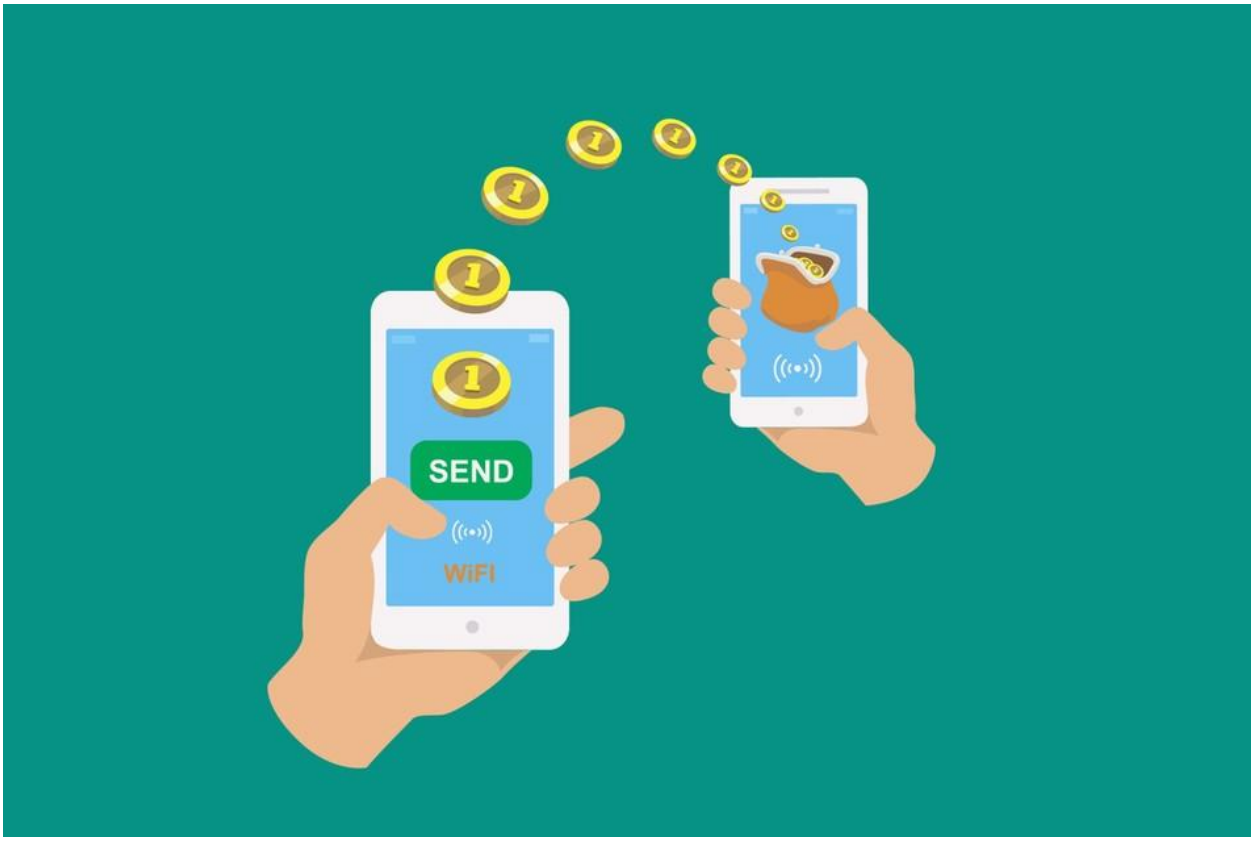
International Research Journal of Management and Commerce
ISSN: (2348-9766)
Impact Factor- 5.564, Volume 5, Issue 5, May 2018
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

NEED OF CYBER SECURITY IN CASHLESS ECONOMY



Bindu Roy
Assistant professor
DAV Centenary College, Faridabad

Anjali Tewatia
Assistant professor
Pt. JLN Govt. college, Faridabad(E)

