cut in the banking sector - more the channels, more the software products and unfortunately more the cracks through which vigilance measures can slip. Banks need to recognize the folly of relying on "after the fact" solutions and enforce solutions that "detect and prevent" as it happens.

However, we need to understand the scale of cybercrime in India and focus on some revealing statistics which will help everyone in banking to sit up and take notice. So where and when did it all start?

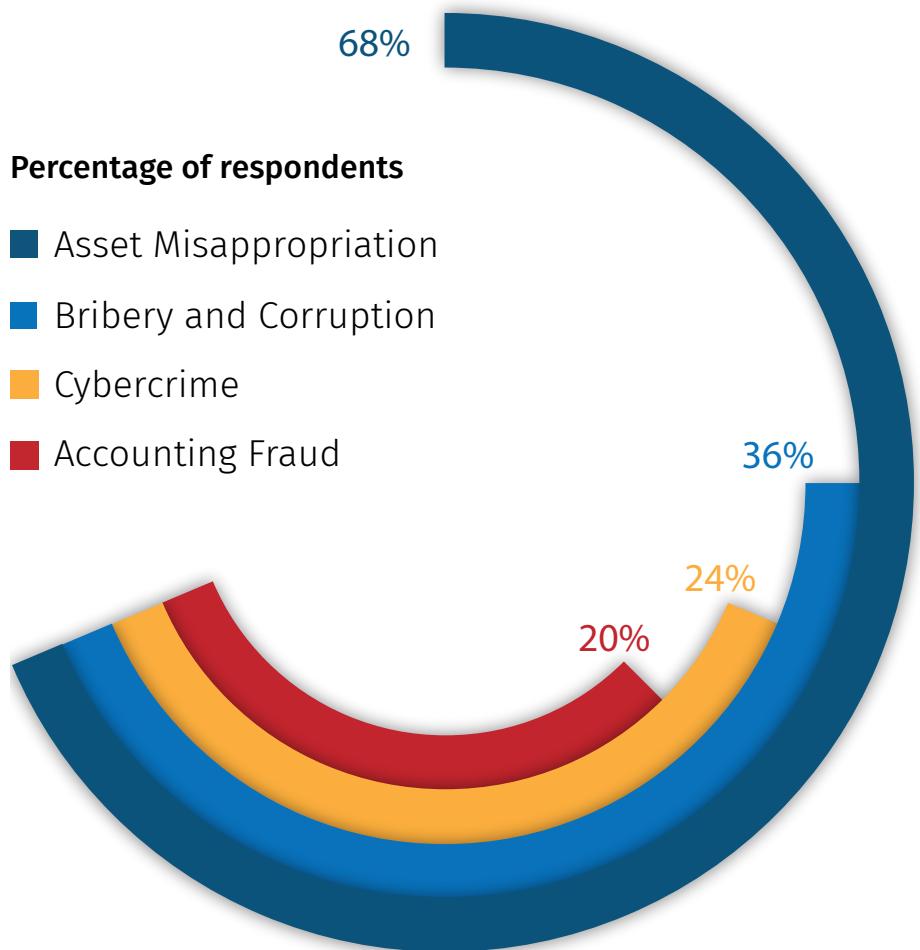
## 02 CYBERCRIME ON THE UPSWING

**In North America, according to a report by Boston-based analyst firm AITE Group, cybercrime was expected to cross US\$ 371 million in 2015 alone.**

2011: the emergence of a new era in banking technology whereby all our banking details could be easily accessed through electronic devices eliminating the need to be physically present at the bank for a large number of transactions. However, as reliance on technology increased, cybercrime also came into play. In 2011, in USA alone, cybercrime in banks accounted for US\$ 210 million in losses.

Meanwhile cybercrime had become one of the top four types of economic crimes across the world. To understand this spike in cybercrime, one needs to realize that the threat of cybercrime owes its origins to both, external and internal factors including unscrupulous entities. Cybercrime is a low-risk high-income crime enticing many, and banks with weak systems act like low hanging fruit proving to be an easy target for fraudsters.

