Research Monograph 51

2021

IT Security of Banks in Bangladesh: Threats and Preparedness

Md. Mahbubur Rahman Alam
Associate Professor, BIBM

Md. Shihab Uddin Khan
Associate Professor, BIBM

Kaniz Rabbi
Assistant Professor, BIBM

Md. Foysal Hasan
Lecturer, BIBM

Shyamol B. Das
Chief Digital Officer, Mutual Trust Bank Ltd.

Md. Saiful Islam
Chief Technology Officer, Bank Asia Ltd.

Bangladesh Institute of Bank Management (BIBM)
Section-2, Mirpur, Dhaka-1216, Bangladesh.

RESEARCH MONOGRAPH 51

IT Security of Banks in Bangladesh: Threats and Preparedness

Md. Mahbubur Rahman Alam
Associate Professor, BIBM

Md. Shihab Uddin Khan
Associate Professor, BIBM

Kaniz Rabbi
Assistant Professor, BIBM

Md. Foysal Hasan
Lecturer, BIBM

Shyamol B. Das
Chief Digital Officer (CDO), Mutual Trust Bank Ltd.

Md. Saiful Islam
Chief Technology Officer (CTO), Bank Asia Ltd.

\

BANGLADESH INSTITUTE OF BANK MANAGEMENT
Mirpur, Dhaka

IT Security of Banks in Bangladesh: Threats and Preparedness

Md. Mahbubur Rahman Alam
Md. Shihab Uddin Khan
Kaniz Rabbi
Md. Foysal Hasan
Shyamol B. Das
Md. Saiful Islam

Editors **Md. Akhtaruzzaman, *Ph.D.***
Director General, BIBM
Ashraf Al Mamun, *Ph.D.*
Associate Professor & Director (Research, Development & Consultancy), BIBM

Support Team **Md. Al-Mamun Khan,** *Publications-cum-Public Relations Officer, BIBM*
Md. Golam Kabir, *Assistant Officer (PPR), BIBM*
Papon Tabassum, *Research Officer, BIBM*
Sk. Md. Azizur Rahman, *Research Assistant, BIBM*
Md. Awalad Hossain, *Computer Operator, BIBM*
Md. Morshadur Rahman, *Proof Reader, BIBM*

Cover Design **Md. Mahbubur Rahman Alam**, *Associate Professor, BIBM*

Design & Illustration **Papon Tabassum,** *Research Officer, BIBM*
Md. Awalad Hossain, *Computer Operator, BIBM*

Published in September, 2021

Published by Bangladesh Institute of Bank Management (BIBM)
Plot No. 4, Main Road No. 1 (South), Section No. 2
Mirpur, Dhaka-1216, Bangladesh.
PABX : 48032091-4, 48032097-8
Fax : 88-02-48033495
E-mail : bibmresearch@bibm.org.bd
Web : www.bibm.org.bd

Printed by Print Plus, 10 Arambag, Motijheel, Dhaka.

Foreword

As part of the ongoing dissemination of BIBM research outputs, the present research monograph contains the findings of the research project: "IT Security in Banks of Bangladesh: Threats and Preparedness." IT security is a growing concern in banks and financial institutions in Bangladesh. Cyber security is a major threat to banks, with a rise in the number of cyber incidents. Digital technologies have driven the growth of Bangladeshi banks with a huge spurt in online transactions but have also generated risks of protecting confidential information and sensitive financial data. The study aims to share the global experience of new online threats and frauds specially for banks and assess the threats, vulnerabilities and preparedness of the banks of Bangladesh. This publication also identifies the challenges of information system security and suggests future courses of actions in ensuring better and secured IT based services of banks.

It gives me immense pleasure, on behalf of BIBM, to offer this important resource of academic inputs to the practitioners of the banks and financial institutions, regulatory agencies as well as to the academics and common readers. I hope, this monograph will be a valuable resource for professionals especially for the banking community for understanding the IT security threats in banks and taking necessary actions to fight against the challenges posed by cyber attackers.

We do encourage feedback from our esteemed readers on this issue which certainly would help us to improve our research activities in the years to ahead.

Md. Akhtaruzzaman, *Ph.D.*
Director General, BIBM

Acknowledgement

This research project has been completed with the great support from many persons and organizations.

We would like to especially thank Dr. Md. Aktaruzzaman, honorable Director General, BIBM for his valuable advice, inspiration, comments and thoughts to progress our research work. The team sincerely acknowledges the contribution of Dr. Prashanta Kumar Banerjee, Professor and former Director (RD&C), BIBM; and Dr. Ashraf Al Mamun, Associate Professor and Director (RD&C), BIBM.

We are also very grateful to all of our faculty colleagues for their comments and positive suggestions to carry out our research. We are also grateful to the bankers who took the pain to complete the research questionnaire.

Our honest indebtedness goes to research assistants, who have facilitated us to get very much useful information from different stakeholders. Our sincere appreciation goes to Ms. Papon Tabassum, Research Officer, BIBM and other related staffs of BIBM for their support.

Finally, we would like to thank all of those who, directly and indirectly, extended their cooperation in our research work.

Md. Mahbubur Rahman Alam
Md. Shihab Uddin Khan
Kaniz Rabbi
Md. Foysal Hasan
Shyamol B. Das
Md. Saiful Islam

RESEARCH MONOGRAPH 51

IT Security of Banks in Bangladesh: Threats and Preparedness

Contents

Tables

Figures

Cases

Box

Abbreviations

ACHS	Automated Clearing House System
ACL	Access Control List
ACPS	Automated Cheque Processing System
ACS	Access Control System
ADC	Alternate Delivery Channel
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
ATM	Automated Teller Machine
BAB	Bangladesh Association of Banks
BACPS	Bangladesh Automated Cheque Processing System
BB	Bangladesh Bank
BCP	Business Continuity Planning
BEC	Business Email Compromise
BEFTN	Bangladesh Electronic Fund Transfer Network
BOD	Board of Director
BIBM	Bangladesh Institute of Bank Management
BYOD	Bring Your Own Device
CBS	Core Banking Solution
CCNSP	Certified Network and Security Professional
CDCDP	Certified Data Centre Design Professional
CEH	Certified Ethical Hacker
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity and Availability
CIB	Credit Information Bureau
CID	Crime Investigation Department
CII	Critical Information Infrastructure
CIO	Chief Information Officer
CISA	Certified Information Systems Auditor
CISO	Chief Information Security Officer
CISSP	Certified Information Security Professional
CMMI	Capability Maturity Model Integration
COBIT	Control Objective for Information and Related Technologies
COO	Chief Operating Officer

CRO	Chief Risk Officer
CTO	Chief Technical Officer
DBA	Database Administrator
DC	Data Center
DDoS	Distributed Denial of Service
DLP	Data Leakage Prevention
DRP	Disaster Recovery Planning
DRS	Disaster Recovery Site
EFT	Electronic Funds Transfer
FCB	Foreign Commercial Bank
FEIB	Far Eastern International Bank
FI	Financial Institution
FICCI	Foreign Investors' Chamber of Commerce & Industry
FS	Financial Service
FTP	File Transfer Protocol
GDP	Gross Domestic Product
GM	General Manager
IBM	International Business Machines
ICCD	Internal Control & Compliance Division
IC3	Internet Crime Complaint Center
ICT	Information and Communication Technology
IDRBT	Institute for Development & Research in Banking Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
ITG	Information Technology Governance
ITIL	Information Technology Infrastructure Library
JNPT	Jawaharlal Nehru Port Trust
KPMG	Klynveld Peat Marwick Goerdeler
LEA	Law Enforce Agency
MD	Managing Director
MIS	Management Information System
MRI	Magnetic Resonance Imaging
NIST	National Institute of Standards and Technology

NMS	Network Management System
NPSB	National Payment Switch Bangladesh
OS	Operating System
PCB	Private Commercial Bank
PCIDSS	Payment Card Industry Data Security Standard
PII	Personal Identifiable Information
PMBOK	Project Management Body of Knowledge
POS	Point of Sales
PRINCE	PRojects IN Controlled Environments
PT	Penetration Testing
PwC	PricewaterhouseCoopers
P2P	Person to Person
RMS	Risk Management Solutions
RSA	Rivest–Shamir–Adleman
RTGS	Real Time Gross Settlement
SB	Specialized Bank
SFIA	Skills Framework for the Information Age
SIEM	Security Information and Event Management
SIM	Subscriber Identity/Identification Module
SLA	Service Level Agreement
SME	Small and medium-sized enterprises
SMS	Short Message Service
SOCB	State Owned Commercial Bank
SQL	Structured Query Language
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TOGAF	The Open Group Architecture Framework

Executive Summary

Bangladesh is rapidly moving towards a digital economy. Coping with the advancement of information technology, most of the banks have introduced core banking system with new transaction methods through alternative delivery channels like payment cards (debit and credit), ATM, Internet and Mobile Phone, etc. Increasing adoption of digital banking and wallets developed new security threats and attract targeted attacks from cyber criminals. Various threats have emerged in the cyberspace such as phishing, key-logging, spyware, malware and other online-based frauds that are specifically designed to target the bank customers. Banking industry has been attacked by sophisticated malware, like botnet, around the world which deliberately pilfer confidential banking and financial information.

Globally a significant change has been seen in technology landscape. As security risks and cyber threats are increasing at an alarming rate, banks and their IT teams face severe challenges to overcome all those risks and threats. In financial institutions cyber-attacks are becoming more common, more erudite, and more widespread than before. On the other hand, cyber-crime groups and other wrongdoers crack systems for financial gain—such as stealing funds through account takeovers, ATM thefts, and other manoeuvres. The cost of technology has been decreasing in the last few decades, as a result the hurdles to entry for cyber-crime also drop. Now it is easy and cheap for offenders to find out new and innovative ways to commit cyber fraud. Also there exists an underworld black market that sells breached data which inspires wrongdoers further.

Banking sector of Bangladesh has been ignoring cyber security for many years. As a result, banking information and critical infrastructures become vulnerable to the cyber attackers. Different studies by BIBM have proved this point very well. Reserve fund heist of Bangladesh Bank (BB) triggered cyber security issue again. The banking industry of Bangladesh also neglected cyber security due to the absence of effective cyber security regulatory norms in Bangladesh. Frequently through the press and media it is seen that banking frauds are happening on account of the absence of client awareness about security. As a result, customers and bank face huge financial loss.

This study evaluated the overall IT security threats and preparedness in commercial banks of Bangladesh. The study used both primary and secondary data. Secondary data has been obtained from different online and physical sources (websites and published articles). Both interview and questionnaire methods were used for collecting primary information. The major strength of the study is the primary data that has been collected from 45 centralized online banks covering SOCBs, PCBS, SBs and FCBs. The study has been enriched by detailed analysis of all the data and information acquired from the filled-up questionnaire of the banks. For the field survey regarding customers' and end-

users' awareness on online banking security, a sample of 750 bank customers and 450 employees were also selected covering all categories of banks. Moreover, our study involved more than 30 individuals in the rank of CIOs, CTOs, CISOs, CROs, COOs and security professionals.

The study finds that the security of the information flow both inside and outside of the bank should be focused. There is a big challenge for the banks having Internet connection to their corporate Intranet. It is the security issue that must be addressed properly with adequate hardware, software and manpower. Every bank should strengthen its ICT security department in ICT division. Recruitment of ethical hacker; placing a proper IT security control and monitoring system etc., are the crying need of banks. Surprisingly, 62% of the banks have no security expert in the IT team. Immediate actions should be taken by top level management of those banks to recruit proper security experts or develop security experts quickly by providing high quality training. Security awareness of both bank customers and employees' is a great concern for banking sector. Customers' awareness can be increased by counseling, advertising and distributing leaflets/brochures. Specialized training on IT security and fraud prevention can be provided to employees of banks.

It is seen that 16% banks have insufficient (less than 2) or no IT Auditors which could be one of the IT risk factors related to operation and finance in banking system. Same weak status is found in this study for Information Security Officers. This is a serious issue and need to be addressed as soon as possible. But most of the banks don't have sufficient IT auditors to audit their back-offices and branches. We found that 45% of the officers related to IT Audit and Security have no certification in this regard. That's why they are not enough confident and efficient for conducting fruitful audit. Although small number of IT personnel has certifications, they are not equipped with relevant banking knowledge. As a result, audit observations and respective recommendations are not focused according to business dimensions. It is clear that poor auditing system of those banks may create another risk for security if auditors fail to identify security holes. Bank management should give special attention to this issue.

According to the study findings, data center of all banks are built in Dhaka. However, 54% DCs and 18% DRSs have been established in high rise buildings having risk of earthquake and fire. On the other hand, DRSs of maximum banks are also established in Dhaka within an average air distance of 12.5 kilometers from the DC, showing very high risk of natural disaster like earthquake. Banks should have immediate plan to set up DRS at separate seismic zone. Both Govt. and BB may take initiatives to provide infrastructure for reliable DRS.

Regular and periodic testing of a DRS is an important and crucial issue for a centralized online bank. This type of testing increases confidence and expertise of recovering data and business operation in case of any disaster. Research findings reveal that only 72% banks tested live operation from DRS in last year. Frequency and duration of live testing is also unsatisfactory. This finding indicates the poor quality and readiness of IT disaster recovery management. Banks should have proper policy and guidelines of business continuity and disaster recovery management. But only 61% banks have approved guidelines of BCP/DRP. About 28% banks have separate BCP team but team size is very small and members are not properly trained. Special decision can be taken by all banks, including Bangladesh Bank, in this regard. Moreover, a Computer Emergency Readiness Team (CERT) may be formed for disaster recovery of the banking sector.

According to our survey, only 32% banks have IT Governance (ITG) framework. It indicates lack of active involvement of top level executives in IT system management in banks. With a view to enhance the level of understanding on the importance of ITG for effective business development, proper discussion forum or roundtable discussion may be arranged for top management (BoDs and Senior Management). Bangladesh Bank and BIBM may play vital role in this case. Research findings indicate that implementation status of ITG in banks is very weak. Still 8% banks not initiated ITG implementation and 60% banks initiated but they have no definite target date to complete. Banks should give proper attention to follow appropriate guidelines, standards and framework (such as COBIT, ISO/IEC 38500:2008) to successfully implement ITG to achieve sustainable business and offer new innovative products/services to its customers.

It is observed that the level of appreciation by most of the banks' management regarding the skills development of IT personnel through training and workshop participation is not at very good stage. Near about 3% of total IT budget goes to training purpose and CTOs are not satisfied regarding this issue. As ICT is rapidly changing and more diversified and sophisticated Cyber-attacks/frauds are increasing, bank management should upsurge their level of understanding and appreciation that there is no alternative to develop IT skills of employees in banks. Blending program can be arranged jointly by software and hardware vendors (IBM, Oracle, Microsoft, Cisco, etc.), expert IT professional of different banks and academicians from different institutes and BIBM. Specialized training, certification and post graduate program for both general bankers and IT professionals of banks may be conducted by BIBM or other related organizations. IT Heads of 88% banks agreed that banking sector should have a center for sharing electronic banking experiences, problems and solutions. An institution like IDRBT (Institute for Development and Research in Banking Technology) which is set up by the Reserve Bank of India can be formed immediately in Bangladesh.

Bangladesh Bank conducts ICT inspection in commercial banks on sample basis once in a year and duration of the inspection is very short (two to three days) which is not well enough as ICT is a very vast area and all of its components have direct impact on business. In practice, IT audit should be comprehensive, not based on sample. Bangladesh Bank may increase the frequency of inspection to ensure a better banking information system. Supervision and monitoring need to be made stronger. More stringent and specific audit mechanism aligned with international standards should be incorporated in supervisory review/audit by BB. Also, BB may conduct system and functional audit. BB may develop ethical hackers so that they can identify security holes of commercial banks by sitting their head office and aware the banks.

Cyber security is a key risk for banks, with a rise in the number of cyber-crimes. Bangladeshi banks are driven by modern digital technologies with a huge growth in online transactions but have also generated risks of protecting confidential information and sensitive financial data. Since the importance of Information Systems Security is increasing in banks, BB has issued an ICT security guideline for banking and financial institutions. BB has also mandated establishment of IT Governance and IT Security for all banks in Bangladesh. Once it was thought that IT security is an issue of ICT division only. Now CEOs and the top management need to rethink that cyber risk is not only IT issue, but also a CEO and BODs issue.

Although ICT risk management guideline has been developed by almost every bank in accordance with the BB ICT Security Guidelines, but in most cases, these are not implemented properly. The banking sector identifies itself as unprotected and exposed in terms of information insecurity. There is, in fact, no comprehensive study found on overall IT security threats and preparedness in commercial banks of Bangladesh. This research project tries to explore the situation of information security measures, challenges in safeguarding this, and proposes some policy alternatives. Further this will assist the industry to develop a highly protected Information System in banks.

IT Security of Banks in Bangladesh: Threats and Preparedness

1.1 Introduction

Bangladesh is rapidly moving towards a digital economy. Coping with the advancement of information technology, most of the banks have introduced core banking system with new transaction methods through alternative delivery channels like payment cards (debit and credit), ATM, Internet Banking and mobile banking. Increasing adoption of digital banking and wallets developed new security threats and attract targeted attacks from cyber criminals. Various threats have emerged in the cyberspace such as phishing, key-logging, spyware, malware and other online-based frauds that are specifically designed to target the bank customers. Banking industry has been attacked by sophisticated malware around the world. For example, botnet is a kind of malware which deliberately pilfer confidential banking and financial information.

As a regulatory body, Bangladesh Bank (BB) has encouraged Bangladeshi banks to keep up smooth and robust e-banking operations. BB has taken necessary initiatives to start e-commerce, e-banking, Automated Clearing House System (ACHS), mobile phone banking, etc. Banks can perform online money transactions, payment of utility bills, transfer of funds, payments for trading goods and services through e-channels like Internet, ATM, Mobile phone, etc. Other major successful projects of BB are NPSB, BACPS, BEFTN, CIB, Data warehouse, etc. Central Bank and the bank management have taken collaborative effort so that the scheduled banks of Bangladesh can be connected to each other for conducting inter-bank online transactions for smooth operation of full-fledged online banking in Bangladesh. Such activities have accelerated the development of ICT in our banking sector, some banks are still striving to upgrade their IT infrastructure. And it is expected that within a very short duration all Bangladeshi banks will be able to provide online services.