NEED OF CYBER SECURITY IN CASHLESS ECONOMY - INDIA

ABSTRACT

As technology becomes more and more deeply integrated into our lives, we become more dependent on it. But this dependence makes us vulnerable if technology fails. In today's world, it's important that technology which is available should be protected and secure. If not, we will suffer consequences in our daily lives. Every year, thousands of cyber security problems are identified in technologies from well-known vendors. Some of those vendors are among the best at cyber security, yet they still have hundreds of security problems each year. The recent demonetisation policy has had a huge impact on various sectors of the Indian economy and has significantly impacted the way people transact in daily life. This led to the adoption of alternative technology platforms. As a result, both the number and value of transactions through these platforms saw a huge surge. The government has been consistently investing in various reforms for greater financial inclusion. Therefore, after the demonetisation move, the economy was ready with the infrastructure required to take the leap towards a cashless society. During the last few years, initiatives such as Jan Dhan accounts, Aadhaar-enabled payment system, e-wallets and National Financial Switch (NFS) have cemented the government's resolve to go cashless. With more platforms being included in the banking ecosystem, cyber threats will continue to evolve. Moreover, cyber threats will only rise as India is moving towards a cashless economy. With more time to detect and time to respond to these attacks, the return on investments for cyber attacks is greater in emerging markets like India as compared to developed markets like US .The types of cyber security incidents such as phishing, scanning, website intrusions and defacements, virus code and denial of service attacks will continue to grow. The objectives of our research paper are to review the growth of cashless transactions after demonetization and to find out the need of Cyber security in cashless economy in India. The study is based on secondary data. The findings of the study reveal that as the country is experiencing a digital revolution, the impact of this transformation makes it imperative for financial service players to revisit their cyber security resilience.

Keywords: Cyber security, demonetisation, cyber threats, digitalization, cashless economy

Introduction

The recent demonetisation policy has had a huge impact on various sectors of the Indian economy and has significantly impacted the way people transact in daily life. From midnight of 8 November 2016, 500 INR and 1,000 INR notes stopped to be considered as legal tender.While the government's aim was to prevent the duplicacy of currency, black money, tax evasion and terrorism funding, demonetisation also had an impact on the way people bank in India.

Clearly, the step involved a lot of planning and serious measures that were taken under utmost secrecy.However, with the announcement coming into effect, 86% of the total currency (amounting to 14 trillion INR) in circulation was abruptly revoked from the economy. In addition, restrictions were imposed on the amount which customers could withdraw and deposit through platforms such as bank branches and ATMs. After the announcement of demonetisation, multiple guidelines were issued by RBI.

Banks had to implement changes such as setting withdrawal limits, changes to cash management applications, core banking applications, coupled with the ability to report additional data to the regulators. Banks also had to push system integrators to incorporate these changes in the various systems such as core banking systems, ATM switches and cash inventory management overnight.The ATM has been the key enabling technology for dispensing funds.

Due to the change to note dimensions, recalibrating the machines and making them operational became the need of the hour. Because this was a covert operation, the ATM supporting industry was unable to reinstall machines overnight.

The entire population faced a severe cash crunch, which led to banks and ATMs being thronged by customers. The replacement of old notes took longer than expected, and hence, routine low-value transactions were severely affected. Simultaneously, replacing a large amount of cash over a 50-day period put humongous pressure on the banking system. This led to the adoption of alternative technology platforms. As a result, both the number and value of transactions through these platforms saw a huge surge. For example, **the value of transactions through e-wallets witnessed 301% growth during the period from 8 November to 27 December 2016. The number of transactions through POS saw a massive 95% increase during the same period. Further, the number of transactions through RuPay cards shot up by 425%.** The government also announced some incentives for going cashless. For example, it was announced

that no service tax will be charged on digital transactions up to 2,000 INR. **Digital payments made for buying petrol and diesel were given a discount of 0.75%. The suburban railway network also announced a discount of up to 0.5% to customers for monthly or seasonal tickets booked through digital transactions. In addition, life and general insurance policies and renewal premiums on public sector undertaking (PSU) insurers' websites provided an 8% and 10% discount, respectively. For payments at toll plazas on national highways using RFID card/Fast Tags, a discount of 10% was made available to users in the year 2016-17.**