### Economic crime experienced in India: 2011



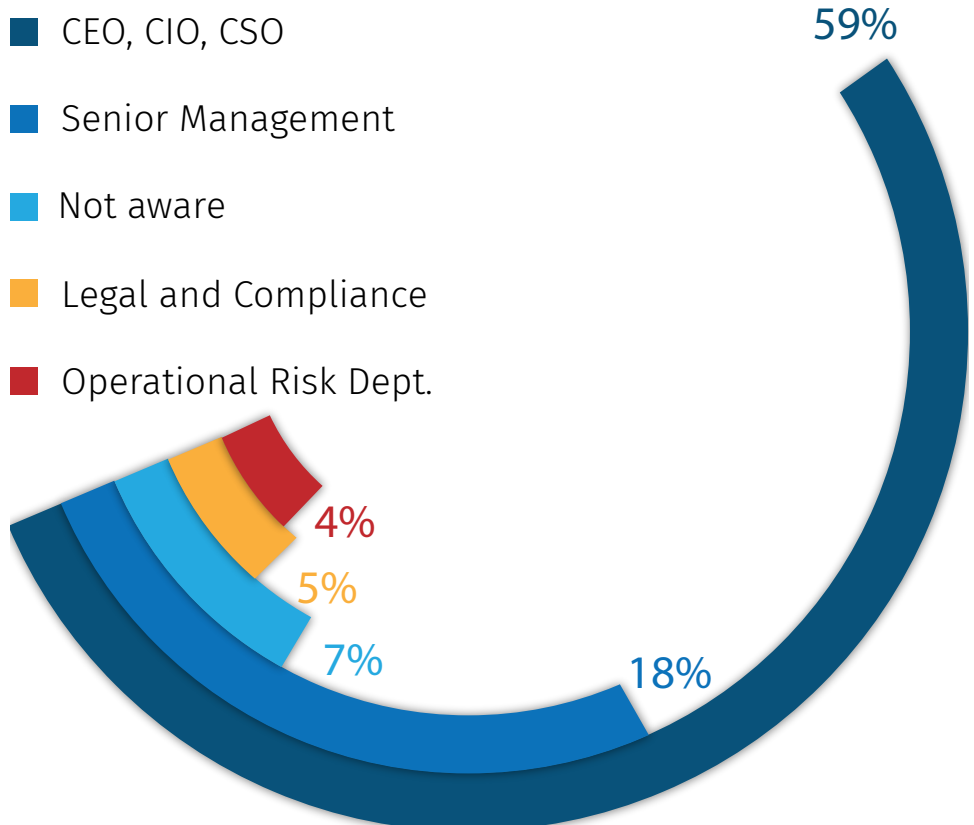
**The PWC report quoted: "It is much easier to be a successful bad guy than a successful good guy; a criminal who is successful in one of his 100 attempts will make off with a tidy sum. Banks on the other hand, must seek perfection in their attempts to protect themselves and their customers."**

The PWC report for Economic Crime in India for 2011 threw up some very revealing and alarming facts:

- ▶ Cybercrime in India was on the upswing and accounted for 24% while accounting fraud in comparison came in last at 20%.
- ▶ According to PWC, the situation was far grimmer. 10% in 2011 compared to 6% in 2009 had no knowledge if their organizations were affected by cybercrime.
- ▶ In 2011, 47% (i.e. 15 % internal and 32%, a combination of internal and external) respondents felt that cybercrime is an internal threat, while the remaining 58% felt the IT department was more susceptible to the threat.
- ▶ According to PWC, 59% of the respondents placed the responsibility of dealing with cybercrime threats on the CIO or the technology director.