Globally a significant change has been seen in technology landscape. As security risks and cyber threats are increasing at an alarming rate, banks and their IT teams face severe challenges to overcome all those risks and threats. In financial institutions cyber-attacks are becoming more common, more erudite, and more widespread than before. Hacktivists want to spread political statements by disrupting the system. On the other hand, cyber-crime groups and other wrongdoers crack systems for financial gain—such as stealing funds through account takeovers, ATM thefts, and other manoeuvres. The cost of technology has been decreasing in the last few decades, as a result the hurdles to entry for committing cyber-crime also drop. Now it is easy and cheap for offenders to find out

new and innovative ways to commit cyber fraud. Also there exists an underworld black market that sells breached data which inspires wrongdoers further.

Cyber security mentions the capacity to safeguard the utilization of internet from cyber attackers. In coming days, the drift of advanced cyber-attack is going to be increased as anticipated by cyber security specialists. What's more, the financial institutions that are essential part of country's basic infrastructure, remains an ideal target for cyber lawbreakers. Like reputational and monetary risk, cyber risk can also impacts banks' main concern. Loosing clients' faith may take a toll on banks' business, and, in many cases, the bank could be considered legitimately blameable. Beyond the effect on an individual bank, cyber threat has significant financial penalties. Because of the intrinsic interconnecting properties of Internet, a security break at some financial institutions can impose a critical danger in growing customer confidence and the country's financial strength.

Banking sector of Bangladesh has been ignoring cyber security for many years. As a result banking information and critical infrastructures become vulnerable to the cyber attackers. Different studies by BIBM have proved this point very well. Reserve fund heist of Bangladesh Bank (BB) triggered cyber security issue again. The banking industry of Bangladesh also neglected cyber security due to the absence of effective cyber security regulatory norms in Bangladesh.

Frequently through the press and media it is seen that banking frauds are happening on account of the absence of client awareness about security. As a result, customers and bank face huge financial loss. IT governance and security audit are two areas that have come into place which mandates that the information security audit has to be done periodically for particular procedure.

Cyber-attack is becoming a societal issue now-a-day. All major industries, especially the financial service industry face severe cyber-attack. Once it was thought that IT security is an issue of ICT division only. Now CEOs and the top management need to rethink that cyber risk is not only IT issue, but also a CEO and BODs issue.

Cyber security is a key risk for banks, with a rise in the number of cyber-crimes. Bangladeshi banks are driven by modern digital technologies with a huge growth in online transactions but have also generated risks of protecting confidential information and sensitive financial data. Since the importance of Information Systems Security is increasing in banks, BB has issued an ICT security guideline for banking and financial institutions. BB has also mandated establishment of IT Governance and IT Security for all banks in Bangladesh. Though BB has issued some basic level guidelines and recommendations for financial institutions but they do not fully comply with international

standards. Again, most of the banks in Bangladesh have failed to conform with the guidelines of BB till now and even absence of clear time bindings has allowed them to take this liberty.

Although ICT risk management guideline has been developed by almost every bank in accordance with the BB ICT Security Guidelines, but in most cases, these are not implemented properly. The banking sector identifies itself as unprotected and exposed in terms of information insecurity. With this background this research project tries to explore the situation of information security measures, challenges in safeguarding this, and proposes some policy alternatives.

1.2 Objective of the Study

This paper will examine the current situation of implementing information security measures and its vulnerabilities. The specific objectives of the study are: **one**, sharing the global experience of new online threats and frauds specially for FIs and Banks; **two,** assessing the threats, vulnerabilities and preparedness of the banks of Bangladesh against these threats; and **three**, identifying the challenges of information system security and suggesting future courses of actions in ensuring better and secured IT based services of banks.

1.3 Methodology

The study used both primary and secondary data. Secondary data has been obtained from different online and physical sources (websites and published articles). Both interview and questionnaire methods were used for collecting primary information. The major strength of the study is the primary data that has been collected from 45 centralized online banks covering SOCBs, PCBS, SBs and FCBs. The study has been enriched by detailed analysis of all the data and information acquired from the filled-up questionnaire of the banks. For the field survey regarding customers' and end-users' awareness on online banking security, a sample of 750 bank customers and 450 employees were also selected covering all categories of banks. Moreover, our study involved more than 30 individuals in the rank of CIOs, CTOs, CISOs, CROs, COOs and security professionals.

1.4 Organization of the Paper

The paper is organized into six sections. **The first section** describes the introduction, objectives, and methodology. **Section two** reviews the literature, **Section three** depicts global experiences regarding threats and frauds in online banks/FIs, **Section four** shows an in-depth analysis of surveyed data related to threats and vulnerability of Banking Information System, and finally **Section five** identifies the challenges and put forward some recommendations.

2. Literature Review

This part reviews relevant literature and findings of previous researches that addressed the IT security in banks. The studies conducted in the context of developed and developing countries are presented here in to highlight existing knowledge.

'The Cybercrime Survey Report: Insights and Perspectives' of KPMG (2017) reveals that, "Over the last few years, cybercrimes have become more intense, sophisticated and potentially debilitating for individuals, banks and nations. Law enforcement agencies are finding it difficult to check and prevent the crimes in the cyber space because the perpetrators of these crimes are faceless and incur very low cost to execute a cybercrime whereas the cost of prevention is extremely high. Targets have increased exponentially due to the increasing reliance of people on the internet. Cybercrimes which were restricted to computer hacking till some time ago, have diversified into data theft, ransomware, child pornography, attacks on Critical Information Infrastructure (CII) and so on. With the increase in cyber incidents across the globe, for instance data hack in a famous financial entity has reinforced that the cyber risk if not managed well, can lead to significant impact. In this case, millions of customers had their personal information compromised and the CEO of the organisation had to resign due to the backlash faced over information leakage."

'The Cyber threat to Banking' study by PwC (2017) tells that, "In the last 10 years, digital technology has revolutionised economic and social interaction. It has transformed the way we do business, the way we educate ourselves, the way we sell and buy products and the way we share data. Internet use is growing and the methods by which it is accessed are diversifying. Malicious cyber actors are fully aware of this revolution and are taking full advantage of it. PwC report that nearly 60 percent of firms identify the speed of technological change as a threat to their growth prospects. The UK financial sector is already spending over £700 million annually. The issue is also being managed at board level, with 86 percent of banking and capital market CEOs identifying technological advances as the trend that will have greatest impact on their businesses."

In 2018, Judge Business School, Center for Risk Studies, University of Cambridge published a paper titled 'Cyber Risk Outlook' showing cyber risk is a continuously evolving threat. According to the study, "Financial theft has continued to be a major source of cyber-attacks and cyber-enabled fraud. Compromising networks of trust to misappropriate financial transfers remains a significant threat, despite major efforts to improve security. Cyber-attacks on customer systems continue to be a major cause of loss. Distributed Denial of Service (DDos) attacks continue to be a major component in the cyber risk landscape. A third of all organizations reportedly experience DDoS attacks, twice as many as a year ago. This trend of growing likelihood of attack is likely to

continue across sectors, geographies, and activity areas, as the firepower capacity of attackers increases, and they seek out new targets."

Deep analysis of different recent cases by SWIFT (The Evolving Cyber Threat to the Banking Community, 2017) reveals that "The attackers are using existing best-of-breed techniques, leveraging legitimate and malicious functionality. The use of these techniques has been mastered through successive attacks, leading to the sophisticated toolkits."

According to a study titled 'Digital Banking Fraud' by Net Guardian (2017), "Revolution in digital banking channels also triggers revolution in banking fraud. Today, digital banking fraud is a major international industry in which sophisticated criminal groups employ increasingly sophisticated tools – and frequently collude with corrupt bank staff – to steal very large sums. Digital banking fraud is now dominated by organized criminal gangs with access to high-end technology tools and detailed knowledge of banks' internal operations. In 2015, the City of London Police Commissioner warned that the value of thefts from banks through digital channels could already have overtaken that of the international drugs trade. There is even evidence that criminal groups that enjoy state sponsorship or protection are engaged in online banking fraud. More generally, too many banks have a weak control culture, where employees do not observe the correct processes and therefore create gaps in the bank's defenses that can allow fraud to slip through."

In 2012, Symantec study 'Banks likely to remain top cybercrime targets' finds that, "The majority of targeted attacks against the finance industry are likely to be for financial gain. Over 300,000 online Citibank accounts were compromised in a targeted hack of the organisation's network in 2011. The size of losses from such attacks is rarely disclosed by businesses, however, according to a 2011 Symantec State of Security survey, some 20% of large enterprise companies quoted an average of $195,000 in estimated damages. According to the Symantec Internet Security Threat Report, targeted attacks use customised malware and refined social engineering to gain unauthorised access to sensitive information. Banks are as exposed to 'mass market' attacks as any other organisation. But the greatest threat is probably from targeted attacks as these can be more difficult to detect and the attacker may focus on a specific system or set of information."

A study by Ernst & Young (Responding to cyber incidents in India, 2017) shows that, "In past two years, India has seen a rise in corporate scams and cases of espionage. Keyloggers, Trojans, hiring professional hackers and bribery are some of the means by which espionage can be performed. Bribery also continues to pose significant challenge in India, where a bribed insider could be involved with corporate espionage. This has resulted in an urgent need to improve detection and prevention measures around data theft. Corporate espionage has been identified as the second most critical motive for a

cybercrime and would continue to pose serious threat to companies in a highly competitive market such as India. In India, According to LEAs, there has been more than 50 percent increase in the number of' cybercrimes being reported in the last year. And 67 percent of LEAs feel that adequate laws are not in place, which address concerns related to cybercrime prevention, detection and investigation."

Another study by Ernst & Young (Confronting the new age Cyber Criminal, 2017) also identified that, "The advent of Digital India and Smart City initiatives has brought about a paradigm shift in terms of connectivity, services and threats for both urban and rural eco-systems. While greater connectivity promises wider deliverables, it also paves the way for the emergence of new vulnerabilities. Leading companies in energy, telecommunications, finance, transportation and other sectors are targeted by new-age cyber criminals. As per CERT-IN, one cybercrime was reported every 10 minutes in India during 2017. This statistics is quite alarming and therefore, merits a focused and collective attention of security enforcement agencies."

According to KPMG's report 'Global Profiles of the Fraudster, May 2016', "In 61 percent of cases weak internal controls were a contributing factor, up from 54 percent in the firm's previous report from 2013. In Europe, 72 percent of fraudsters told KPMG that weak controls presented the opportunity they were looking for." The study also mentioned that "Vendors, suppliers, customers and employees are all critical components of a successful business, but come with risks, and successful attacks against these often perceived weaker links will have an indirect impact. As technological systems and controls improve, people are increasingly seen as the weakest link. Employees at all levels within an organisation can act as insiders wittingly or unwittingly. They can either use their access to systems to assist malicious actors in conducting attacks or to compromise systems for their own gain. Threat actors are increasingly employing targeted social engineering techniques, such as spear-phishing, to trick individuals with access to key systems to inadvertently act as insiders. Insiders present a potent threat due to their privileged position with access to systems and knowledge of procedures. The study shows 41 percent of economic crime was committed by employees within an organization."

"Political instability is often a trigger for cyber-attacks. The recent Russia and Ukraine crisis not only had a huge impact on banks' sanction obligations but also caused a wave of retaliation cyber-attacks from Russian and Ukrainian groups. Another well-reported example of politically motivated cyber-attacks were committed against US banks in 2013 by the Muslim hacktivist group al-Qassam Cyber in retaliation for the posting to YouTube of a film that mocks the founder of Islam. Again in 2013 South Korea suffered a cyber-attack that impacted on payment services and cash machines that is suspected to

be part of their ongoing dispute with the North Korea – interestingly in this example the anonymous hacktivist collective 'claimed' the attack, although South Korean officials suggest this was false"-according to the 'Confronting the New Age Cyber Criminal, 2017' report of Ernst & Young.

3. Experience of Global Cyber Threats and Online Frauds

According to World Economic Forum, "Corporations and consumers are increasingly adopting and embracing digital innovations which are dependent on mobile and digital technologies to manage their businesses and daily lives. In 2017, world's population stood at 7.467 billion whilst internet user population grew by 10% in 2017 to 3.773 billion, up 354 million compared to 2016. In 2017, there were 2.8 billion social media users globally. It was also remarkable that active social media users increased by 21% in same year, up 482 million compared to previous year. 66% penetration of global mobile users in 2017 equals to 4.92 billion. The number of mobile connections in Association of Southeast Asian Nations (ASEAN) has outpaced global average at 133%. Moreover, more than 1.6 billion e-commerce shoppers worldwide spend a combined total of close to US$2 trillion in 2016. Cyber-crime is a growing and persistent threat to corporations and consumers who are relying on mobile, social media and online platforms. Up to 2016, annual cost to global economy is US$500 billion. Despite big corporations, 20% of small and medium-sized businesses have been targeted to date. Estimated annual cost (2020 and beyond) of malicious data breaches is US$2.1 trillion. Businesses are set to dramatically increase their spending on security."

In 2017, World Economic Forum identified that "Income disparity, extreme weather events, unemployment and underemployment, climate change and cyber-attacks as top 5 global risks in terms of likelihood." World Economic Forum forecasts that "delays in adopting sound cyber security hygiene could result in a US$3 trillion loss in economic value by 2020. Reputational impact can reach to US$180 million."

Box 1: Top Cyber Crime in 2017

- 200K+ Computers in 150 countries were affected by Wannacry malware
- Wikileaks published a data trove containing 8761 documents stolen from CIA
- Two days before France's Presidential runoff, hackers dumped a 9 GB trove of leaked emails from the party of Emmanuel Macron
- 125+ machines in 64 countries faced the threat of Patya ransomware
- Cyber risk researcher discovered a publicly accessible database with personal information for 198M USA voters in 2017

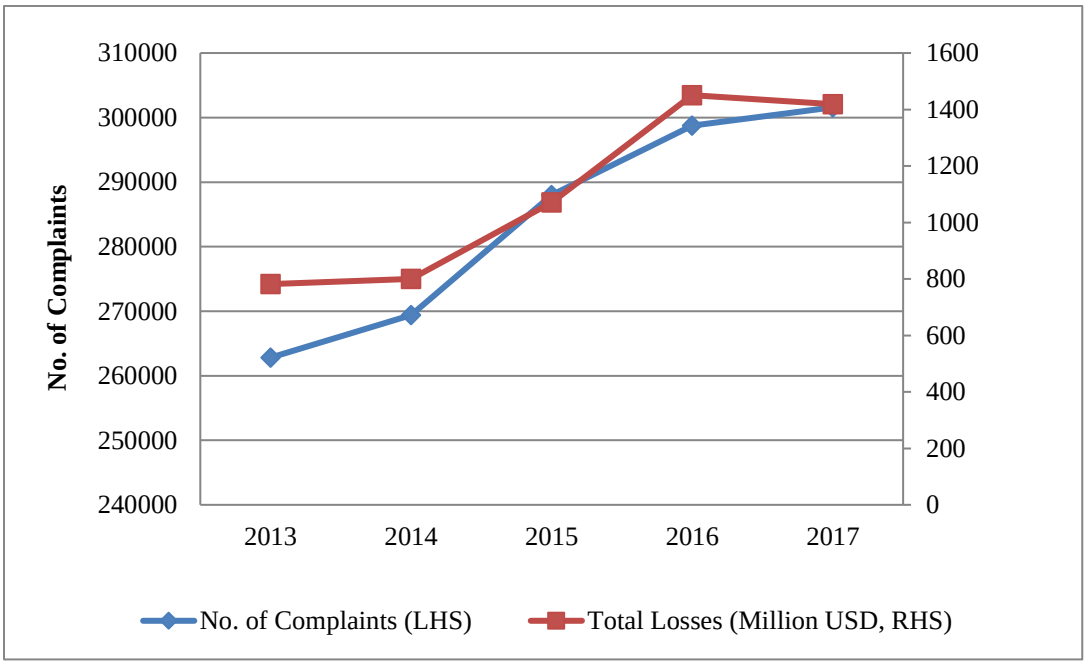
Source: Confronting the New Age Cyber Criminal, Ernst & Young

3.1 Cyber Threats and Fraud Identified by RSA

The RSA® Quarterly Fraud Report contains fraud attack and consumer fraud data and analysis from the RSA® Fraud and Risk Intelligence team. It provides a picture of the cyber fraud situation, providing actionable intelligence to consumer-facing organizations of all sizes and types to facilitate more operational digital risk management. According to the report, "For the period starting January 1, 2018, and ending March 31, 2018, RSA observed 25, 581 global fraud trends across attack vectors and digital channels. Phishing accounted for 48 percent of all cyber-attacks observed by RSA Canada, the United States, India and Brazil were the countries most targeted by phishing. Financial Trojan horse malware accounted for one out of every four fraud attacks observed by RSA. Consumer transactions and fraud continue to grow in the mobile channel. In the first quarter, 55 percent of transactions originated in the mobile channel and 65 percent of fraud transactions used a mobile application or browser. More than 80 percent of observed fraudulent e-commerce transactions originated from devices that were 'new,' meaning unknown to RSA's Risk Engine at the time of observation."

3.2 Internet Crime Identified by IC3

Figure 1: Internet Crime Reported by IC3



Source: IC3

According to the 'Internet Crime Report' by IC3, "In May 2000, the Internet Crime Complaint Center (IC3) was established as a center to receive complaints of Internet crime. There have been 4,063,933 complaints reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of more than 284,000 complaints per year. The complaints address a wide array of Internet scams affecting victims across the globe. The 2017 Internet Crime Report emphasizes the IC3's efforts in monitoring trending scams such as Business Email Compromise (BEC), Ransomware, Tech Support Fraud, and Extortion. In 2017, IC3 received a total of 301,580 complaints with reported losses exceeding $1.4 Billion."

3.3 Cyber Threats and Fraud Identified by Kaspersky

Kaspersky report 'A global survey into attitudes and opinions on IT security' identifies that "Nearly half of the business organizations feel cyber threats will be a top priority in the next two years and yet 45% don't feel fully prepared. 91% organizations have been affected by attacks in the last year. 45% are under-prepared for dedicated cyber-attacks and 17% have lost financial information as a result of attacks. 57% have banned access to social networks due to potential security risks and 30% have still not fully implemented anti-malware software.