By 30 December 2016, old 1,000 INR and 500 INR notes worth around 13 lakh crore INR were deposited back in the banking system. However, the rate at which new notes were infused into the economy was much lower. Clearly, the shortage of notes has led to people considering cashless avenues for transactions. Although the journey to creating a cashless economy remains an ongoing one, there have been several milestones along the way, led by RBI and supported by banks and the other players in the financial infrastructure system. T**he government has been consistently investing in various reforms for greater financial inclusion. Therefore, after the demonetisation move, the economy was ready with the infrastructure required to take the leap towards a cashless society. During the last few years, initiatives such as Jan Dhan accounts, Aadhaar-enabled payment system, e-wallets and National Financial Switch (NFS) have cemented the government's resolve to go cashless.**

'Scrapping these notes has opened other avenues to make payments. Download apps of banks and e-payment options. Shopkeepers can keep card swiping facilities and everyone can ensure they pay safe using their credit and debit cards. If not a 100% cashless society, I request you to make India "less-cash society".'
– PM Narendra Modi during his address to the nation on 27 November 2016

REVIEW OF LITERATURE

Sumit ranjan (2017) believes that there is a great need of cashless economy so as to avoid black money transactions, to avoid time consuming, to avoid risk , It helps to economic growth ,it helps to increase security, It helps to reduce illegal business , It helps to avoid the threat of counterfeit currency , Help to effective utilization of resources , It help to effective transaction , To avoid criminal activities, Reduces the circulation of liquid money .Unavailability of plastic money with the people of rural areas, which have caused popularity of paper cash. Lack of adequate infrastructure and lack of knowledge are two major obstacles that impede mass connectivity. Most card and cash users fear that they will be charged more if they use cards. Further, nonusers of credit cards are not aware of the benefits of credit cards.

The ultimate goal of cyber security is to protect electronic information both in transit, and at rest. The national government plays a vital role in cyber security, both creating regulations that force businesses to conform to tighter security measures for their information, and protecting vital infrastructure, such as the nation's power grid.

In response to the increasing threat of cyber attack Indian parliament passed its "INFORMATION TECHNOLOGY ACT, 2000" on 17th oct to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes..

Bijay Bhandari (2017) gave safety tips such as Use antivirus software , Insert firewalls , pop up blocker, Uninstall unnecessary software, Maintain backup, Check security settings, Use secure connection, Open attachments carefully, Use strong passwords , don't give personal information unless required. He further added that The only system which is truly secure is one which is switched off and unplugged. So , only way to be safe is Pay attention and Act smart.

IDSA Task Force Report(March, 2012) states that the use of cyberspace depends on physical facilities like undersea cables, microwave and optical fibre networks (NWs), telecom exchanges, routers, data servers, and so on.The defence of cyberspace necessarily involves the forging of effective partnerships between the public organisations charged with ensuring the security of cyberspace and those who manage the use of this space by myriad users like government

departments, banks, infrastructure, manufacturing and service enterprises and individual citizens. The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown apace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security.

Vaishnavi J. Deshpande , Dr. Rajeshkumar Sambhe(2014) coined Cyber Terrorism as one more term associated with this topic "Cyber Security", i.e., "cyber terrorism". Now what this exact means is very important to know. This term is associated with the safety of our nation's strategy because this is a way to invade the privacy of any nation's infrastructure. Cyber terrorism is a way or a path or a mechanism through which an enemy is trying to know all the secrets of any nation and posing the threat to nation's policy.

OBJECTIVES OF THE STUDY:

The main objectives of the study are as under:

1- To review the growth of cashless transactions after demonetization in Indian economy.
2- To find out the need of Cyber security in cashless economy in India.

RESEARCH METHODOLOGY

The study is based on secondary data. To review the growth of cashless/digital transactions, the researchers have reviewed so many journals, research papers and articles. The secondary data is collected from various published reports of Reserve Bank Of India, various economic survey reports, published papers and articles in magazines, newspapers and websites etc. The time period for the study is considered after demonetization.