### Ownership and responsibility of cybercrime: 2011

#### Percentage of respondents



**Majority of the banks realized that fraud had been committed post incident.**

Despite these alarming figures, about 80% of banks in India did not emphasise enough on Fraud and Risk Management solutions. Unfortunately, only 20% of all banks thought of fraud risk management as being an effective method of fraud control and a large number of these banks realized they had been victimized only after they received tip-offs, conducted audits, rotated personnel or via whistle blowers.

In an ever-growing globalised network of operations and transactions, with customers demanding convenient access from multiple devices, time zones and geographies, with banking now taking place not only in the precincts of a physical brick and mortar space but over the Internet with mobile banking and ATMs and POS systems, banks have to understand the vulnerability of relying on manual interventions or solutions that alert you to a financial crime after it had been committed.

- ▶ By mid-2013, cybercrime had claimed its first victim.
- ▶ According to a McAfee report, cybercrime had already cost USA alone, over US\$ 100 billion and claimed more than 508,000 jobs.
- ▶ By 2014, cybercrime was a Frankenstein monster and cost banks US\$ 300 billion globally. India wasn't far behind really.

## 03 INDIA AND CYBERCRIME

It shouldn't come as a surprise that while the world reeled under the cybercrime attacks, Indian banks too were exposed to the dark underbelly of financial cybercrime. According to Norton, as of mid-2013:

- ▶ 42 million instances of cybercrime were committed pan India.
- ▶ 52% of which faced monetary and other collateral losses due to scams and frauds.

80 people became victims of frauds every 60 secs.

42% of the financial loss was due to fraud.

7% of the total global cyber fraud was carried out in India.

India tops the table globally in terms of spam attacks, second in virus attacks and third in all other threats.

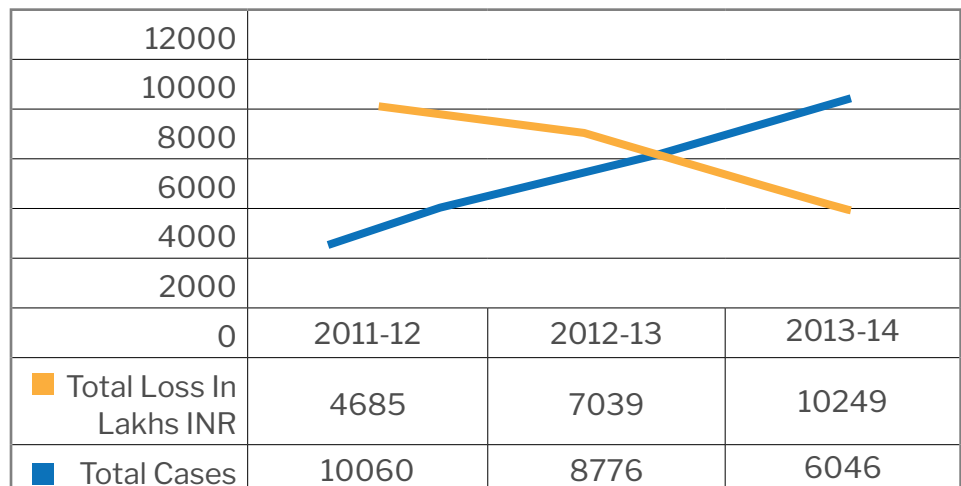
### Financial losses due to cybercrimes: 2011-2014

RBI/CBI reports	2011-12	2012-13	2013-14	Total
Loss due to Cyber Fraud (RBI) in Lakhs	3800	6700	5400	15900
Loss due to Cyber Fraud (CBI) In Lakhs	885	339	4849	6073
Total Loss In Lakhs INR	4685	7039	10249	21973

### Reported cases of cybercrime: 2011-2014

RBI/CBI reports	2011-12	2012-13	2013-14	Total
Cybercrime cases- RBI	10048	8765	6035	24848
Cybercrime cases- CBI	12	11	11	34
Total Cases	10060	8776	6046	24882

### RBI/ CBI Report: 2015



## 04 ERRING ON THE SIDE OF PRECAUTION

**A KPMG Survey on cybercrime in India in 2014 & 2015 uncovered how adverse and deep rooted the effects of it were in the banking realm. It revealed that close to 70% believed their institution was ill equipped to prevent cyber fraud.**

So what did all this mean for Indian banks and what was the Reserve Bank of India, the central policy-making body for the banking sector doing about it?