The majority of threats (61%) coming from malware and network intrusions, the threat for businesses is not just from external sources. Internally, the top vulnerability came from flaws in existing software – with 44% of organisations having a related incident in the last 12 months. Staff also poses an internal threat to data loss – 10% of organisations have been victims of fraud or sabotage from their own staff and 16% of organisations highlight intentional data leaks as their most concerning data threat for the future.

Social networking, for example, is now seen to be the second biggest threat to IT security – with 57% of organisations viewing use of social media by employees as a significant risk to the business. 53% of organisations have banned social networking sites for end users to some extent.

Unfortunately for organisations across the globe, these are not just threats coming round the corner in the future – but real issues that are affecting them across the business every day. In the last year, 91% of organisations have experienced at least one attack, most commonly in the form of malware, subsequently followed by Spam and Phishing attacks. Of these, 24% have had their network intruded in some way – with 7% losing sensitive business data as a result, at a significant cost to the business. In developing countries, the levels of data loss are much higher, due to the lack of experience to correctly build and defend infrastructure against modern attackers."

Case 1: Equifax Data Breach

"In July 2017, credit reporting agency Equifax was the victim of a significant data breach which resulted in an estimated 143 million U.S. records containing customer information being stolen by hackers. This included social security numbers, dates of birth, and the credit card details of over 209,000 Americans. The breach also impacted other countries, with Equifax admitting that 15.2 million records of British citizens and 8000 Canadians were stolen in the breach. There was over a month's delay in disclosing the data breach. Senior executives were criticized for selling shares in the days before the breach was announced to the public. The intruders managed to gain access to the records using a weakness in a popular back-end website application. The vulnerability was made public in March 2017, but Equifax were slow to fix the bug in their networks, highlighting the importance of maintaining the latest patches. The Equifax hack had the markings of a sophisticated cyber-attack, leading to speculation about attribution, with some in the cyber security community blaming Chinese-backed groups due to similarities with other attacks such as the U.S. Office of Personnel hack in 2017. The potential for the stolen Equifax data to be used in financial fraud has caused U.S. banks such as Citi Group and Wells Fargo to step up anti-fraud controls."

Source: Cyber Risk Outlook 2018, University of Cambridge.

Case 2: Denial of Service Attack on Swedish Transport System

"DDoS attacks not only threaten the internal infrastructure of a company but also pose a threat to physical structures which rely on working networks. Starting on October 11, 2017 DDoS attacks disrupted the Swedish Transport Administration (Trafikverket) which sent the IT system that monitors the company's train locations, email systems, and road traffic maps off-line. This network disruption brought Sweden's transportation services to a standstill. The Transportation agency was forced to stop or delay trains during the attack and the traffic maps were affected into the upcoming days. The following day, the attacks on the Swedish Transportation System continued. On October 12, 2017, the DDoS attacks focused on the website of the Swedish Transport Administration who is responsible for regulating and inspection systems and the transport operator Vasttrafik – taking down both their online booking and travel planning services for trains, buses, ferries, and tram transports.The perpetrator for these attacks has yet to be named, but presumed motivations of disrupted transportation services were successful. This cyber-attack was the second in a four-month span for Sweden's Transport Administration, with a previous attack targeting Sweden's air traffic control center. Swedish officials attributed this November 2015 attack which grounded flights, to Russian cybercriminals."

Source: Cyber Risk Outlook 2018, University of Cambridge.

Case 3: WannaCry Malware Attack

"WannaCryptor ransomware spread via file-sharing network protocols on computers using outdated Windows XP and v8 OS. It resulted in 300,000 infections of computers across 150 countries. WannaCry used a NSA exploit code named EternalBlue (made available the previous August by ShadowBrokers). It predominantly affected personal users, public sector organizations, and SME-scale companies, affecting unpatched boxes and equipment on dedicated older operating systems. Several dozens of large companies also reported disruption and losses from infections of their systems. Of the roughly 400 million actively-used Windows computers running version 8 or earlier operating system, approximately 0.1 percent was infected. The great majority of the Windows computers running version 8 or earlier were protected by a Microsoft patch MS17-010 issued two months earlier, in March 2017. The event highlighted the issue of equipment software latency, i.e. that machines and sub-networks within organizations may rely on specific versions of operating system that render them vulnerable. In these cases, although the majority of systems within organizations ran more up-to-date operating systems, certain departments and activities were maintaining the older versions that contained the vulnerability. Machines such as medical MRI scanners and X-Ray machines that were certified on XP and v8 and maintained on those operating systems were among those that were crippled by the attack.

Businesses reported substantial losses from lock-outs of systems around the world, such as manufacturing processes, dispatch and ordering systems, gas pump payment applications, and telephone exchange equipment. We estimate the direct costs and indirect business disruption losses from WannaCry to be around half a billion dollars. If the WannaCry malware was created to generate ransom payments then it was remarkably unsuccessful. The BitCoin accounts that it requested payments into received less than $150,000 in payments and may not have been claimed by the criminals. No company that paid a ransom got its data back. The motivation was more likely to sabotage some of the affected companies, rather than generate funds for the hackers. It is possible that the widespread economic disruption was collateral damage to mask a targeted destructive attack. The propagation of WannaCry was stopped after four days by a researcher finding a kill-switch within the software. Otherwise the infection could have spread to many more machines and had a more severe impact. RMS counterfactual analysis suggests that if the kill-switch had not been triggered, and if the attack had occurred prior to the issuing of the MS17-010 patch for Windows 8, the infection rates and losses could have been an order of magnitude higher, perhaps reaching $3 to $6 billion."

Source: Cyber Risk Outlook 2018, University of Cambridge.

3.4 Cyber Threat Landscape- Global

According to ASEAN Bankers Association, there is a bustling underground cybercrime economy that easily undermines global cybersecurity spend of US$75 billion annually. Cybercriminals often spend weeks to months (up to 146 days) within their victim's network learning about their systems, business processes and people before mounting an attack. 91% of cyber-attacks start with a phishing email. It also seen that there is a 76% reduction in spend on responding to security events when employees are security-aware and trained. Moreover, 95% of security incidents investigated worldwide was attributed to human error.

Currently there is a well-established "Cybercrime Economy" in the globe. Cost per 1000 credit card number or e-mail accounts is 50 cent to $20. $7 to $8 is given for hacking cloud accounts. Price per healthcare record goes up to $50. Average cost of a data breach in 2016 was US$4 million, 13.6% increase from 2015. Up to $1000/day is paid for DDoS attack and up to $3500 is paid for custom malware attack.

3.5 Cyber Threat Landscape- ASEAN

Just like its neighbors in North and South Asia, ASEAN faces a complex cyber threat landscape where cyber adversaries have persistent intent to commit espionage, sabotage and steal corporate data.

- Hackers are 80% more likely to attack organizations in Asia.
- Asian organizations take 1.7 times longer than the global average to discover a breach. Average dwell time is 146 days for global and 520 days in Asia.
- 70% of firms do not have strong understanding of their cyber posture. Asian firms spent 47% less on information security than North American firms.
- 78% of internet users in Asia have not received any education relating to cybersecurity.
- 74% of organizations in Asia found it difficult to recruit talent in cybersecurity.
- An anti-cybercrime operation led by INTERPOL in April 2017 has uncovered 9000 malware-infected servers and 270 compromised websites in South East Asia.
- The first cases of "WannaCry" infections were reported in Asian countries such as India, Hong Kong and the Philippines.

Recent attacks in ASEAN countries are summarized in the following table.

Table 1: Recent Attacks in ASEAN Countries

Country	Attacks
India	3.2 million Debit cards from at least five banks were compromised as cyber attackers introduced malware in the payment services systems.
Bangladesh	Cyber attackers stole $ 81 million from the central bank by hacking into an official's computer and transferring the funds to the Philippines.
Hong Kong	Personal data of 6.4 million children were leaked in cyberattack of a digital toymaker firm.
Japan	7.9 million Individual personal details were exposed when Japan's largest travel agency was compromised.
Taiwan	16 ATM thieves installed three different malware programs into ATMs to steal more than $ 2 million.
Philippines	68 government websites were compromised, including defacement, slowdowns and distributed denial-of service (DDoS)
Vietnam	An airline system was breached and the personal information of 400000 frequent flyers was leaked online.
Thailand	$350000 from 18 ATMs belonging to a local savings bank was stolen by individual with malware-equipped ATM card.
Singapore	850 personal at the Ministry of Defence had their personal details stolen, in an attempt to access official classified information.

Source: ASEAN Bankers Association

3.6 Cyber Threat Actors: Lazarus Group

"Lazarus group are assessed to be a North Korean state sponsored threat actor who has been active since 2009. Linked to a number of high-profile attacks, they have recently been linked to a recent campaign against financial institutions, the aim of which appears to be financial gain."- ASEAN Bankers Association.

Attack History:

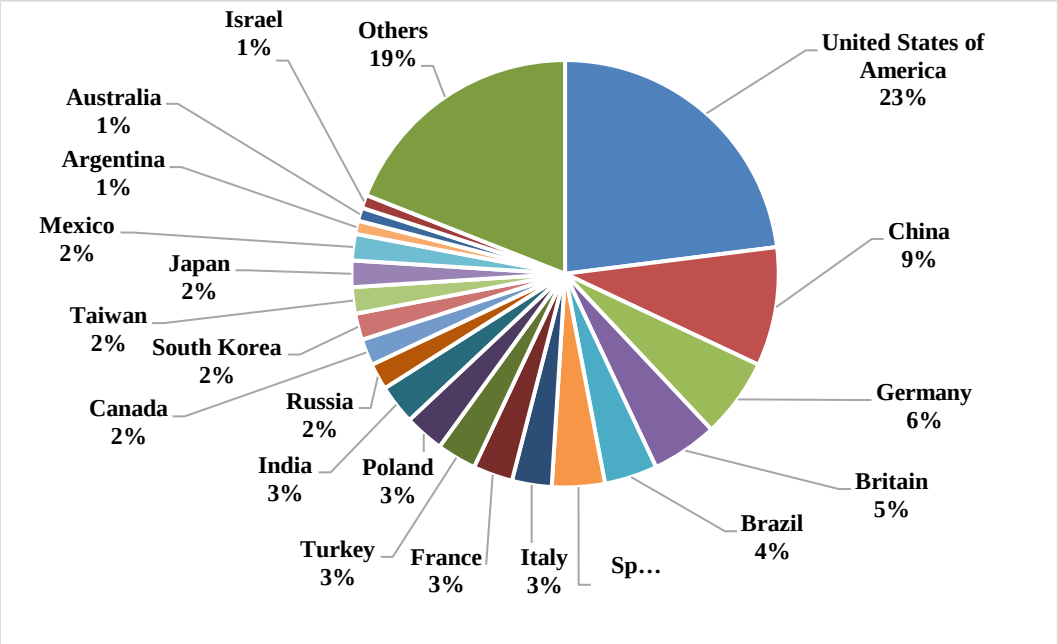
Apr 2011- Nonghyup Bank	Jul 2016- First Bank Nigeria
Mar 2013- Shinhan Bank	Oct 2016- Financial Supervision Authority Poland
Mar 2013- Jeju Bank	Oct 2016- Bank of Eastern Republic of Uruguay
Jul 2014- Online Casino	Nov 2016- National Banking and Securities
Nov 2014- Sony Pictures	Commission Mexico
Jan 2015- Banco Del Austro	Dec 2016- Akbank, Turkey
Oct 2015- Unnamed Philippines Bank	Dec 2016- Bangladesh Uttara Bank
Feb 2016- Bangladesh Bank	Feb 2017- Nonghyup Bank
Feb 2016- Credit Union South Korea	Feb 2017- VAN ATM
Mar 2016- ICICI Bank	Mar 2017- Unnamed Bank in Gabon
May 2016- Tien Phong Bank	Apr 2017- Capital Bank Botswana
Jun 2016- Unnamed Ukraine Bank	May 2017- WannaCry (200,000 computers across 150
Jul 2016- INTERPARK	countries)

Source: ASEAN Bankers Association

3.7 Cyber Crime and Frauds in India

Jul 7, 2018, 'The Times of India' reported that, "Cyber crime cases across India rose 44% between 2013 and 2017. Of the 3,474 cyber crime cases reported in India last year, a majority (60%) related to online banking. India is estimated to be losing 0.21% of its GDP to cybercrime and the numbers of incidents are increasing each year."

Figure 2: Top 20 Countries Impacted by Cybercrime



Source: Confronting the New-Age Cyber-Criminal, Ernst and Young.

According to the study, 'Confronting the New Age Cyber Criminal: Background', "India is becoming increasingly vulnerable to this menace because of rapid digitization and proliferation of mobile data without matching pace of cyber security and cyber hygiene. At present, India is ranked third in terms of cybercrime incidents behind the United States and China (Figure 2). As per CERT-IN, one cybercrime was reported every 10 minutes in India during 2017.

Ransomware continues to be a major threat the world over. In 2017, WannaCry, Petya, Not Petya, etc. caused major disruptions in the connected cyber ecosystem of the world. India was also affected. CERT-In confirmed 37 incidents of WannaCry and Petya attacks in India between May and June 2017. Petya caused extensive disruption of services in India. One terminal of JNPT, Mumbai had to switch over to manual operations due to this attack. India was the worst affected country in Asia and seventh overall, due to Petya attack.

Apart from ransomware, another area of significant concern is theft of personally identifiable information (PII) and financial credentials of individuals. In another incident

of cybercrime, criminals stole personal data of over 2.74 lakh Indian users of the Ashley Madison website. Hackers, who stole 300GB of personal information of the users, put it up on sale over the dark web. Also, Cryptojacking is another lucrative method adopted by attackers to deploy a malware forcefully and unknowingly into a victim's computer to use their hardware for generating cryptocurrency. It is becoming yet another tool of choice for cyber criminals because it cannot be classically categorized as a crime.

One reason why cybercrimes are becoming more sophisticated, better orchestrated and increasingly ambitious is because many of the perpetrators operate outside the jurisdiction of the victim's country. As per industry estimates, 32% of the threat vectors originate from Eastern Europe and Russia and social engineering is the preferred mode of launch for most perpetrators."

Table 2: Rise in Cyber-Crime in India

Cyber Crime	2017		2016	% Increase
Online Banking	2095		1341	56.2
Facebook related	316		151	109.3
Email hacking	125		97	28.9
Sexual harassment	81		51	58.8
Lottery fraud	42		15	180.0
Data theft	47		43	9.3
Job fraud	49		40	22.5
Twitter related	12		4	200.0
Total Cases	**3474**		**2402**	44.6

Source: Confronting the New-Age Cyber-Criminal, Ernst and Young

3.8 Cyber Fraud Related to Cryptocurrency

According to the study, 'Confronting the New Age Cyber Criminal', "Cryptocurrency or virtual currency is a type of exchange currency where cryptography is used to process payments, safeguard transactions and limit the production of additional units. The Blockchain technology, where a decentralised ledger keeps logs of all transactions, creates the foundation for these cryptocurrencies. These currencies work independent of central banks and Governments and there are a number of cryptocurrencies available for use online such as Bitcoins, Litecoins or Dogecoins. The value of this virtual currency is unaffected by country-specific economies, as the currency is finite in number and depends on factors such as usage, supply and demand. The challenges in using virtual currency is that these systems are capable of facilitating tax evasion or illegal activities because of the anonymity factor which is built into the system. As a result, Bitcoin is a preferred mode by hackers for ransomware. That said, the number of transactions done globally are rising – statistics available on blockchain.info suggest that per day transactions for Bitcoins have increased from approximately 100,000 transactions in

January 2015 to approximately 350,000 transactions in January 2017, a 250% rise. The rise in usage can lead to a surge in cyber-attacks, raids and fraud."

Case 4: Demand of Bitcoins as Ransom

"By tracking the Bitcoin accounts associated with ransomware, researchers at University of Padua, Italy have calculated how much cyber criminals have extracted from their victims. They created a database of Bitcoin accounts associated with ransomware activity since 2013 when "Crypto locker" became the first ransomware to ask for payment in bitcoins. It has emerged that "Crypto wall" has collected more than US$4.5 million in bitcoins and other transactions and remains the most productive malware till date. Contrary to popular perception, WannaCry and NotPetya received only US$86,076.76 and US$9,835.86 respectively despite the hype around them. Cybercriminals use cryptocurrencies because of anonymity. However, bitcoin transactions are pseudonymous because even a single transaction that links Bitcoin account to a personal account can reveal the identity of the cybercriminal. This prospect should excite the LEAs and encourage the use of analytics to establish such linkages."

Source: Confronting the New-Age Cyber-Criminal, Ernst and Young

3.9 SWIFT Related Financial Theft

The study 'Confronting the New Age Cyber Criminal' by Ernst and Young noted that "There has been a significant evolution in the cyber threat facing the global financial industry as adversaries have advanced their knowledge. They have deployed increasingly sophisticated means of circumventing individual controls within users' local environments, and probed further into their systems to execute well-planned and finely orchestrated attacks. The groups behind these attacks are deploying ever more creative techniques to access users' critical assets. These include gaining Administrator rights for operating systems, manipulating software in memory, and tampering with legitimate functionality to bypass two-factor authentication. Highly covert malware is now being deployed, designed to withstand traditional detection techniques. Furthermore, in any single attack a mix of malicious files will often be used, whether that be to acquire credentials or to bypass authentication requirements; to learn how internal operations or messages work; to create distractions and delay local security teams' responses; or to securely delete log files and other traces of the attacks. Forensic investigations are increasingly being hampered by the attackers' efforts to erase their activity and obscure their techniques. It is clear that the adversaries are prepared to invest considerable time in planning and preparing for attacks. In some cases it is observed that the attackers had been quietly present on customers' systems for longer than 12 months before actually attempting to execute the frauds – often doing so around public holidays."

Case 5: The Return of Lazarus: More SWIFT Financial Thefts in 2017

"Sophisticated cyber-attacks continued to enable financial thefts from the SWIFT inter-banking financial transaction system, following on from the major attacks in 2016. The victim of the 2017 attack was Far Eastern International Bank (FEIB) based in Taiwan. The gang used a vulnerability in the banks security, which allowed the group to secretly implant their malicious malware onto the bank's computers and servers. This lead to a SWIFT terminal operated by the bank becoming compromised.