DATA ANALYSIS AND INTERPRETATION

The evolution of India's financial infrastructure

On its part, RBI along with National Payments Corporation of India (NPCI) leveraged technology and introduced newer avenues for banking with the overall objective of improving customer experience, security and ease of transactions. The evolution of India's financial infrastructure can be divided into three phases:

1. First phase of technology initiatives:

• 1984: Introduction of Magnetic Ink Character Recognition (MICR) technology

• 1987: First ATM installed in Kolkata

• 1988: Computerised settlement operations at clearing houses of RBI

• 1998–2000: Core banking software

2. Second phase of technology initiatives

• 2001: Internet banking

• 2004: National Financial Switch (NFS)

• 2004–2005: Real Time Gross Settlement (RTGS), National Electronic Funds Transfer (NEFT)

• 2007 : Mobile banking

• 2008: Cheque truncation systems

3. Third phase of technology initiatives

• 2010: Immediate Payment Service (IMPS)

• 2012: Adoption of ISO 20022 messaging standard in the Next Generation RTGS (NG-RTGS) system

• 2014: Jan Dhan Yojana, National Unified USSD Platform, RuPay Card, Bharat Bill Payment System (BBPS)

• 2016: Unified Payment Interface (UPI), payment banks, mobile wallets,

• 2017: Bharat Interface for Money (BHIM) app

With the evolution of the financial infrastructure ecosystem, the digital platforms available for payments have been transformed. Financial inclusion has gained prominence as the banking system flourished and various platforms were adopted in India. With the rise of technology in the financial infrastructure ecosystem came a greater flow of funds. Today, financial inclusion is seen as a realistic dream because of mobile and smartphone penetration across the country.

According to TRAI, as on 30 September 2016, 82 out of 100 citizens in India owned a mobile phone. The evolution of the telecom ecosystem has occurred at an opportune time, given that call and data rates are decreasing significantly, along with the prices of smartphones, further propelling the shift to a cashless society.Demonetisation has given an impetus to e-wallet services. Mobile wallets have witnessed a massive rise in app downloads. **With programmes for financial inclusion, digitalisation of the economy and increased use of smartphones, online transactions are already quite popular among the urban Indian population.**

The result has been that leading mobile wallets have witnessed growth of upwards of 100% in app download numbers and have similarly seen an increase of upwards of 400% increase in wallet recharges. This smartphone revolution has led to the emergence of e-commerce, m-commerce and other services, including app-based cab aggregators,who encourage digital payments for use of various services. The value added services such as cashback, bill payment facilities, loyalty points, rewards and ease of use have promoted increased usage of such digital platforms.

- 3X increase in the download of a leading mobile wallet app within 2 days of the demonetisation announcement
- 1 million: Number of newly saved credit and debit cards within two days of demonetisation announcement
- 100%: Day-on-day growth in customer enrolment with leading mobile wallets after demonetisation
- 30%: Increase in app usage and
- 50% increase in the download of wallets backed by leading banks

Growth in Digital Transactions after demonetization in India

The Digital Story

ALL NUMBERS IN MILLIONS

Month (2017)	No. of digital transactions*	No. of PoS terminals	No. of UPI transactions	No. of PPI transactions	No. of credit, debit card transactions
April	909.6	2.61	7	89.2	231.1
May	926.55	2.69	9.16	91.3	233.4
June	920.2	2.77	10.15	84.7	232.4
July	938	2.84	11.44	88.7	237.6
August	964.4	2.88	16.6	89.7	243
September	958.6	2.9	30.7	87.5	240.3
October	1048.3	2.95	76.7	96.2	255.7
November	1081.58	2.99	104.8	92.8	244.6
December	1150.28	NA	145.4	99.1	263.9

Source: RBI, NPCI, * Includes RBI's provisional figures along with Aadhaar Enabled Payment System numbers from NPCI but does not include electronic toll payments and other transactions for which data are not publicly available

INTERPRETATION

Number of digital transactions have shown a growth of 27% since april 2017 to december 2017. While UPI (unified payments interface) has shown a tremendous growth of 1971%.

Cashless isn't yet King

Month	UPI		Debit+Credit Cards	
	Volume (m)	Value (₹ cr)	Volume (m)	Value (₹ cr)
November 2016	0.3	90	205.5	35240
December	2	700	311	52220
January 2017	4.2	1660	265.5	48120
February	4.2	1900	212.3	39150
March	6.2	2390	229.7	41620
April	6.9	2200	231.1	43140
May	9.2	2770	233.4	45080
June	10.2	3070	232.4	46820
July	11.44	3381	237.6	43933
August	16.6	4130	243	45710

Source: RBI

Future is Digital

Despite mixed growth of digital payments the future is less cash, at least far less than the current 95%-plus transactions via cash and cheque books. According to a report on digital payments in India, total payments via digital instruments are expected to touch $500 billion by 2020. By then the fintech companies will be worth about $2.4 billion.