In 2014 the RBI published a new mandate: banks were asked to migrate to advanced Basel II-based systems. Indian banks reciprocated in a positive manner. They upgraded their Risk Management processes, systems and infrastructure. However, the Risk Management systems were still at a nascent stage and hence, vulnerable to different attacks, which the banks were well aware of. But in the larger scheme of things, erring on the side of caution was better than throwing caution to the wind.

### KPMG Report on cybercrime in India

Description	2014	2015
Cybercrime was perceived as major threat	89%	94%
Cybercrime was part of board agenda	30%	41%
Enterprises faced cybercrime in past year	49%	72%
Financial loss due to cybercrime	45%	63%
Financial sector primary target	58%	72%
External party involvement in cybercrime	84%	83%

### Some observations that surfaced in the KPMG Survey on cybercrime in India 2014-15

- ▶ Both internal and external factors are involved in fraud.
- ▶ Financial gain is the primary motive and industrial espionage being second.
- ▶ In both the years, 2014 & 2015 cyber risk assessment was not carried out while the primary focus of the board was getting latest technology.
- ▶ In both the years an overall risk assessment tool was absent in a majority of the banks.
- ▶ Close to 70% believed their institution was ill equipped to prevent cyber fraud.



**Less than 25% of the fraud losses were recoverable due to the excessive time taken to uncover the fraudulent activity.**

A 2015 Deloitte report on cybercrime in India reveals that besides core banking functions, several other channels of banking were also major targets for committing fraud. Internet banking, e-banking, ATM and retail banking were some of the key channels where financial crime could be committed easily. This same report also threw light on the fact that one of the top reasons for increase in incidents of fraud was a lack of risk assessment tools.

Besides financial losses, banks also had to tackle the issue of reputational loss and customers' anxiety despite following regulatory compliance. Orthodox processes such as an audit / reconciliation were notorious for taking inordinately long to complete their investigations. Ergo, positioning an intelligent, agile and reliable system with the ability to cross-pollinate data on a real time basis was the need of the hour for banks, if they were to plug the leak on financial losses due to cybercrimes and frauds.

While banks focused on prevention of cybercrime, malware and payment card fraud were also prevalent. Kaspersky Labs uncovered that approximately US\$ 1 billion was stolen from banks worldwide through malware attacks. According to the FFA UK report, payment card fraud accounted for 75% of UK fraud losses in 2015, most of which was 'remote purchase fraud' using card details stolen through data hacks and malware.

The writing was on the wall – fortify or perish. Banks all over the globe and in India had to cast aside their preconceived notions and wage a full-on battle to win the war.

### **Deloitte Report on cybercrime in India: 2015**

#### **Status of frauds**

- ▶ 93% respondents indicated that there has been an increase in fraud incidents in the banking industry in the last two years.
- ▶ More than half the respondents indicated that the banking industry has seen more than a 10% increase in fraud incidents in the last two years.

The Reserve Bank of India meanwhile has issued an ultimatum to Indian banks on cybercrimes, asking them to immediately report any breach of security so that the overall network is not compromised. The tough stance follows the reluctance of some banks to report such frauds in order to avoid negative publicity. The banking regulator has set a deadline of March 31, 2017, for banks to put in place a mechanism to report cyber attacks immediately.

**Deloitte Report on cybercrime in India 2015: 93% respondents indicated that there has been an increase in fraud incidents in the banking industry in the last two years.**

### Top reasons for increase in fraud incidents

- ▶ Senior management was lacking vision and leadership.
- ▶ Pressure of running the business.
- ▶ Collusion between external bodies and employees.
- ▶ Absence of potential risk assessment tools.