Once the group gained access to the SWIFT network and acquired the credentials necessary for payment transfers, the group attempted to fraudulently transfer $60 million to accounts in United States, Cambodia and Sri Lanka. Due to a mistake by the criminals causing an error in the specific fields of the SWIFT transfer, banking officials were alerted and all but $500,000 was recovered.

As with previous attacks on the SWIFT network, the attackers used a specifically-crafted malware with many layers of subterfuge to avoid discovery. The sophistication of the attack is highlighted due to the incorporation of ransomware in the attack, which is likely to have been used to mislead the cyber security community. However, the money laundering process was less sophisticated than in previous attacks on the SWIFT network, and two 'money mules' were arrested attempting to physically withdraw stolen funds from a bank account in Sri Lanka.

Some have attributed this attack to the North Korean state-sponsored hacking group Lazarus due to the similarities in the method of attack. This group is a sophisticated advanced persistent threat (APT) group which has been associated with many high-profile financial thefts including Bangladeshi SWIFT attack in 2016 and the 2017 attack on Polish banks.

The continuation of attacks on financial network highlights that these are attractive targets offering big rewards to cyber criminals. Systems in place continue to manage to stop the criminals extracting the full potential from the initial penetration, although other attacks are known to succeed."

Source: Cyber Risk Outlook 2018, University of Cambridge.

Case 6: Phishing Scam

"In June 2013, three men were jailed in the UK for a total of 20 years after police uncovered a phishing scam that targeted people in 14 countries and involved 2,600 fake webpages. After their arrest, the Metropolitan Police's Central e-Crime Unit located servers containing details of 30,000 bank customers, including 12,500 in the UK, and 70 million customer email addresses. They produced evidence at the men's trial that their arrest had prevented the theft of up to £59m from UK bank customers alone."

Source: Confronting the New-Age Cyber-Criminal, Ernst and Young

Case 7: Tesco Bank Suffers UK's First Mass Account Theft

"In November 2016, the bank owned by UK supermarket group Tesco suffered a huge online security breach in which a total of £2.5m was removed from 20,000 of its 136,000 current accounts and suspicious activity was discovered on a further 20,000. The robbery happened over a weekend, while bank staff were absent, and there has been no official explanation of exactly how the thefts were executed. However, experts suggested that hackers had identified a weakness in the Tesco Bank website and exploited it to steal thousands of customers' account details that were then used to make online purchases. On discovering the fraud, Tesco temporarily blocked online payments by its current account customers while continuing to allow them to use cards for cash withdrawals, chip and pin, and bill payments."

Source: Digital Banking Fraud, Net Guardian

Case 8: Android Malware Installs Fake Apps on Smartphones

"In June 2017, security specialists at FireEye reported that they had identified malware that installs fake versions of eight popular apps including Facebook, WhatsApp, Uber, Google Play and Viber on victims' smartphones. They are sent a text message saying: "We have not been able to deliver your order. Please check your shipping information here", followed by a link. Once the victim clicks the link, it installs the malware, which waits for the user to open one of the targeted apps. The malware then overlays a fake interface on top of the legitimate app and attempts to trick victims into divulging their online banking information. The phishing texts were first seen in Denmark, where 130,000 victims were tricked into clicking the link. The malware is thought to have spread to the UK, Germany, Luxembourg, Spain, Sweden, Norway, the Netherlands, Italy, Greece and Turkey."

Source: Digital Banking Fraud, Net Guardian

Case 9: Poor Security at Software Supplier Opens The Door to Fraudsters

"In one recent East African case cited by fraud specialist Gilbert Nyandeje, chief operating officer of Enovise, a software developer at the company hired to build a mobile banking app left a "back door" in the source code that was not detected before the app went live. Once implemented, the back door created an outgoing, or reverse, connection from the bank's systems that criminals could use to access customer accounts, stealing a total of more than $50,000 before the flaw was detected. This method of breaching the bank's security succeeded because while internal firewalls prevent outsiders from getting into the system, they do not necessarily block outgoing connections."

Source: Digital Banking Fraud, Net Guardian

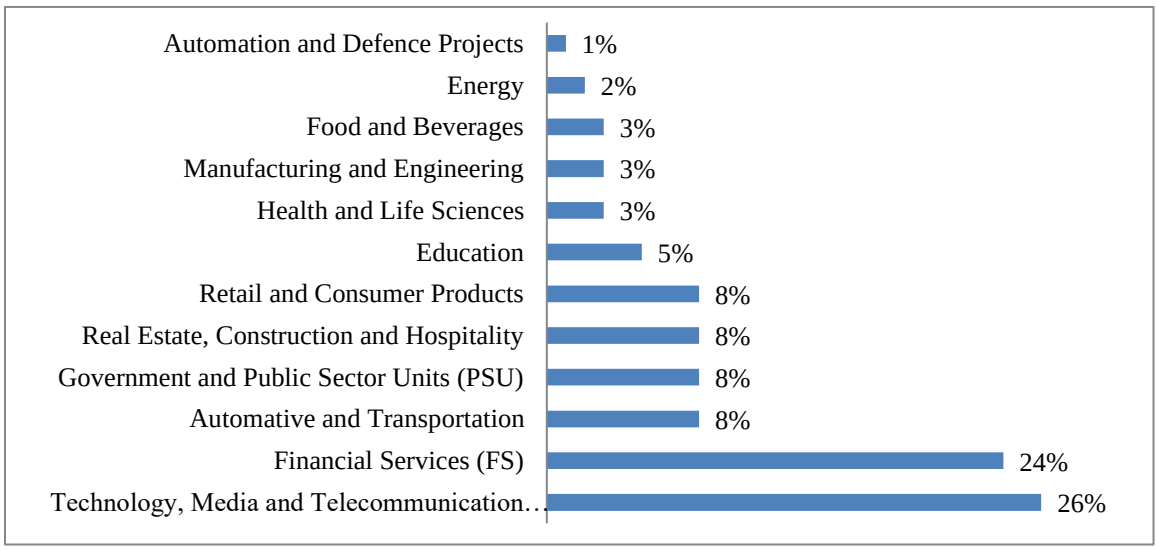
3.10 Confronting the New age Cyber Criminal: Ernst and Young

According to Ernst & Young, "Today, cyber criminals are well funded, persistent, sophisticated and globally coordinated. Their level of knowledge and the understanding of new technologies supersede most others. This, coupled with companies trying to integrate their systems and processes with new technologies and platforms, further broadens the areas vulnerable to attacks.

The advent of cybercrime was characterised by usage of Trojans or worms, scams, keyloggers, phishing and adware. The hackers' attack vector was very similar to the military strategy involving 'carpet bombing or saturation bombing'. This was used by various countries during the World War II, where thousands of unguided bombs would be dropped on the enemy soil without any specific target. Hackers used the same strategy and went after the masses for even small gains per hit as for them there is no cost per attack.

With the turn of the decade and with more sophisticated cyber-weaponry at their disposal, the hackers turned their focus on more lucrative targets. Instead of throwing their net around for small fish, they started going after the big whales. Attacks on core banking infrastructure, advanced persistent threats, ransomware attacks using social engineering and DDoS attacks using botnets created out of the internet of things (IoT) devices have now turned out to be the flavour of the season. The cybersecurity controls deployed have also evolved in the last decade as the awareness amongst the organizations has increased. Instead of focusing on 'prevention' after the incident, the focus is now on detecting the attacks in real time and responding to them in an appropriate manner."

Figure 3: Sectors that have witnessed a Cyber-Attack

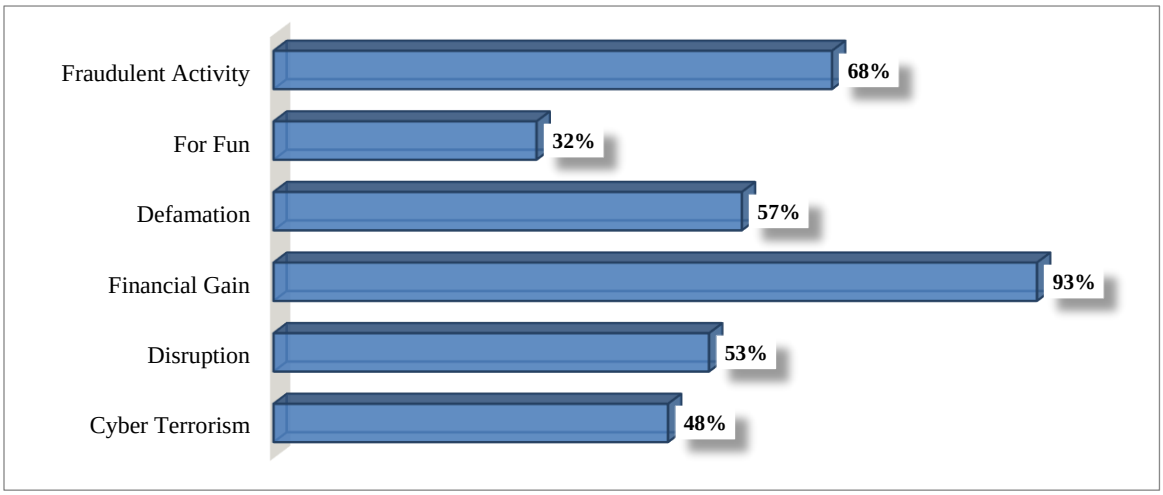


Source: Ernst and Young

"Incidents such as ransomware, data breach and DDoS attacks on organizations are making headlines worldwide. For organizations dealing with such situations effectively is a key priority. This can be a difficult task due to the changing nature, high complexity and huge volume of cyber incidents."- Ernst and Young

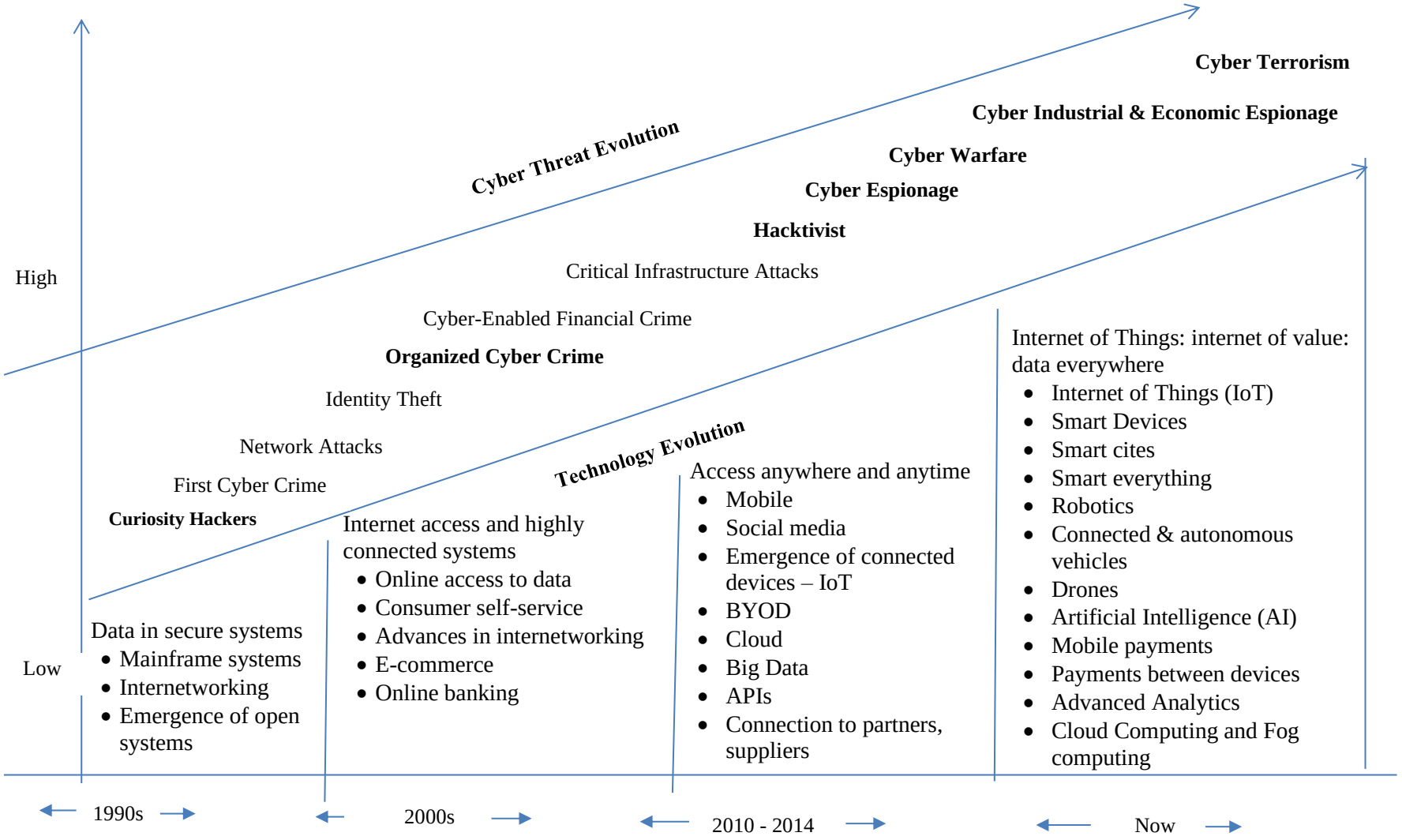
Motives of the cyber-attacks are identified by the LEA of India are shown below (Figure-4). It is found from the figure that 93% cyber-attack take place for monetary purpose. Fraudulent activity (68%) is another prominent reason behind this kind of attack. Also denouncing a particular organization drives many attackers to conduct cyber-attack (57%). Among other motives, disruption of service (53%) and cyber terrorism (48%) is noticeable.

Figure 4: Motives of Cyber Attack



Source: Confronting the New-Age Cyber-Criminal, Ernst and Young

Figure 5: Technology vs. Cyber Threat Evolution



Source: ASEAN Bankers Association

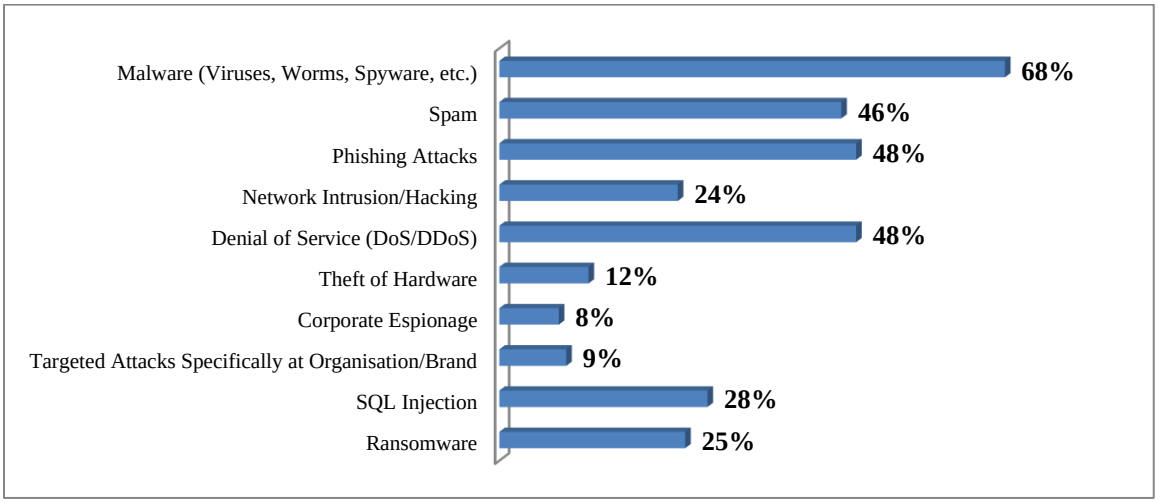
4. Analysis and Findings

4.1 Threats and Vulnerability of Banking Information System: External Threats

4.1.1 Cyber Security Incidents, Breaches and Impact on Business

For Bangladeshi banks, it is not like that cyber security breaches are yet to occur in the future. These issues are already disturbing them every day. Figure-6 depicts various types of attack faced by our banking sector. In 2017, 68 percent banks have faced malware attack which includes viruses, worms, spyware, etc. It is evident that malware attack is very common in our banking sector. It is also seen that 48 percent banks have experienced both problematic phishing and DDoS attacks respectively. Spam, SQL Injection, and ransomware attacks are growing in the banking and financial sectors. Again, 24% banks have faced network intrusion problem which bears momentous cost to the business. Also, a number of attacks are being explicitly directed to particular banks. We have found, among the surveyed banks about 9% have underwent a targeted attack in 2017 and they have lost some type of intellectual property in the attack. In fact, it can be said that this figure could be higher, as many banks may have been implicitly under attack but did not sense the situation.

Figure 6: Types of Attack



Source: BIBM Survey

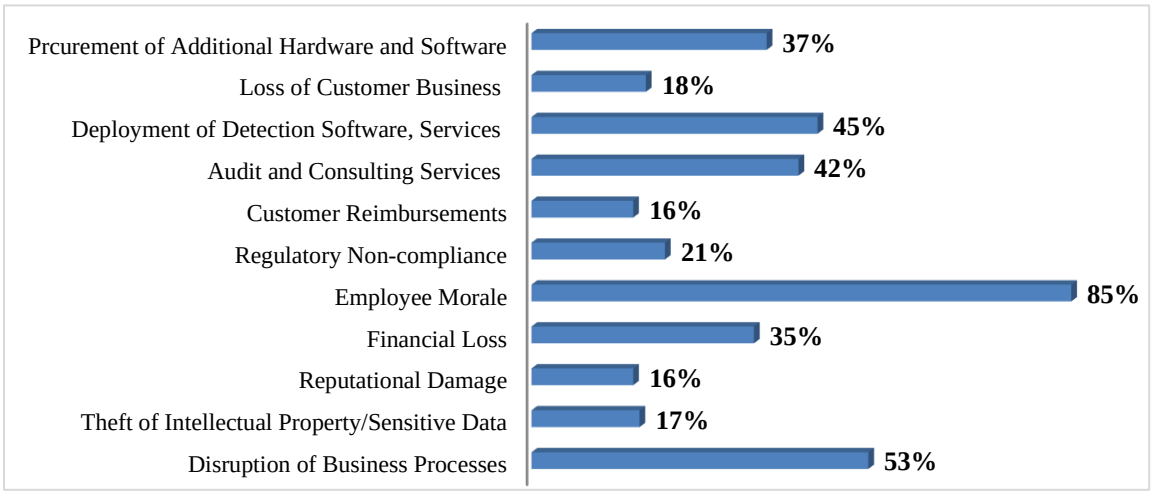
Regular security patch deployment can be an effective measure against malware and ransomware attack. Modern malware can target a particular weakness in the banks' systems through which attackers can spread malware and interfere their business. Recently these attacks are becoming more intensive. In recent world, ransomware tends to be more deadly because attackers are now attacking via specially crafted attacks. Banks should be prepared to tolerate ransomware attacks. The study reveals that 35 percent of banks were certain that they were not satisfactorily equipped to handle such kind of attacks, while 16 percent expressed that they were unaware of what to be done in

case of a ransomware attack. Some 59 percent banks knew that ransomware could cause a weighty business risk and 15 percent indicated that they were attacked by ransomware in the last year.