India's shift towards a digital economy where dependency on cash is significantly reduced, is taking gradual, successful steps. As per data released by Prime Minister Narendra Modi on his website, cashless transactions have picked up ever since demonetisation had come to effect and initiatives were being taken by various wings of the government, encouraging people to go cashless. In the financial year of 2016-17, there were a total of 865.9 crore digital transactions across all banking platforms. This is a significant rise from the 2013-14 number of 254.5 crore digital transactions. Within a period of 3 years, the amount of digital transactions has more than tripled. Recently, Niti Aayog principal advisor Ratan Watal shared similar statistics, stating that digital payments grew 55 per cent in volume and 24.2 per cent in value in 2016-17 over 2015-16.

The present Union government has laid stress on the importance of adopting cashless methods of transactions, to ensure that every transaction leaves a trace. Though wholesome digitisation of the economy is still a distant dream, the number of people conducting digital transactions throughout the country has definitely increased.

The government has repeatedly stressed on the importance of using mobile banking and has urged people to use their mobile phones for banking purposes. The government maintained that India's 117 crore strong base of mobile phone users can do much better in terms of utilising mobile banking applications. The Bharat Interface for Money (BHIM) app, which enables users to make payments across bank accounts is a significant achievement for the cashless mission, already being downloaded by over 2 crore people. The Prime Minister's website stated that over 72 crore transactions were done using mobile banking in 2016-17, compared to 9.47 crore in 2013-14. The value of mobile banking transactions increased to Rs. 10,572 crore from 224 crore in 2013-14. Digital transactions rose up to 3 crore daily in March 2017, compared to 96 lakh daily in March 2014. The increase is huge and shows that mobile banking has caught on very well with people, given how easy it is to conduct transactions using mobile phones and reduces dependency on physical bank visits or cash transfers.

The government worked towards the laying of optical fibre cables for broadband networks and asked the public telecom operators BSNL, as well as private companies such as Reliance and Bharti Airtel to ensure better internet connectivity, especially in rural and semi-urban areas. The total broadband network in 2017 amounts to 2,05,404 kilometres, compared to the merely 358 kilometres in 2013-14 This will ensure that internet connectivity in many parts of the country is much better and helps people in conducting cashless transactions without any hiccups.

It will be particularly challenging for the government to successfully implement the habit of going cashless in rural areas, which have been traditionally dependent on cash. However, with due infrastructure and policies in place, India's transition to a cashless economy could become a reality with time.

During this speech at the Global Citizen Festival (19 November 2016), Prime Minister Modi referred to the classic song by Bob Dylan: 'We better get out of the way as indeed the times they are a changing.' Thus, it is quite clear that the cashless economy is very much a thing of the near future in the Indian economy.

Need of Cyber Security in Cashless Economy

Cybercrime has increased drastically in the country after demonetisation and has been under-reported, cyber experts said at a fintech conference organized by the Confederation of Indian Industry ."I have begun to see a landscape which is believe me, very scary. The last eight months have been the most fertile months in the history of independent India for the growth of cybercrime," Pavan Duggal, president at Cyberlaws.Net and an advocate in the Supreme Court, said at a panel discussion on 'Risk and Regulation in FinTech World'. "After demonetisation, cyber crime has grown manifoldly and we have not been able to identify the extent to which it has grown."From global ransomware attacks that hit hundreds of systems to phishing and scanning rackets, at least one cyber crime was reported every 10 minutes in India in the first six months of 2017. That's higher than a crime every 12 minutes in 2016, said a report in The Economic Times last week.

According to Indian Computer Emergency Response Team (CERT-In), 27,482 cases of cybercrime were reported from January to June. Analysis of data from 2013-2016 shows that network scanning and probing, which is seen as the first step to detect vulnerabilities in systems so that sensitive data can be stolen, made up 6.7% of all cases while virus or malware attack accounted for 17.2%, it added in a report.

"As a country we are clueless as to how to address cyber security barring coming up with National Cybersecurity Policy of 2013 which has primarily remained a paper document. Till this

point in time, there is no dedicated law for cyber security," said Duggal.There is a need for a legal framework in the context of emerging technologies like blockchain, he added.