### Challenges in fraud detection

- ▶ Lack of complete awareness among staff, customers and other stakeholders.
- ▶ Lack of Integrated Solution throughout the bank.
- ▶ Lack of fast and adequate fraud detection tools.

### Major targets of fraud

- ▶ Internet banking
- ▶ ATM fraud
- ▶ E- banking
- ▶ Identity fraud
- ▶ Retail banking and
- ▶ Corporate banking

## 05 RISK FORTIFICATION IS KEY

**Around US\$ 65 billion was collected in fines, across banks in Europe and the US.**

Year 2016; the cracks in the various banking systems were slowly becoming visible. 2014 had already become the year of fines for US and European banks. Around US\$ 65 billion was collected in fines, across banks in Europe and the US. Most fines levied were due to money laundering and asset misappropriation with some of the biggest leaders in the banking firmament being incriminated. This phenomenon of regulators cracking down on banks became commonplace across the world. For instance:

- ▶ Latvia: Baltic International Bank fined US\$ 1.2 million (Money Laundering/Fraud).
- ▶ ABN AMRO fined Dh 2.3 million by the Dubai regulatory authority over money laundering systems.
- ▶ A UK bank had to pay US\$ 13.75 million in settlements with US regulators (Compliance/Fraud).
- ▶ A trio of regulators ordered a big bank to pay US\$ 34 million for deposit discrepancies (Money laundering/ Fraud).
- ▶ South African regulator imposed sanctions on 'Big Four' banks: lessons for overseas financial institutions (Compliance/Money Laundering).
- ▶ FCA fined Barclays £ 72 million for poor handling of financial crime risks.

While regulators were coming down hard on banks for various financial irregularities, the Reserve Bank of India intervened wielded its whip, figuratively speaking and started pulling up Indian banks for several cases of banking irregularities.

- ▶ RBI imposed penalties on 6 banks for regulatory lapses.
- ▶ RBI fined 2 prominent Indian banks over fake customers.
- ▶ RBI penalized 22 banks for violating KYC norms.
- ▶ Iconic Indian public sector bank fined INR 3 crores by RBI.

**Indian banks are resistant to change to new methodologies and employ silo-based approach to systems.**

While cybercrime was a contemporary threat and couldn't be wished away, bank regulators seemed to be telling banks to wake up and smell the coffee. Banks could no longer hide under a rock and pretend that financial crime was something that could be tackled with weak technological solutions or that reactive measures were enough to counter threats. Enduring frauds and resultant financial losses was no longer an option.

During this span of time, it was clear that Indian banks (like most other banking systems around the world) were burdened by a few shortcomings such as:

- ▶ Resistance to change to new methodologies.
- ▶ Each department looking at a customer differently rather than as a single person with multiple connections.
- ▶ Absence of early warning systems for possible breaches.
- ▶ Silo-based approach to systems.
- ▶ Viewing Anti-Money Laundering and Banking fraud as two different entities.
- ▶ Unwilling to expand the scope of technology to products and services in banking.
- ▶ Being reactive rather than proactive to fraud.
- ▶ Lack of organizational level involvement in understanding inherent risks due to cybercrime.
- ▶ Viewing Risk Management as a mere compliance need.

Taking into stock these revelations, RBI can incorporate the following approaches, which we at CustomerXPs feel will help provide banks with the tools and strategies they need to fight fraudsters and adhere to their compliance needs.

**According to a 2014 EY Report on banking, the only way for banks to become better every day is to improve, expand and innovate.**

- ▶ Scientific approach to Enterprise Fraud Management.
- ▶ Institutionalize Fraud Management.
- ▶ Innovate and adapt to changes technologically and product wise.
- ▶ Innovation and adaptation to be an organization-level mandate, guided and regulated across all departments by a specific independent authority, for synergistic and unbiased development across all departments.
- ▶ Institutions to create a talent pool for specific purposes to preempt any shortage and ensuring business continuity.
- ▶ To conduct regular as well as ad hoc Risk Assessment tests to check if the system is functioning as per expected level of dependencies.
- ▶ A sense of ownership to be promoted and rewarded in organizations.
- ▶ To invest in a cross-channel integrated Enterprise Fraud Management solution which can calculate risk and mitigate the same.
- ▶ Acknowledge the need for a system which can analyze and check for instances of fraud and preempt it in real time.