Now it is evident that financial industries are facing threats in a variety of natures and procedures. For example, 12% of banks have lost their hardware from their sites, which is one of the easiest ways to get sensitive information for future attacks. Organizations must embrace a resilient strategy consists of manifold layers of protection. It should also include anti-malware and full disk encryption technology to maintain safety as close as 100%.

Figure-7 shows the impact of cyber-attack in banking sector. According to the study, there is an impact on the morale of current workforce in the event of cybercrime attack across banks. 85 percent respondents believe that employees' confidence has ruined due to cyber-attack. The study also reveals that cyber-attack may cause the distraction of business process which is believed by 53 percent of the respondents. Attackers mainly target financial information. Almost 35 percent of the banks said that they have lost up to Tk. 40,00,000, due to cybercrimes. Banks that experienced financial loss in last year due to cyber security breaches have identified several factors in order to calculate the monetary loss. These factors were: (1) customer compensations (16%), (2) audit and consulting services (42%), and (3) placement of detection software, services and strategies (45%). Although many banks included factors like loss of client business (18%) and loss of brand/reputation (16%) into total loss calculations, but in many cases these losses were likely too challenging to measure overall economic loss resulting from a cyber-breach.

Figure 7: Impact of Cyberattack



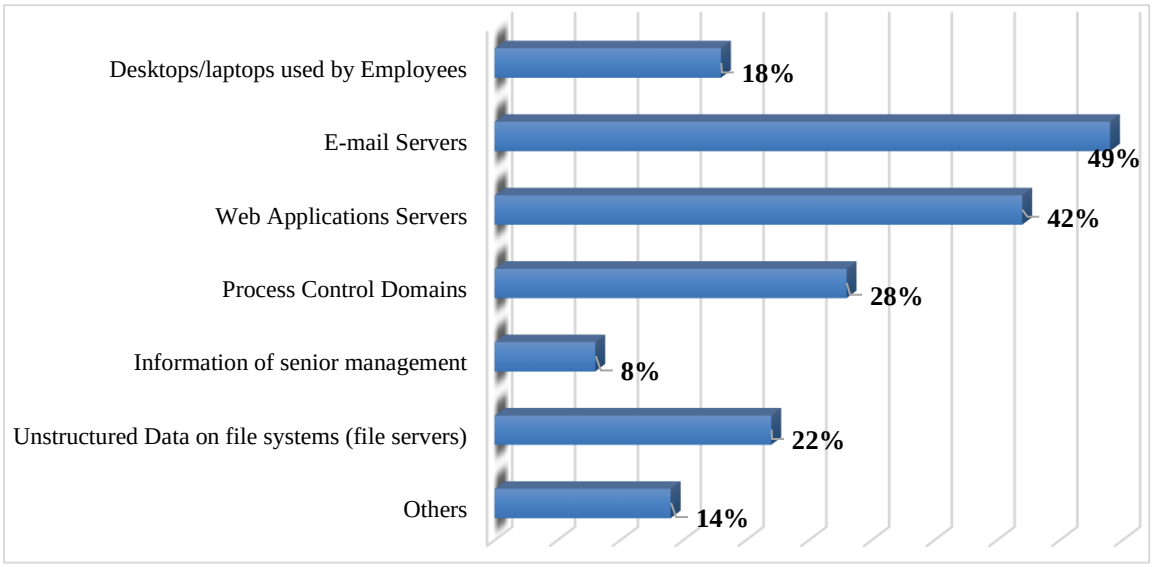
Source: BIBM Survey

In addition to monetary loss banks are also exposed to espionage. 8 percent banks feel that they may have been exposed to corporate espionage/spying and their CXOs (CEO, CTO, COO, CRO, CFO, etc.) devices and data are at risk of cyber-attack. 59 percent of the banks sense that they may be eavesdropped by attackers and 41 percent banks feel that their official emails might be captured and read by someone else who is not a legitimate user.

In recent years, cyber attackers use email-based attacks. Phishing, spywares, malwares and other threats are spread through unsolicited mails and mess up business procedures.

The following bar chart (Figure-8) represents banks main targets of cyber-attack. The study shows that 49 percent respondents believe that email servers are one of the main targets of cyber criminals. Once the cyber criminals hack the email servers, they can commit various malicious activities using that server. The study also reveals that cyber attackers also try to hack the web application server (42%). Other than that, cyber attackers also target process control domain (28%), unstructured data on file systems (22%) etc.

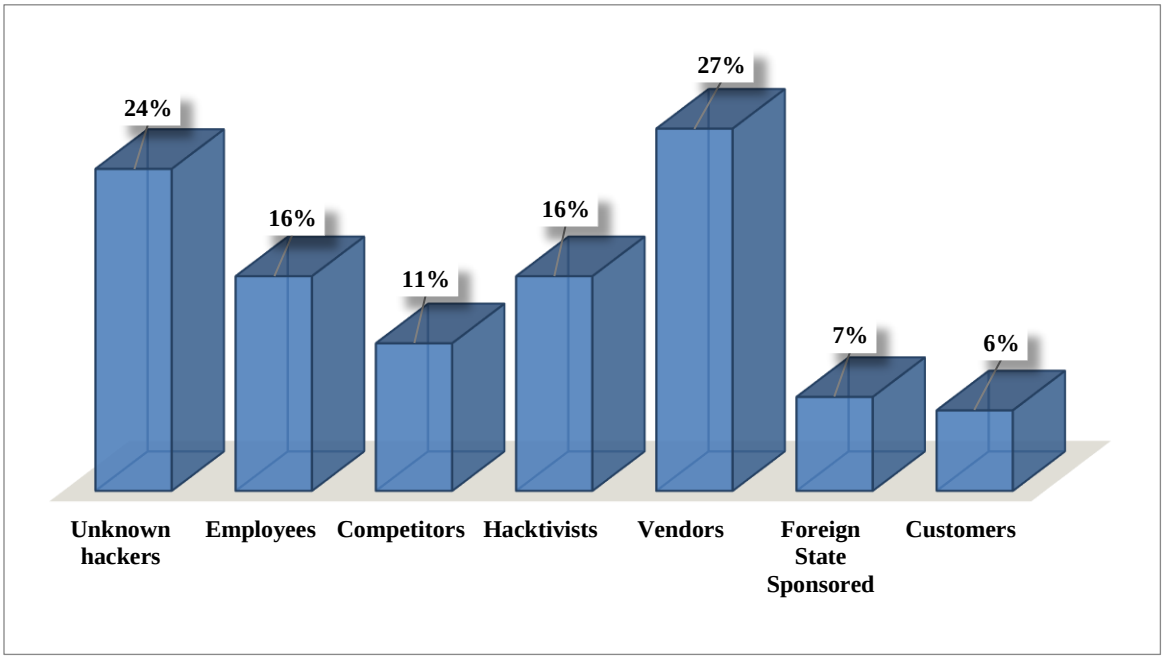
Figure 8: Main Targets of Cyberattacks



Source: BIBM Survey

Figure-9 illustrates the responsible parties and person behind the cybercrime. According to the study, it is seen that vendors (27%) are highly responsible for security breach. Bank employees share their credentials with the vendors. Vendors take those advantages to hack the systems. Moreover, unknown hackers (24%), hactivists (16%), and employees (16%) are also behind the security breach. The alarming issue is that the employees are engaging themselves in such criminal activities.

Figure 9: Who is behind Cybercrime/Security Breach?



Source: BIBM Survey

4.1.2 Response to Cyber Attacks

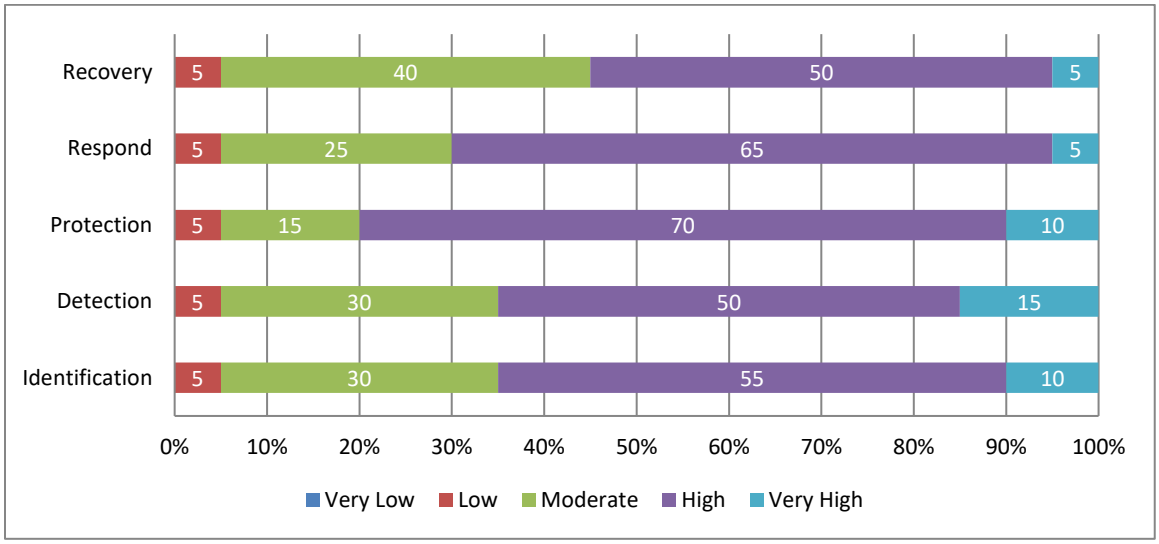
Cyber security status of our banks is depicted in Figure-10.

Identification: It is seen that, only 65% banks have enough expertise (very high 10%, high 55%) and used up to date technology to identify a threat in time. 35% (low-5%, moderate-30%) banks do not have that capability, which is not a good sign at all.

Detection: Cyber incidents are increasing in Bangladeshi banks. However, a little more than 50% of the surveyed banks are able to identify these happenings successfully (5% very high and high 50%). That means, 35% banks are not properly prepared in detecting threats.

Protection: To protect a bank from cyber threat, only 80% banks belong to 'high' and 'very high' group, i.e., they are capable enough. 20% (low-5%, moderate-15%) banks are in vulnerable group.

Figure 10: Cyber Security Status of Banks (% of Banks)

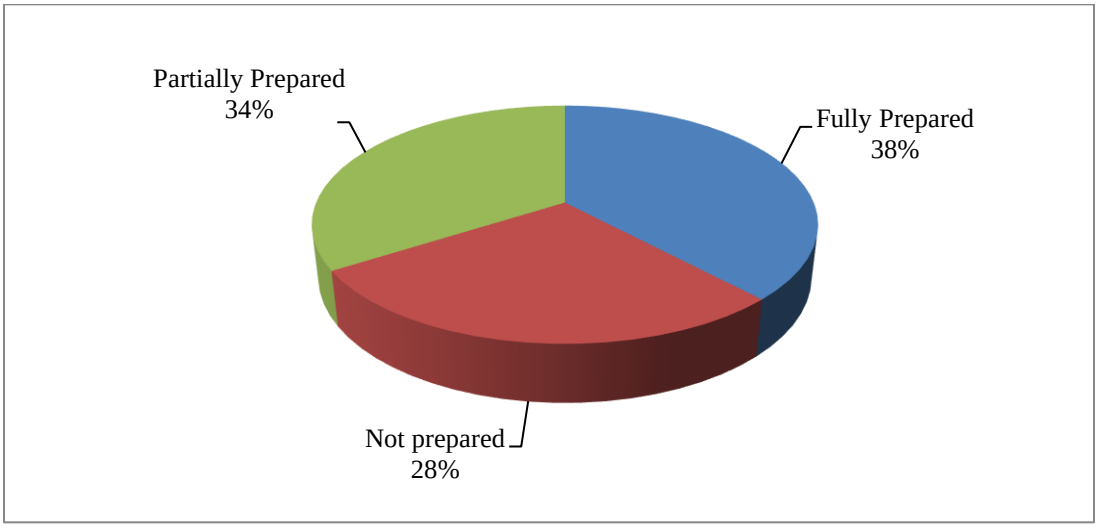


Source: BIBM Survey

Respond: In our banking industry, 70% (very high-5%, high-65%) banks can respond to cyber-attack very quickly and efficiently, which indicates a very decent status. But 35% banks belongs to 'moderate' and 'low' group, which is not expected at all.

Recovery: After any disaster if a bank can recover itself fully in the possible shortest time, then it indicates that the bank is totally prepared to handle such events. But the scenario is somewhat traumatic in our banking industry. Only 55% banks belong to 'very high' and 'high' category. But 45% banks are in 'moderate' and 'low' group, which is totally unsatisfactory.

Figure 11: Readiness to Handle Large-Scale Cyber Attack



Source: BIBM Survey

The pie chart (Figure-11) is designed to visualize the readiness of banks to handle large scale cyber-attack. Only 38 percent banks are fully prepared to handle large scale cyber-attack which is a shocking issue for our banking systems. Whereas 34 percent banks have partial preparedness to handle large scale cyber-attack. The most alarming finding is that 28 percent banks do not have any preparation to face severe cyber-attacks.

While internet has emerged as a risk factor, management of only 23 percent bank are conscious about it which shows improved awareness of the corporate leadership on cyber security. Cyber breach around the world is increased. Bangladesh Bank's reserve heist has reminded us that the cyber risk if not dealt well, can lead to momentous loss. According to the study, 71% banks pay no heed to the cybersecurity risk issues that are identified by audit committees for incident avoidance, detection and reaction.

The survey revealed that 90% banks discuss with vendors immediately after an incident and only 21% of the banks approach specialists to assist them. Banks have confidence that their processes are proficient to handle cybercrime instances but the expertise of staff needs to be upgraded.

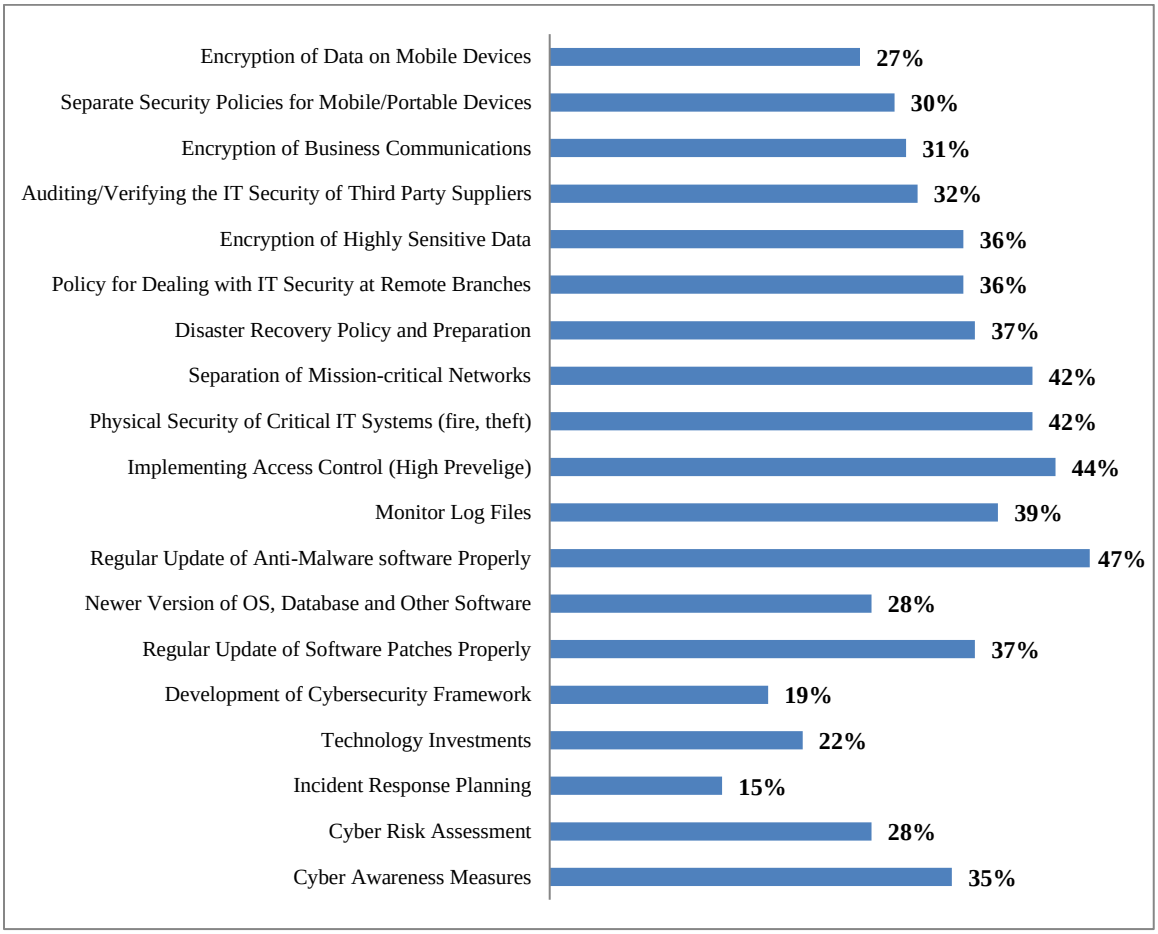
It is need of the time that banks should detect their prime resources that need to be secured in order to cope up with the relentless upsurge of cyber breaches and its devastating impact. Emergency response team is setup by 18 percent banks, while a mere 9 percent banks own internal cyber forensic and investigation team. Comprehensive cyber risk assessment need to be carried out by banks to make sure that vital assets are amply protected to lessen the impact of breaches.