To regulate mobile applications accessing private data, the experts suggested putting in place a comprehensive cyber security law. Another member of the panel, Amlok Singh, director of information technology security at Infologic Solutions, said the payments and fintech space will be most vulnerable to cybercrime.

"Security shouldn't be an afterthought but an important aspect during the conception stage itself...external experts should scrutinize the product to detect flaws which should be immediately mitigated," Singh added.

Several industry experts participated in the day-long conference to discuss the scope of new technologies like Unified Payments Interface (UPI), Aadhaar enabled payments, blockchain, artificial intelligence and robotics.

With more platforms being included in the banking ecosystem, the sources of transaction origination will see a significant increase, which means cyberthreats will continue to evolve. Moreover, cyberthreats will only rise as India is seeing a shift towards a cashless economy. With more time to detect and time to respond to these attacks, the return on investments for cyberattacks is greater in emerging markets like India as compared to developed markets like the US.4 The types of cyber security incidents such as phishing, scanning, website intrusions and defacements, virus code and denial of service attacks will continue to grow. As the country is experiencing a digital revolution, the impact of this transformation makes it imperative for financial service players to revisit their cyber security resilience. The number of incidents occurring in banking systems has increased in the last five years. In the month of October 2016, an ATM card hack hit Indian banks, affecting around 3.2 million debit cards.5 Hence, efforts are needed to enhance cyber security as businesses and citizens embrace this new digital wave.

Undoubtedly, for the players in the financial services ecosystem, it's not business as usual. A collective effort is needed to ensure preparedness for the new cashless economy. We believe that

the areas below will have to be re-examined to ensure adaptive and real-time cyber defence. While data will be at the core, the network perimeter will extend to end devices. Faster development will demand agile security. More intelligent transaction monitoring will have to be carried out as part of continuous surveillance. Crisis response and recovery strategies will have to step up along with the increased digital footprint. Security awareness of all the stakeholders will be a vital pillar of a secure cashless society.

1. Agile security practices: For financial services players, faster development and roll-out of theservices will be a critical success factor. Accordingly, all technology development and refresh will be delivered using an agile development framework. Security in this context can no longer be a standalone post-facto toll gate. Security assessment and testing will need to be embedded into the agile development life cycle. Agile security testing methods based on automation will have to be adopted. In many ways driving, a paradigm shift is needed in the way security testing is undertaken today.

2. Securing the hyper-interfaced environment: The new era will call for hyper-interoperability across different value chain players. In order to enable this, each ecosystem player will need to create multiple application programing interfaces (APIs). While this will deliver a seamless experience to customer, there is also a risk of malware injection through such APIs. With faster proliferation of interfaces, protecting APIs will become critical to ensure malware and persistent threats do not propagate through such untrusted/ untested APIs.

3. Next generation authentication: In the new cashless world, frauds will be driven mainly by impersonation and will become a daily affair. Accordingly, the need for stronger authentication of transactions will gain significance. The current techniques of authentication based on location and timing will no longer be adequate. Adaptive authentication will need to be embedded into the heart of transaction processing. Next generation authentication will use triangulation techniques while considering larger data sets including the nature of transaction, merchant type and transaction channel.

4. Protecting context-rich personally identifiable information (PII): The new generation data marts will not be limited to traditional transactions and account-related information but will have enriched data insights such as spending patterns, patterns of digital platform usage, preferences and other person-specific information sets.

5. Security of the new perimeter— mobility: In the new digital/ cashless economy, mobility-based solutions will continue to gain prominence and, hence, security concerns will no longer be limited to the organisation architecture boundaries. Mobility will form a new perimeter of the organisation. In order to ensure endpoint security containerised apps with built-in advanced persistent threat (APT) capabilities will have to be developed. Controls for in memory data and additional controls like device certification will be considered. To ensure security of data in endpoints, there may be a requirement for guidelines to define the kind of sensitive data that end devices retain. Hence, the next generation financial infrastructure may involve the adoption of advanced end-user device management solutions.