These recommendations are clear, but for banks to deal effectively, efficiently and continuously with imminent cybercrime attacks, they need technologically advanced tools, a thinking, learning, intuitive system that can preempt danger. A product that has a brain.

## 06 WEAPONS OF CYBERCRIME DESTRUCTION

**A financial crime fighting technology must have the ability to gather and analyze non-financial information across bank's multiple channels.**

While regulatory compliance for staying secure is mandatory, banks also need to have in place an intelligent fraud detection and prevention framework as a critical component of their operational risk strategy. With increasing sophistication in financial fraud it becomes imperative for financial institutions to rethink conventional fraud defense strategies and consider equipping themselves with a new arsenal to stay ahead of the game. We believe that these new weapons of cybercrime destruction should be armed with several characteristics including:

- ▶ Presence of real time cross-channel transaction stoppage / transaction verification support capabilities.
- ▶ The ability to gather and analyze non-financial information across bank's multiple channels.
- ▶ An integrated Case Management with a Unified View across channels and products.
- ▶ A dynamic customer behavior profiling across all channels.
- ▶ The capability to integrate futuristic authentication systems e.g. biometric, retina scan, etc.
- ▶ Having an endpoint assessment (for preventing Trojans, spyware from stealing user credentials and ability to examine the browser to ensure it has not been tampered with by a Trojan).
- ▶ Having an endpoint abolishment (removing all traces of a customer's activity including web page caches, registry keys, downloaded components and files and cookies from the system once they log off. This enhances security in a shared-workstation environment like cybercafes, kiosks, etc.)
- ▶ Provision of a secure access gateway (eliminating the need for making any changes to the existing Internet banking application enabling strong multi-factor authentication).
- ▶ Prohibiting session-saving cookies.
- ▶ Unified audit logs, alerts, reports.
- ▶ Fully automated token distribution.

**Solutions that have been deliberately designed with an almost human-like intelligence are the future in fraud and risk management systems.**

- ▶ Employee or Internal Fraud Prevention.
- ▶ Issuer Card Fraud Prevention (Debit & Credit Cards).
- ▶ Customer Looped Fraud Prevention.
- ▶ Merchant acquiring Fraud Prevention (Debit and Credit Cards).
- ▶ Risk-based Authentication.
- ▶ Internet Banking Fraud Prevention.
- ▶ Cross-channel Fraud Prevention across multiple CBS.
- ▶ Deposit account Fraud Prevention.
- ▶ Loan Account Fraud Prevention.
- ▶ Organized Ring Fraud Detection.
- ▶ Real time Anti-Money Laundering (AML) solution.

It is evident that a contemporary solution that fights cybercrime and mitigates risk should be imbued with all these features. Solutions that have traditionally operated in silo-based channels are not equipped to combat real time financial threats and attacks. Only solutions that have been deliberately designed with an almost human-like intelligence with self-learning capabilities that can analyse patterns of human behaviour and enable decision making in real time can truly thwart and protect banks from repeated onslaughts of cybercrime.

## In conclusion

Over the years cybercrime has grown in leaps and bounds causing losses to the tune of billions and is a very potent threat banks and financial institutions. With increasing reliance on technology for the entire gamut of banking operations, being in control of billions of transactions across multiple channels including ATMs, to POS machines, mobile banking to internet banking, and more, is humanly impossible.

It is imperative for banks in India to fight their attitudinal mindset and wake up to fight incumbent cyber attacks and financial frauds on a war footing. It is incumbent on them to invest in smart, intelligent and multi-faceted solutions that can tackle cybercrime threats by preempting suspicious activity across a customer's journey through several touch points.