Through rehearsing and practicing cyber crisis can be managed efficiently. Banks should develop teams which need specialized trainings like business continuity, incident management, cybersecurity drills and crisis management workouts. In order to test the efficiency of crisis management plan and improve cyber intelligence, cybersecurity drills must be steered. However, 82% banks responded that their IT security teams do not have adequate experts to deal with cybercrime happenings.

4.1.3 Measures Taken to Protect Cyber Incidents

Timely response is a vital thing of cyber strategy. It aids banks to react effectively to cyberattacks. The study indicates, 82 percent of banks believe that banks' cyber incident response teams and cybersecurity specialists need major expertise and talent development.

Figure 12: Measures Taken to Protect Cyber Incidents



Source: BIBM Survey

To fight against the attacks/threats, several security measures have been taken by banking sector as shown in figure-12. The study discloses that 47 percent banks conduct regular upgradation of anti-malware software, although the percentage is not up to mark. Implementing access control (44%) is another measure which has been taken by banks to protect cyber incidents. Other than that banks also take several steps to protect cyber incidents such as separation of mission critical networks (42%), physical security of critical IT systems (42%), regular update of software patches properly (37%) etc.

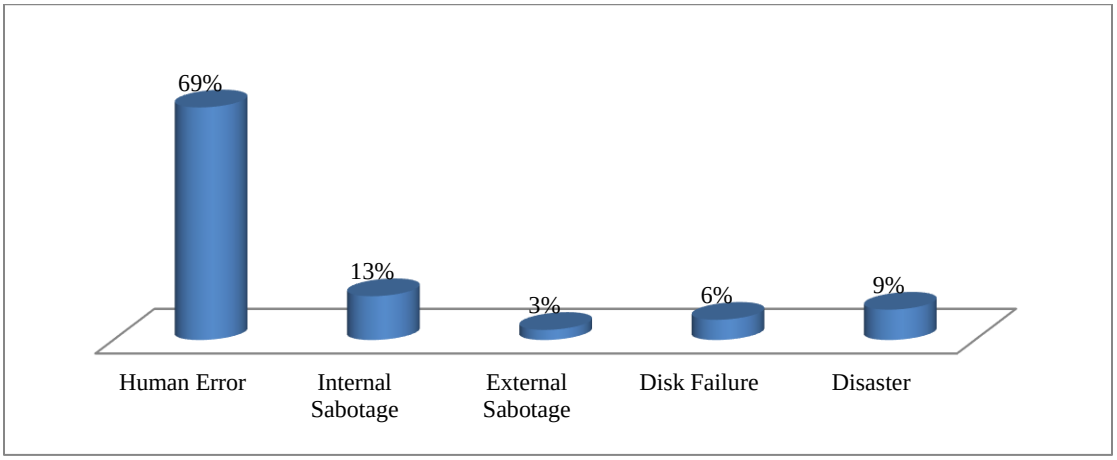
4.2 Threats and Vulnerability of Banking Information System: Internal Threat

4.2.1 Technical Flaws

Last year, 24% of banks faced incident related to the weakness arises from faults in their existing software. Staff also responsible for internal threat to data loss – 13% of banks fall prey to sabotage due to internal staff and 30% of banks fear that intentional data leaks may appear as their most concerning data threat in near future.

Figure-13 depicts the causes of security breach or data loss in banks. According to the study, human error (69%) is mainly responsible for security breach. Sometimes, bank management ignores the man behind the machine. It may bring danger for the bank and financial institutions. Natural or human made disaster may cause security breach or data loss. Proper Disaster Recovery Planning (DRP) can help to prevent such loss. Moreover, in-house and outside sabotage is responsible for 13% and 3% security breaches in the banks respectively.

Figure 13: Causes of Security Breach or Data Loss



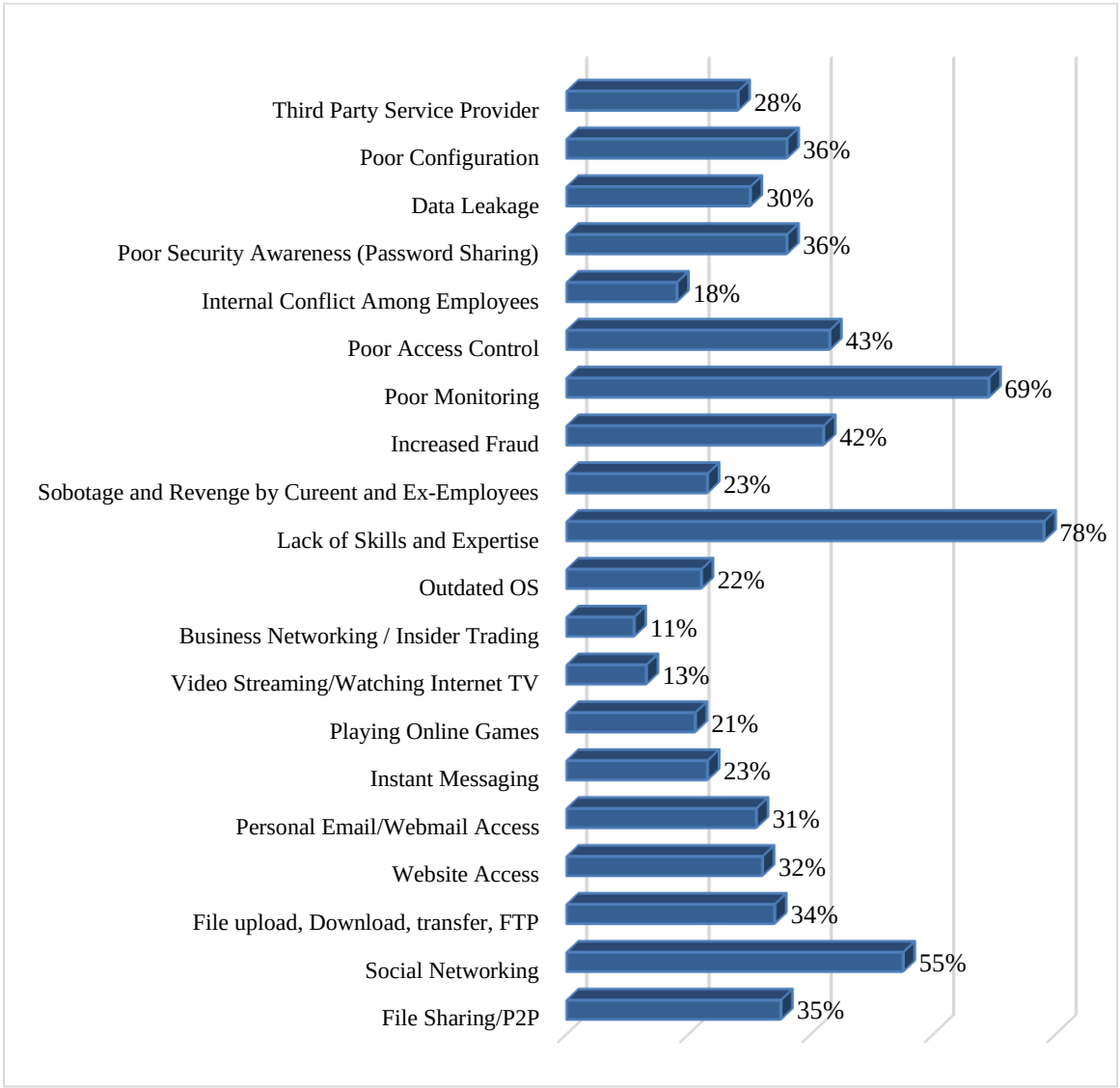
Source: BIBM Survey

Threats from internal workforce do not always originate from malicious intentions. The online tools used by employees both in the office and at home may have a negative consequence on business security. Malware can be spread through social media and file sharing sites in particular can be a source of difficulties for IT security. Social networking sites are now said to be the second major threat to IT security. 55% of banks believe employees who use social media may create a significant danger to the banking environment. If employees share extensive details about their working nature and profile on social networking sites then cybercriminals can use these social platforms to recognize and target key person for a successful breach.

It is no wonder that social networking sites are now banned by more than 50% banks. Further 35% bank limit access in some ways in order to make social media the third most restricted activity in banks. But the study found that this type of restriction does not work well in real life because employees will always discover an alternative way to use these social medias – whether at home or on their private devices. Eventually, creating awareness among employees by educating them is more fruitful to create defense against this threat. Still banks' security team have blocked peer-to-peer file sharing method. 35% of banks believe file sharing activity can pose greatest threat to their security.

The following figure (Figure-14) represents various internal threats which are responsible for security breach or data loss. According to the survey, 78 percent of the respondents believe that lack of skills and expertise is one of the major internal threats. Developing skills and expertise is a major concern among the IT professionals. As IT domain changes very frequently, to cope with the changes training and attending skill development programs is mandatory. Additionally, poor monitoring (69%) is another internal threat which can be mitigated through proper watching and supervision. Other than that social networking (55%), poor access control (43%) are some internal threats faced by our banking systems.

Figure 14: Internal Threats

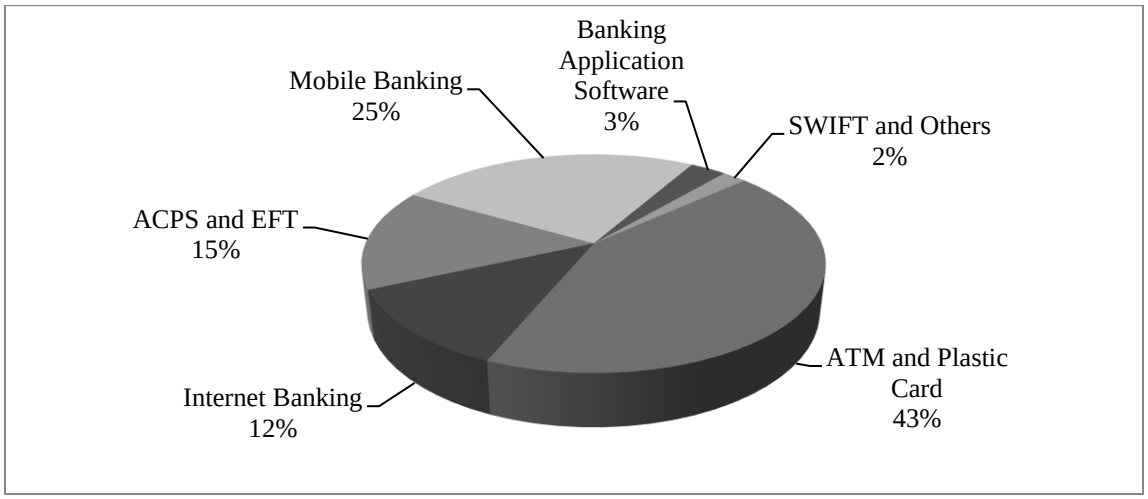


Source: BIBM Survey

4.2.2 Increased Frauds

To observe and analyze the status of frauds through electronic delivery channels committed in Bangladeshi banks, we have taken 50 fraud cases as a sample. The sources of collecting these cases are the Bangladesh Bank, daily newspapers, victims and employees of different banks. According to our analysis (Figure-15), we found that rate of frauds related to Mobile Banking, ATM and Plastic Card transactions are higher than all other fraud areas.

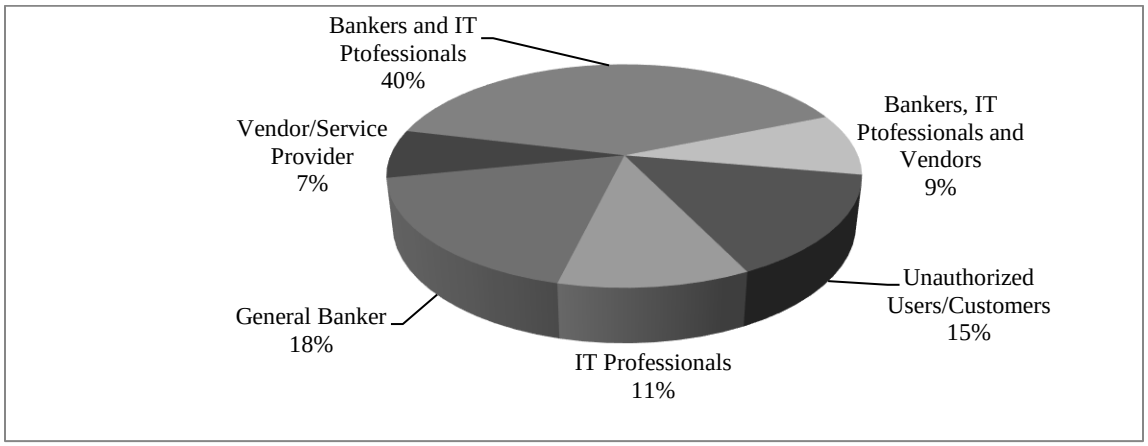
Figure 15: Categories of Frauds



Source: BIBM Survey

The Figure-16 shows that in most of the fraud cases both general bankers and IT professionals are jointly involved in perpetrating financial frauds. A reasonable number of unauthorized external users are also responsible for banking crimes. It is clear that poor security, access control and monitoring help fraudsters to commit fraud.

Figure 16: Category of Fraudsters



Source: BIBM Survey

4.2.2.1 Some Selected Fraud Cases

Some selected fraud cases are given below for understanding the nature and current scenario of online banking frauds.

Case 10: Cyber-Heist: The $951 Million Raid on Bangladesh's Central Bank

"In early 2016, a criminal gang penetrated the security systems of Bangladesh Bank with malware that cloned legitimate transactions. On February 4, the malware sent 35 withdrawal requests through the international SWIFT system to the New York Federal Reserve, where the Bangladeshi central bank had money on deposit. The fraudsters attempted to steal a total of $951m. Thirty of the orders, worth $850m, were blocked by the New York Fed, but the gang succeeded in having $101m transferred to banks in Sri Lanka and the Philippines before their activities were noticed, thanks to a spelling mistake in one of the transfer requests. Subsequently, $20m was recovered from a Sri Lankan bank, but officials were too late to stop the remaining $81m from disappearing. A spokesman for the Federal Reserve of New York said: "The payment instructions in question were fully authenticated by the SWIFT messaging system in accordance with standard authentication protocols." The gang involved is thought to have consisted of between 20 and 40 members with a range of skills and including financial and banking experts, hackers and software engineers. Had it not been for one slip-up, their audacious attempt to steal almost $1bn might have succeeded – a prospect that has caused huge concern among banks and their institutional customers, which keep large sums on deposit to pay staff and suppliers."

Source: *Digital Banking Fraud*, Net Guardian

Case 11: Fraud in ATM by Using Skimming Devices

Detectives arrested four IT experts from different parts of the capital on Tuesday, July 23, 2013 for cheating credit and debit cardholders using fake cards. Several fake debit and credit cards, card readers, writers, magnetic blank chip cards, high-power hidden camera and computers were confiscated from their possession. The ringleader worked as an IT expert for an IT industry while among the rest of the detainees, two worked as IT support staff for ATM booths of different banks and one is from B Data Network. They stole around Tk 2.00 crore in the past two years from different ATM booths using over 180 fake debit and credit cards. The criminals set up cameras above ATM machines to record the clients typing in their passwords, fixed a small device to the ATM card reader to copy the cardholder's information. They then put the information into new debit and credit cards with magnetic blank strips, using devices that can read and write cards. They then withdrew money from the booths or buy products from shopping malls using the cards and passwords.

Source: BIBM Survey

Case 12: Fraud through Phishing (Internet Banking)

Mr. Sajid Hasan (name changed) is a middle aged financially solvent businessman who isn't very tech savvy. Mr. Sajid received an e-mail, which appeared to be from his bank informing him that they are updating their database and they need the customers to go to the bank's website and provide the account information. For the convenience of the customers, they provided a link in the mail. The mail was very convincing as it contained the bank logo and other things like the actual mails of the bank.

Mr. Sajid, being unaware of phishing scam, followed the link and provided his account number and other details in the website. The website as not the original website of the bank of course though it looked like the actual one. Such websites are well known as mirror website. However, as soon as he provided the account details, the fraudsters started transferring funds from his account. Fortunately Mr. Sajid used to check his bank statement online regularly and noticed the unusual withdrawals. He notified the bank instantly to freeze his account realizing that he had become the victim of a phishing scam.

Source: BIBM Survey

Case 13: Clients Being Robbed Through Fake Cash-In SMS

"An organized gang is stealing money by sending fraud cash-in messages (SMS) to bank clients. On September 14, Bank Asia's Uttara branch client Yasin Shikdar, 23, received a cash-in SMS in his bank account for Tk659,000. The client quickly went to the bank with a cheque to collect money. The bank officials checked the account and found that a deposit was posted in the account from the bank's Ishwardi branch, but there was no money in the account. Then the Ishwardi branch was asked to explain the reasons for the delay of this transaction. In response, the manager of Ishwardi branch said someone claiming to be the bank's head of IT department phoned him and said there was a problem in the bank's server. Later the manager was asked to deposit an amount to an account to test whether the server was working properly or not. So the manager gave a posting of Tk659,000 in Uttara branch's client Yasin's account. As a result, he rushed to the bank to cash out the deposit. After talking to Ishwardi branch, Uttara branch officials told him that there was no transaction in his account. Then a serious quarrel took place between bank officials and Yasin inside the bank. On November 6, Bank Asia Vice-President and Operation Manager AKM Mohsin Uddin filed a case against the client in Uttara (East) police station. The bank officials reported that Yasin Shikdar wanted to collect money by cheating, and he had threatened to kill the officials. But the bank authorities did not say anything about how the SMS was sent using the bank's own server. They claimed that the Ishwardi branch manager resigned after the incident."

https://www.dhakatribune.com/bangladesh/crime/2018/01/06/bank-fraud-fake-cash-sms
Published at 10:16 pm January 6th, 2018

Case 14: Hotel Owner Arrested in Dhaka over POS Terminal Fraud of Tk 32 Million

"A hotel owner has been arrested in Dhaka for allegedly stealing Tk 32.2 million using a City Bank Point of Sale (POS) terminal. The Detective Branch of Police arrested Abdul Hasnat, owner of Uttara's Comfort Inn residential hotel. According to the case details, Abdul Hasnat applied for a POS machine for his hotel on Jan 12, 2015. City Bank delivered it to Comfort Inn on Mar 9. Hasnat made 140 transactions to withdraw a little over Tk 32 million using the terminal between Jun 8 and Jul 31. The bank found those transactions to be fraudulent after some debit cardholders had filed complaints. In keeping with policy, City Bank returned the money to the defrauded account holders."

https://bdnews24.com/bangladesh/2016/04/05/hotel-owner-arrested-in-dhaka-over-pos-terminal-fraud-of-tk-32-million
Published: 2016-04-05 20:45:32.0 BdST

Case 15: Tk 2 Million Stolen Thru Card Forgery

"At least 49 clients of five private commercial banks have lost around Tk 2 million when a criminal gang withdrew the money from booths by using cloned debit and credit cards recently. Victims and bank officials said the frauds collected information for cloning the cards when the clients went to purchase in an outlet of a super shop in Banani area in the capital. The victims are clients of private BRAC Bank, The City Bank, United Commercial Bank (UCB), Eastern Bank and Bank Asia. Both credit and debit card were cloned for withdrwaral of money from ATM (automated teller machine) booths. The banks concerned confirmed the matter after receiving complaints from the clients. Bank officials apprehend that the number of victims might be higher.