6. High velocity identification, containment and eradication: Each consumer today is using multiple platforms and using services across the ecosystem. Any threat that impacts such a user can potentially proliferate and bring the entire financial services ecosystem to a standstill. As the ecosystem continues to be interconnected and overlapping, cybercriminals will try to exploit possible lapses and, hence, strategies need to be built to deal with such eventualities. Given this interdependence on the all the players of the financial ecosystem, it becomes crucial to identify any anomaly at a pace which mirrors real time or near real time. Once an anomaly is identified, containing it is of paramount importance before it spreads and crosses a point where the damages have transcended organisational boundaries and services. Response strategies will have to be quick and customised to meet various incident scenarios based on situational awareness. Further, these strategies will have to be orchestrated across own infrastructure and encompass various digital partners and other stakeholders.

7. Augmented ecosystem control: The new age enterprises will adopt the cloud for faster roll-out and to address non-linear growth. Technology partners could include start-ups, garage shops and large conglomerates, who come together to deliver end products. The security boundaries of the various players will be extended to end users, third parties and other ecosystem partners.

Security controls will no longer be defined in contracts limited to uptime and resolution of vulnerabilities, but will actually be embedded in the partner ecosystem. The process for monitoring of parameters will also have to be integrated with the company's incident response framework.

8. Ubiquitous awareness: The cashless economy means that the stakeholder community will now not just be limited to internal stakeholders but will also include external as well as peripheral stakeholders (like merchants). With the influx of first-time users, users from various linguistic ethnic groups and users of different channels, the soft targets will be multifold. The awareness theme for tomorrow will thus be multichannel, multilingual and multicultural, and hence go beyond the scope of traditional programmes. Regulators may have to start thinking across industries and develop awareness programmes that addresses this need. Social media can be a key enabler to propagate awareness.

CONCLUSION

Cyber security will continue to be a type of asymmetric warfare:Each organisation will face a multitude of cyber adversaries, and their ranks will grow and become more sophisticated. The new reality is that cyber attackers are sufficiently capable and motivated to break through the defences. Hence,organisations will have to develop novel preventive control mechanisms and significantly invest in reactive capabilities. We believe mastering the areas highlighted above will help financial services companies reach the forefront of the industry. This is because incorporating a more agile cyber risk management approach may enable them to more effectively harness the ongoing digital revolution to their advantage.

REFERENCES

1.Aishnavi J. Deshpande & , Dr. Sambhe, Rajeshkumar (March 2014), "Cyber Security: Strategy to Security Challenges- A Review",International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 9.

2.Digital Divide: A Barrier in Making Cashless Society Presented by- SUMIT RANJAN (Senior Research Fellow) Department of Library & Information Science BBAU, Lucknow (2017)

3.Garg, Preeti and Panchal, Manvi, " Securing the cashless economy-Sivarama Krishnan Leader, Cyber Security PwC India", IOSR Journal of Business and Management (IOSR-JBM) e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 19, Issue 4. Ver. II (Apr. 2017), PP 116-120 www.iosrjournals.org

4.Lee, Jinkook, Fahzy Abdul-Rahman, and Hyungsoo Kim. "Debit card usage: an examination of its impact on household debt."Financial Services Review.16.1 (2007): 73. 5.More wedge, C. K., Holtzman, L., & Epley, N. (2007). Unfixed resources: perceived costs, consumption, and the accessible account effect. Journal of Consumer Research, 34(4), 459–467).

6. Moses-Ashike, H. (2011), ―Cashless Economic can Reduce Risk of Carrying Huge Cash‖, [Online] Available: http://www.businessdayonline.com/…/22217.

7. Odior, E.S., and Banuso, F.B. (2012): Cashless Banking in Nigeria: Challenges, Benefits & Policy Implications. European Scientific Journal. Vol 8, pp. 12 – 16.

8.Roth, B. L. (2010).―The Future of Money: The Cashless Economy – Part 1‖. [Online] available: https://www.x.com/.../futuremoney-cashless-economy—part-i.

9.Woodford M. (2003). ―Interest & Price: Foundation of a Theory of Monetary Policy‖, Princeton University Press.

10. IDSA Task Force Report March 2012

11.https://www.papermasters.com/cyber-security.html

12.https://www.microsoft.com/en-us/research/academic- program/write-great-research-paper/

13.http://www.slideshare.net/lipsita3/cyber-crime-and-security-ppt

14. http://riverdelfin.blogspot.in/2013/09/an-introduction-to-cyber- crime.html