Indian banks now have an opportunity to go beyond regulatory compliance to proactively implement an intelligent, cross-channel defense framework that besides helping save billions can protect their brand reputation and customer trust.

## About the author





### KARUNAKAR MOHAPATRA


Karunakar is a Research Analyst at CustomerXPs. He monitors developments in the BFSI technology domain and publishes significant trends that impact the sector. You can find Karunakar on [LinkedIn](#).




*This report contains information on protection from cybersecurity and cybercrime. The information provided is not advice, and should not be treated as such. All trademarks acknowledged to their respective owners. CustomerXPs and Clari5 logos are registered trademarks of CustomerXPs Software.*

 clari5@customerxps.com

 /company/customerxps

 /customerxps

 customerxps.com

## References

- AB, M. (2015, July 27). [Indian companies mostly uninsured against cyber attacks](#). Retrieved August 2016, from DNA
- Ashford, W. (2016, March 18). [Cyber crime is driving UK fraud losses, totalling £755m in 2015](#). Retrieved from ComputerWeekly
- [Bank fined for lax security resulting in online fraud](#). (2016, June 30). Retrieved August 2016, from TOI
- BOYCE, L. (2015, February 16). [Banks are hit by largest cyber-crime ever detected: Are they doing enough to prevent fraud or are we now at the hackers' mercy?](#) Retrieved August 2016, from THISISMONEY.CO.UK
- Deloitte. (2016). Cyber Security De-Risking India's Banking Industry. Deloitte.
- Deloitte. (April 2015). India Banking Fraud Survey. Deloitte.
- EY and Indian Banks Association. (2014 January). Banking on Technology Perspectives on the Indian Banking Industry. EY and Indian Banks Association.
- India, R. B. (2016, June 2). [Cyber Security Framework in Banks](#). Retrieved from Reserve Bank of India
- [Indians suffered loss of over Rs 219 cr due to cyber frauds](#). (2013, December 13). Retrieved August 2016, from ET times
- Joseph, G. (2013, June 24). 'India has 42 mn cyber crime victims every year'. Business Standard.
- KPMG. (2014). Cybercrime survey report. KPMG.
- KPMG. (2015). Cybercrime Survey Report 2015. KPMG.
- McAfee. (June 2014). Net Losses: Estimating the Global Cost of Cybercrime. McAfee.
- Morgan, S. (2016, January 17). [Cyber Crime Costs Projected To Reach \\$2 Trillion by 2019](#). Retrieved August 2016, from Forbes:
- PWC. (December 2011). Safeguarding organisations in India against Cyber crime Global economic crime survey. PricewaterhouseCoopers Private Limited.
- Sasi, A. (2016, July 22). [Cyber crime: With vulnerability rising, RBI calls for a safety net](#). Retrieved August 2016, from The Indian Express:
- Shetty, M. (2015, January 14). [6 banks, telecom firm to pay for credit card frauds](#). Retrieved August 2016, from TOI:
- Taylor, P. (2013, July 24). [Cybercrime costs US \\$100bn a year, report says](#). Retrieved August 2016, from Financial Times:
- Yurcan, B. (2011, September 23). Cybercrime to Account for \$371 Million in Losses by 2015, According to Report. Bank Systems & Technology.

## About CustomerXPs

CustomerXPs is an enterprise software product company offering Enterprise Financial Crime Management (EFCM), Anti-money Laundering (AML) and Customer Experience Management (CEM) products for Tier-1 global banks. CustomerXPs is revolutionizing Fraud Management and Customer Experience Management in Fortune 500 banks by harnessing the power of extreme real-time, cross-channel intelligence. Voted 'Best Fraud Detection Product 2016' by OpRisk / Risk.net, CustomerXPs' flagship product Clari5's differentiated approach deploys a well-synchronized, context-aware 'central nervous system' in banks with the ability to stop fraudulent transactions with real-time, actionable insights.