Bank officials said three clients -- Ishrat Jahan, Sajia Chowdhury and Aporupa Chowdhury -- bought some goods from Shwapno's Banani 11 and Kamal Ataturk Avenue outlets on 22 February. Later on 10 March, an amount of Tk 50,000 was withdrawn from a booth of AB Bank in Kalshi, Mirpur. When she received SMS from the bank to her cell phone about the withdrawal, she informed the bank authorities of this.

In the same way, another Tk 600,000 was withdrawn from BRAC Bank's nine clients. BRAC bank authorities came to know about these following complaints from clients.

The frauds withdrew Tk 400,000 from the accounts of 11 clients of Eastern Bank, Tk 150,000 from the accounts of four clients of Bank Asia and Tk. 600,000 from the accounts of 22 clients of City Bank.

Authorities of the five banks later closed their ATM services of the clients concerned."

https://en.prothomalo.com/bangladesh/news/172860/Tk-2m-stolen-thru-card-forgery
Update: 13:31, Mar 21, 2018

Case 16: Mobile Banking Fraud in Bangladesh: 11 Including 5 Grameenphone Employees Arrested

"Rafiqul Islam, owner of mobile banking outlet Rawa Enterprise at Fakirapool, had complained that on Jan 31 someone had withdrawn Tk 24,500 and Tk 5,000 in two fake transactions using his mobile number. That night, when one person turned at the shop and asked for a cashout of Tk 1,000, the agent showed the number to be deactivated.

Rafiqul informed Dutch-Bangla Bank Limited and bKash about these fraudulent transactions and later came to know that someone had cloned his SIM card and was using it for cash withdrawal from his account. CID official told the media conference that following the enquiry in Rafiqul's complaint, 11 persons were arrested from different areas including Dhaka, Madaripur and Faridpur. He said that the five employees of Grameenphone working in its customer care cell were arrested after meticulous investigations proved their involvement in passing on mobile banking details to the fraudsters. "This gang used the Grameenphone staff to clone the SIM of agents and customers to siphon off money from customer accounts." "We took time to zero in on the gang and used different tactics to acquire the agent passwords used by them," Shah Alam said."

https://bdnews24.com/bangladesh/2016/04/19/mobile-banking-fraud-in-bangladesh-11-including-5-grameenphone-employees-arrested
Published: 2016-04-19

Case 17: 'More Money Stolen at Point-Of-Sale'

"Foreign fraudsters in collaboration with local bankers and merchants are believed to have committed more card frauds on point-of-sale (POS) terminals than what they had done with ATMs, experts and investigators said.

The issue came to the front after police arrested the City Bank's three officials who had been working with the bank's POS terminals at different merchants. "If the bank officials concerned get involved with merchants, it is very easy to do card frauds at POS terminals," said Mashrur Arefin, additional managing director of the City Bank.

Arefin was surprised to see that his bank's three junior officers, who were the supervisors of the bank's POS acquiring team, collaborated with an international gang of card frauds.

Fraudsters make counterfeit cards with data skimmed off cards used at the merchants. According to industry insiders, most of the cards that get counterfeited are foreign. The fraudsters then use the cloned cards to buy goods and services.

Bankers said as a side income, merchants also swipe cards and then provide cash to the cardholders instead of any goods or services. In this case, fraudsters make duplicate cards with skimmed off data and then go to the collusive merchants to get cash and share the sum with bankers and merchants. Generally, foreigners use their cards to buy goods and services. Fraudsters steal data of these cards in collaboration with the merchants from where foreigners

had bought their goods or services. The ATM frauds that took place between February 6 and February 12 shocked people as it was first of its kind in Bangladesh. So far, the investigations found that fraudsters took away over Tk 25 lakh using around 40 cards. The gang used data skimmed off cards at four ATMs in the capital and the central bank investigation detected that the gang had stolen data of over 1,200 cards.

But investigators found Thomas (aka Piotr) and his accomplices committed far more frauds at POS terminals and at ATMs. Kazi Saifuddin Munir, managing director of IT Consultants that run Q-Cash, the largest private payment switch in Bangladesh claimed that he had received a lot of complaints from VISA, a global payment technology company, about foreign card frauds but the banks did not pay heed to these complaints."

https://www.thedailystar.net/frontpage/more-stolen-point-sale-660367
Published: February 25, 2016

4.2.3 High Availability (DC, DRS, ADC and DRP)

We found that 96% banks have centralized database operations through data center. Except foreign banks, data center of all banks are setup in Dhaka. Among the DCs, 54% are set up in high-rise buildings. Moreover, 28% banks have set up additional data center (ADC) and 14% of the ADCs have been set-up in high-rise buildings.

We also found that 88% disaster recovery sites have been set up in Dhaka, 4% in Jessore and 8% in other places. It is also seen that 18% of DRS are set up in high-rise buildings. The lowest, highest and average distances between data center and disaster recovery site are 5, 30 and 12.5 kilometers, respectively. Moreover 34% banks were planning to replace their DRS far away from data center, at least 100 kilometers away in a separate seismic zone.

Regular and periodic testing of a DRS is an important and crucial issue for a centralized online bank. This type of testing increases confidence and expertise of recovering data and business operation in case of any disaster. Research findings reveals that 72% banks tested live operation from DRS in 2017. Among them, most of the banks tested the live operation in holidays – Friday or Saturday (after 4 p.m.). That means they are afraid of testing in working hours. It is also seen that only 30% banks tested whole CBS operations and rest of the banks tested one or two modules/applications (e.g., ATM, I-banking etc.) from DRS.

About 45% of the banks are afraid of testing the disaster recovery site by shutting down the data center any time. This finding indicates the poor quality and readiness of the technology including proper management of data center and disaster recovery site. Up to December, 2017, no bank has achieved any certificate from international organization for

their DC and DR operations. It is seen that only 38% banks have Certified Data Centre Design Professional (CDCDP) for effective maintenance of DC and DRS which was 18% in 2015 and 35% in 2016.

In case of any disaster, disaster recovery plan plays an important role. In 2017, about 61% banks have approved guidelines of BCP/DRP. Among the banks, all are following the BB ICT Security Guidelines and 45% follow ISO standard in addition. But during data validation it appears that most of the banks did not follow standard guidelines and methodology to develop the BCP. Only 28% banks have separate BCP and DRP department. Minimum, maximum and average number of employees are working in these departments are 3, 13 and 7, respectively in 2017.

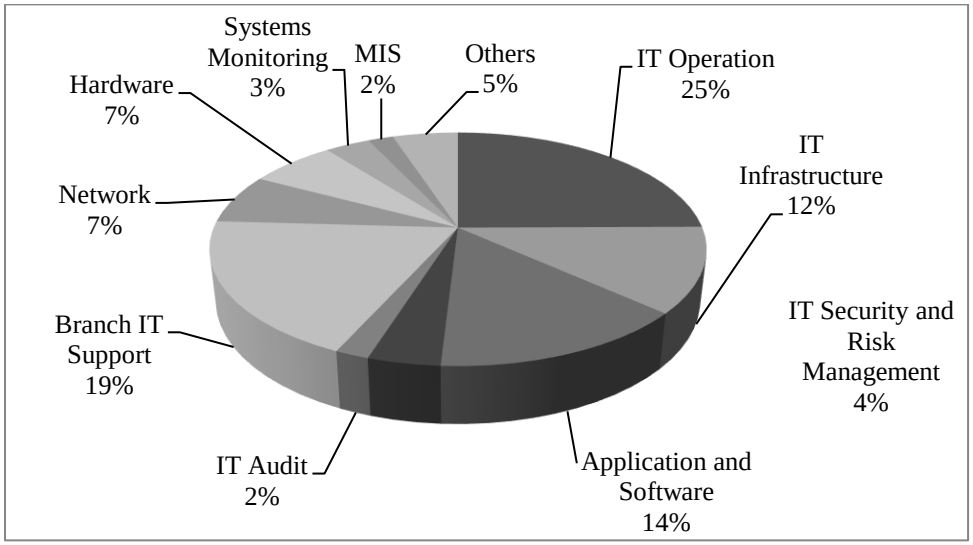
4.2.4 Human Resource in ICT Departments

4.2.4.1 Size of the IT Department

Currently, a total of 3430 employees are working in the IT departments of all banks in Bangladesh. A common complaint of IT Heads is that, the number of workforce employed in IT department is not satisfactory and they face tremendous work stress. It is found that average, minimum and maximum number of employees of IT department are 56, 3 and 367 respectively in 2017.

It is seen from Figure-17 that highest number of IT employees (25%) are working for IT operations followed by branch support (19%), application and software monitoring (14%) and IT Infrastructure support (12%). Only 4% employees are working for IT security and Risk Management.

Figure 17: Distribution of IT Employees in 2017 (% of Total IT employees)



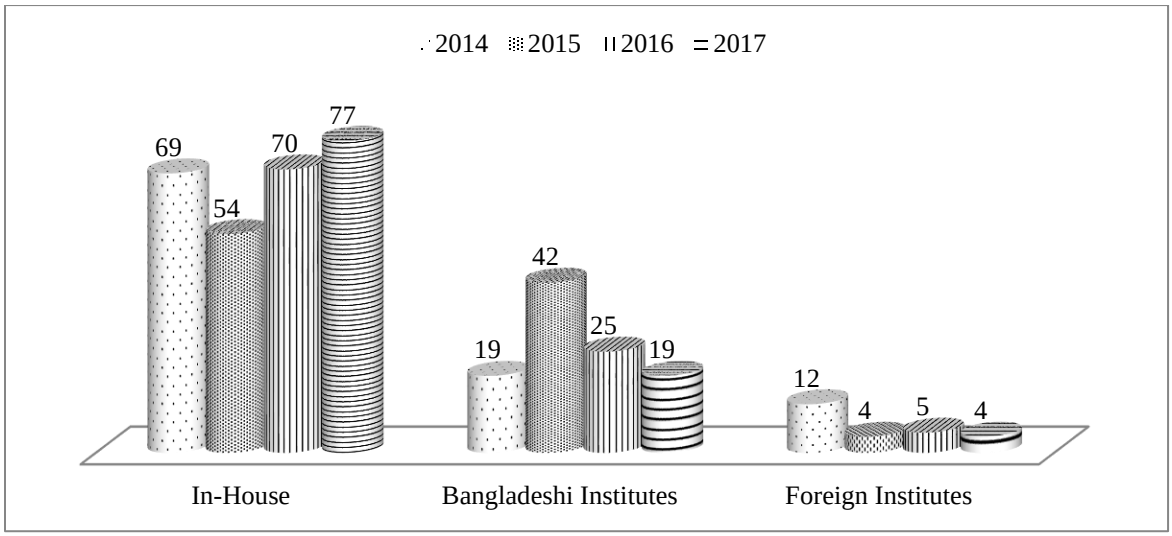
Source: BIBM Survey

4.2.4.2 Training

It's important to stay updated when working in IT. The ability to keep up with the competition in regards to IT, training is vital to a bank's survival. The goal of IT training is to empower a bank to effectively manage information storage, retrieval and flow. Each year, more advanced technology systems are developed. Computers, software and networks have to be updated to not fall behind the competition. The technology department must constantly be aware of these changes. Also, security may be hampered due to the lack of latest technological knowledge. It is the duty of the bank to upgrade their employees regularly by providing training in home and abroad. But this is much more ignored by the most of the banks. Near about 3% of total IT budget goes to training purpose.

However, within this limited budget, banks tried to send their employees for better training as much as possible. In 2017, a total of 2573 employees received training from home and abroad. Banks are providing in-house training facilities. 77% of total trainee received in-house training in 2017. Training in different institutes of Bangladesh and abroad is decreasing. Figure-18 represents the scenario on training in different training institutes.

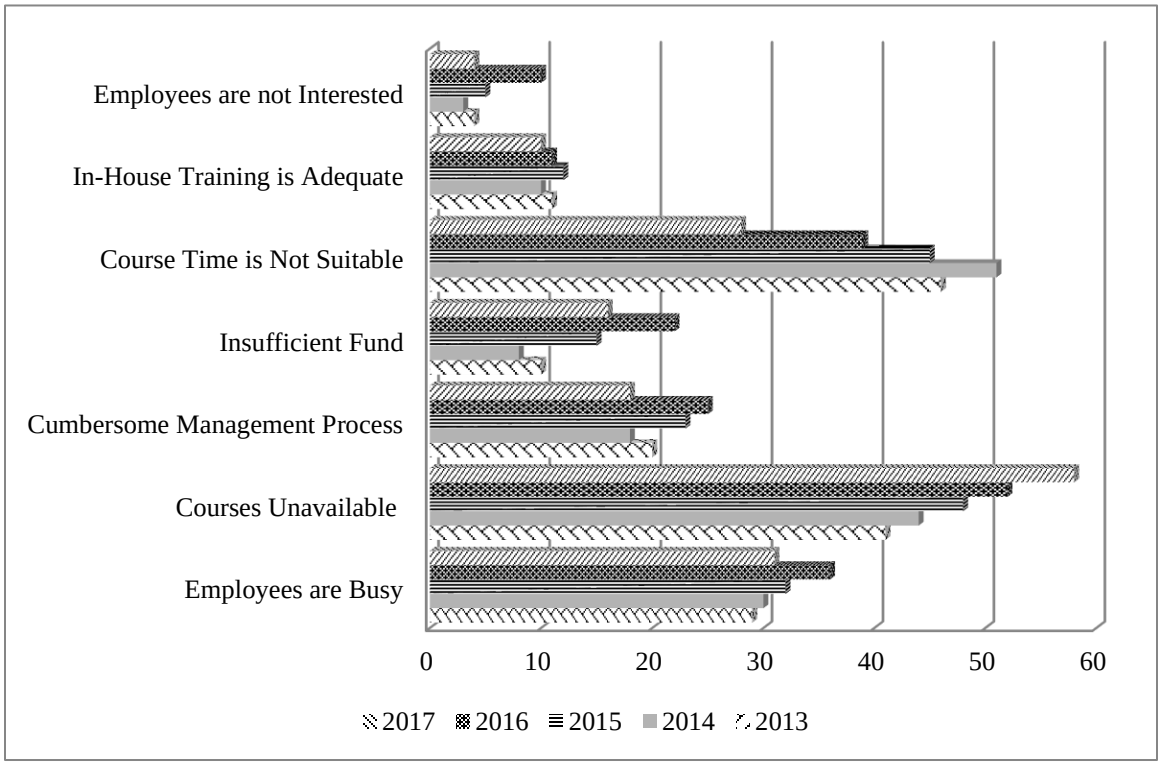
Figure 18: Type of Institutes from Which Training was Received (% of Participants)



Source: BIBM Survey

Though the budget allocation for training was very low in 2017, bypassing this limitation sometimes it was not also possible to send the employees to receive training due to shortage of sufficient time, unavailability of the course and insufficient employees as shown in Figure-19.

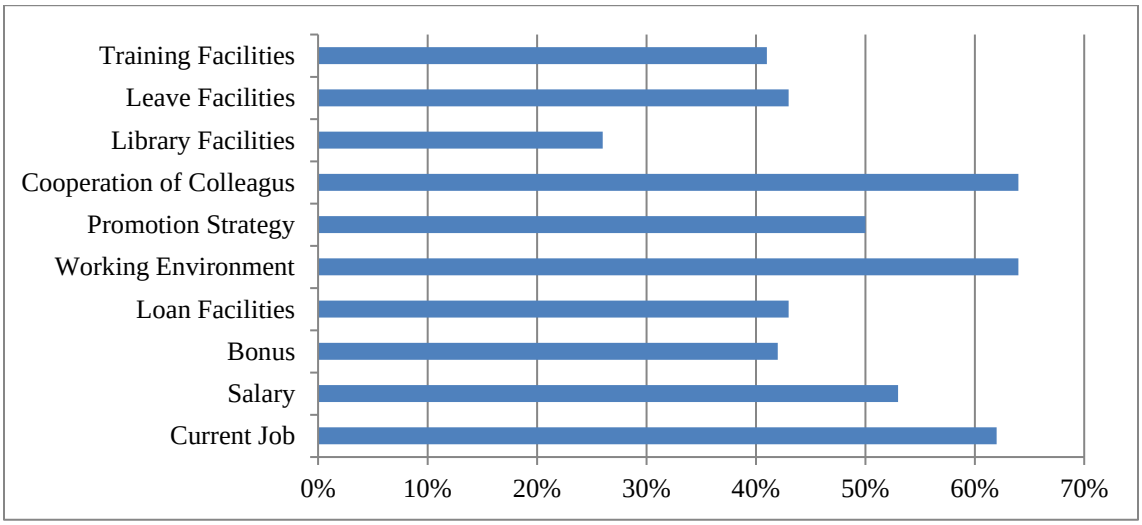
Figure 19: Factors Affect Providing Training



Source: BIBM Survey

4.2.4.3 Job Satisfaction

Figure 20: Job Satisfaction of IT Employees



Source: BIBM Survey

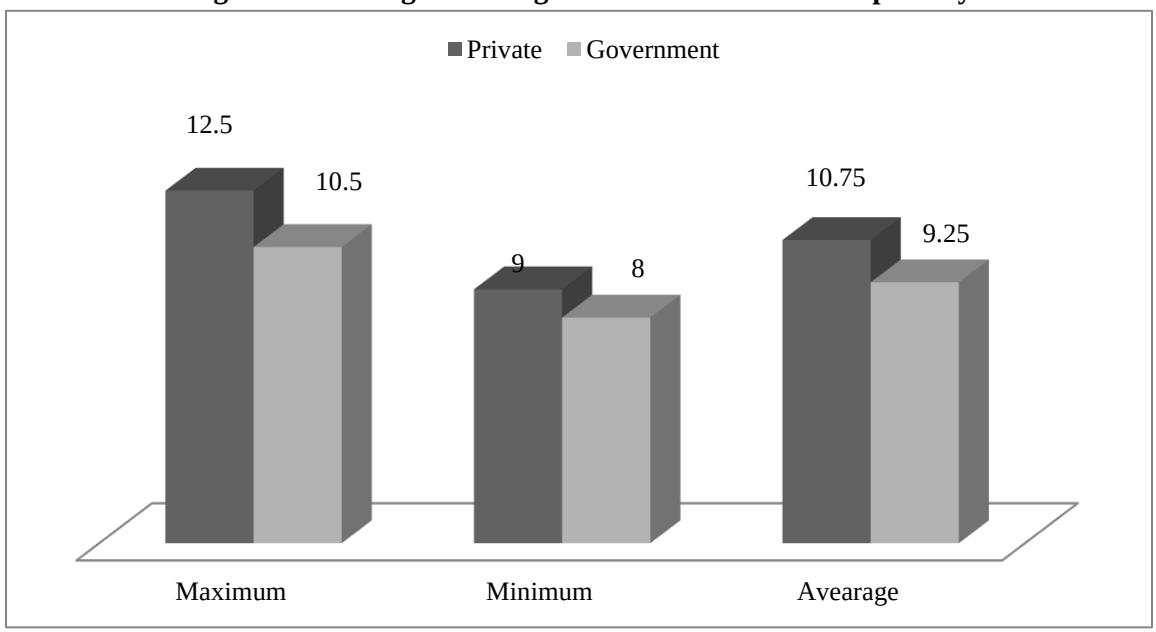
Are the people who are navigating the electronic banks, by spending their lives, happy about their job facilities and benefits that are given to? Figure-20 shows the details. Leave facilities are not very easily enjoyable for an IT professional compared to other departments of banks, according to 42% professionals.

4.2.4.4 Work Load

As 59% IT Heads reported that time is not available for the employees to receive training, it indicates that they are under tremendous pressure in the industry. This is also supported by the findings drawn in Figure-21. This graph shows that on an average a professional of private bank has to stay near about 10.75 hours per day to complete his/her duty. For govt. bank it is 9.25. Moreover, employees of private banks works for minimum 9 to maximum 12.5 hours per day, whereas it is 8 to 10.5 hours for a govt. bank's employee.

In case of IT leaders, 68% of them have been suffering from excessive work load. Consequently, 34% of them added that they have been suffering from hypertension, influencing heart disesase, and diabetes also.

Figure 21: Average Working Hour of IT Professionals per Day

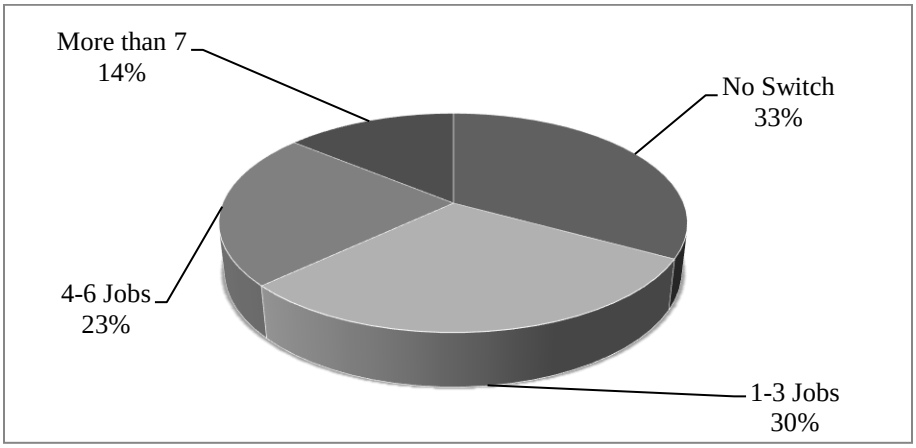


Source: BIBM Survey

4.2.4.5 Job Switching

If employees are not satisfied with their job in all aspects, unrest may prevail on the banking sector hampering IT operations and security. Current switching rate of IT professionals are shown in the graph below. It is seen that 30% IT professionals changed their jobs 1 to 3 times whereas it is 4 to 6 times for 23% professionals. Moreover, 14%, mainly the top level professionals/Heads of IT, have experiences of changing their jobs more than 7 times in the carrier path.

Figure 22: Job Switching of IT Professionals



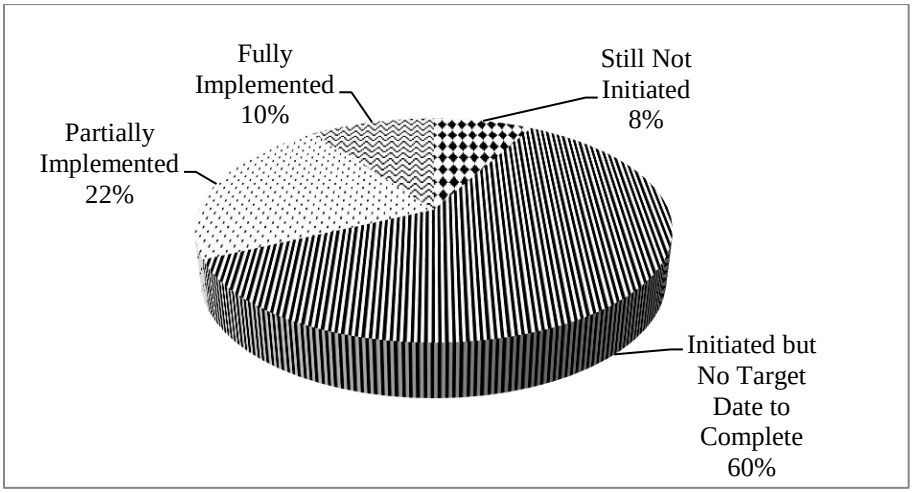
Source: BIBM Survey

4.2.5 IT Governance (ITG)

4.2.5.1 Status of ITG Implementation

According to our survey, only 32% banks have ITG framework, indicates severe weakness of management's active involvement in IT operations in banks. Figure-23 shows that 8% banks still not initiated the activities to implement ITG and 60% banks though initiated are not confident enough about the completion of the activities within the targeted date. Banks should give proper attention to follow appropriate guidelines, standards and framework (such as COBIT, ISO/IEC *38500:*2008) to successfully implement ITG to attain business goals.

Figure 23: Status of ITG Implementation

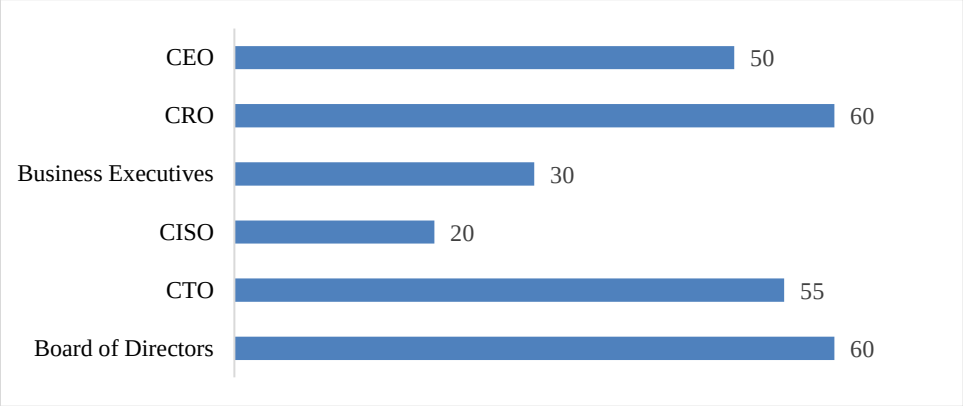


Source: BIBM Survey

4.2.5.2 Executives Involved in IT Governance

From the research findings it appears that there is a lack of understanding of IT Governance activities and responsibilities in banks. As per international standard and best practices, Board of Directors is responsible for the IT Governance in an organization. But only in 60% banks, Board of Directors are involved in IT Governance. Moreover, in case of 55% banks, CTOs are also involved in IT Governance (Figure-24). Participation of other executives in IT Governance is shown in the following figure.

Figure 24: Executives Involved in IT Governance

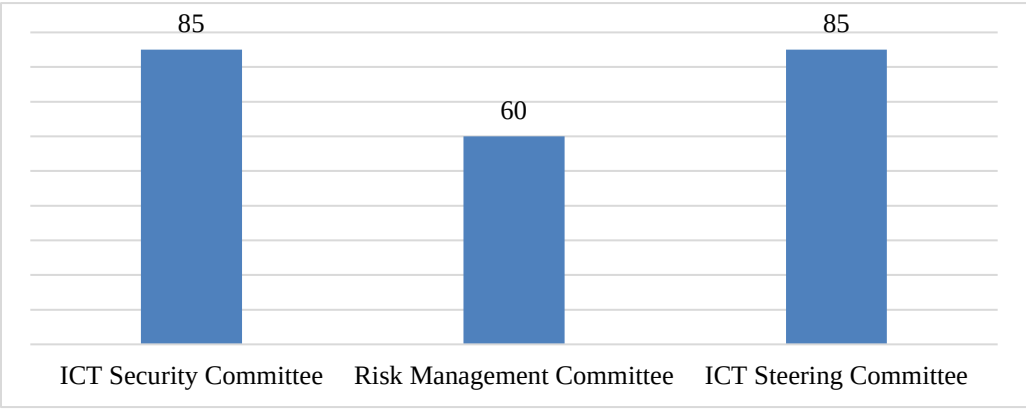


Source: BIBM Survey

4.2.5.3 Formation of IT Committees related to IT Governance in Banks

From Figure-25, it is seen that 85% of banks have both IT Security Committee and IT Steering Committee and 60% banks have ICT Risk Management Committee. But with a view to establish better IT governance practices in all banks, it is required to set up these committees as early as possible to take the full benefits of today's tech-based banking and competitive advantages.

Figure 25: Formation of IT Committees in Banks

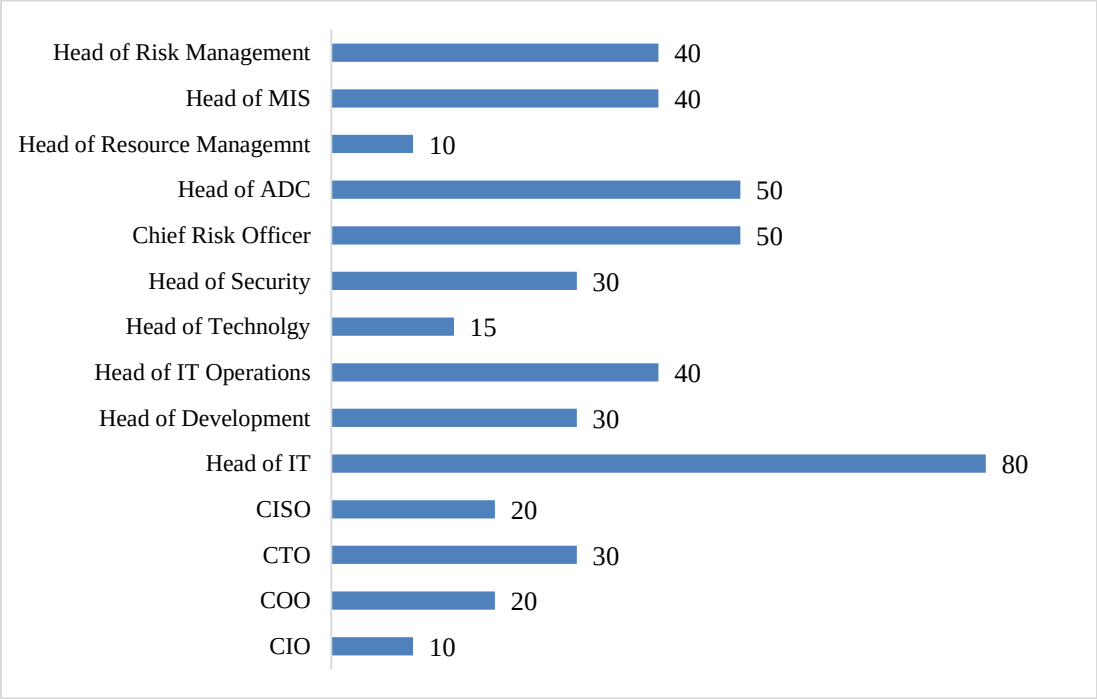


Source: BIBM Survey

4.2.5.4 Effective Organization Structure for IT and Key IT Role Players in Banks

IT Organization Structure is an important element of IT Governance Framework. Proper IT Organization Structure in banks can play a vital role to ensure efficient and cost-effective use of IT resources for achieving business goals and benefits. It is also observed that 30% of banks do not have proper IT Organization Structure to support effective IT governance practices. In accordance with the best practices of IT governance, banks should recruit key IT role players to ensure efficient management of IT services and good governance. From Figure-26, we do not observe very strong initiatives to employ Key IT Role Players in banks. Only 10% banks have CIO and 20% banks have CISO.

Figure 26: Key IT Role Players in Banks



Source: BIBM Survey

4.2.5.5 IT Policies/Guidelines/Frameworks

With a view to implement ITG, banks are following different standards or guidelines which are shown in the following table. From Table-3, we observe that all banks are following BB ICT Security Guidelines, 45% and 6% banks have started to follow ISO 27001 and ITIL, respectively. Only 8% banks are following COBIT to implement ITG. Moreover, one bank implemented ISO 27001 and PCIDSS is implemented by two banks. Though all banks follow Bangladesh Bank ICT Security Guidelines, it is seen that 85% of banks implemented about 75% of the requirements according to the guidelines whereas 15% banks implemented only 50% requirements.

Table 3: Use of IT Security Policies/Guidelines/Frameworks

IT Security Guidelines or Standards	% of Banks Follow
Bangladesh Bank ICT Security Guidelines	100
ISACA	20
ISO 2700X	45
COBIT	8
PCI DSS	35
NIST	15
ITIL	6

Source: BIBM Survey

4.2.6 IT Audit

Conducting proper IT Audit is an acute problem in the banking sector. Near about 84% banks have dedicated IT auditors. Number of IT auditors ranges from 1 to 8. On an average, 3.5 IT auditors are dedicatedly employed in those banks. As 16% banks have no IT Audit team, they totally depend on external auditors or wait for BB Audit team. It is also seen that only 55% IT auditors are internationally certified. Among them 40% and 15% are CISA and ISO certified, respectively. Moreover, all banks are visited by BB inspection and audit team once in a year. It is also found that, 12% banks audit their system quarterly, whereas 88% banks conduct it yearly.

4.2.7 IT Risk Management

Around 47% banks have established a separate IT Risk Management department in 2017. Minimum, maximum and average numbers of employees working in these departments are 2, 15 and 7, respectively. Only 38% banks have certified information security professionals. In banks, number of such professionals ranges from 3 to 10. On an average, 8.5 security professionals are dedicatedly employed in those banks. Among them CISSP (49%), CCNSP (17%), CEH (17%) and RSA (17%) professionals are available in those banks. Approximately, 73% banks have a dedicated security management unit that handles all sorts of security management issues.

4.2.8 Penetration Testing (PT) to Assess Vulnerabilities

In modern banking arena, the exercise of testing computer system, network or web application to detect weaknesses through which an attacker could abuse the system is known as penetration test. These types of tests are done industry-wide. In our country 75% of banks are undertaking such testing. About 62% banks conduct penetration tests yearly, 9% quarterly and 4% on monthly basis. Although penetration testing is a vital component through which a bank can defend cyber breach, but it is seen that such assessments deliver only a snapshot of a bank's susceptibilities. Also, it can become

invalid as soon as a new threat occurs. So, it is apparent that ongoing systems monitoring is a must to identify weaknesses and possible exposures.

Penetration tests should be carried out from both internal and external sources, which will bring the best result for a bank. More than half of all banks conduct penetration tests in this way. Although external threats always make headlines, but insider breaches from workers, experts, and others can also do the same or in some cases more harm to a bank.

More than 85% banks those carry out PT depend on third-party vendors and almost 28% banks have completed PT with their own experts supported by consultants.

4.2.9 Monitoring Log Files (Logs)

IT security is the prime concern of the banks. Regular monitoring and auditing of the access log and the commands being given by the admin users to various applications, databases and devices may reduce the security risks. A central ACS monitored and audited by the separate security management team of the IT division is an excellent way to get control over the whole IT system. However, survey shows that only 48% of the banks have such control system. Rest of the banks should have such system to reduce the IT risk arising from the attempt to unauthorized access or executing undesirable commands.

The following table shows the status of accessing logs of critical devices in 2017.

Table 4: Status of Checking the Access Log of Sensitive Devices/ Servers

Access to Device/ Software	% of Banks
Access to Core Router	83
Access to Core Switch	83
Access to IDS/IPS	75
Access to CBS	41
Access to Switching Software	41
Access to Database	41

Source: BIBM Survey

Regular monitoring of the access log of the most critical devices or systems should be a mandatory task of the IT security department of every bank. The survey data shows that the monitoring is not satisfactory. However, in order to properly implement this monitoring, bank should engage some dedicated officers in the IT security department. Bank may include this issue in the IT security policy and auditors should take special care about this issue for proper implementation of it. About 60% of the banks those implemented ACS do not prepare any report to see the list of unauthorized access and preserve it. About 84% banks informed that they have Access Control Policy but only 75% banks reviewed their policy each year. Banks should have sound monitoring system

for accessing log of above critical devices but only 53% banks maintain this monitoring system. The following table indicates different types of monitoring system used by the respective banks.

Table 5: Monitoring Systems Used by Banks

Name of Monitoring System	% of Banks
Security Information and Event Management (SIEM)	40
NMS log monitoring System	10
System Center Operation Manager	15
Check Point Smart Event Management	5
Oracle Log Analytics	12
RSA envision	5
Solarwinds Network Performance Monitor	15
Nagios	5

Source: BIBM Survey

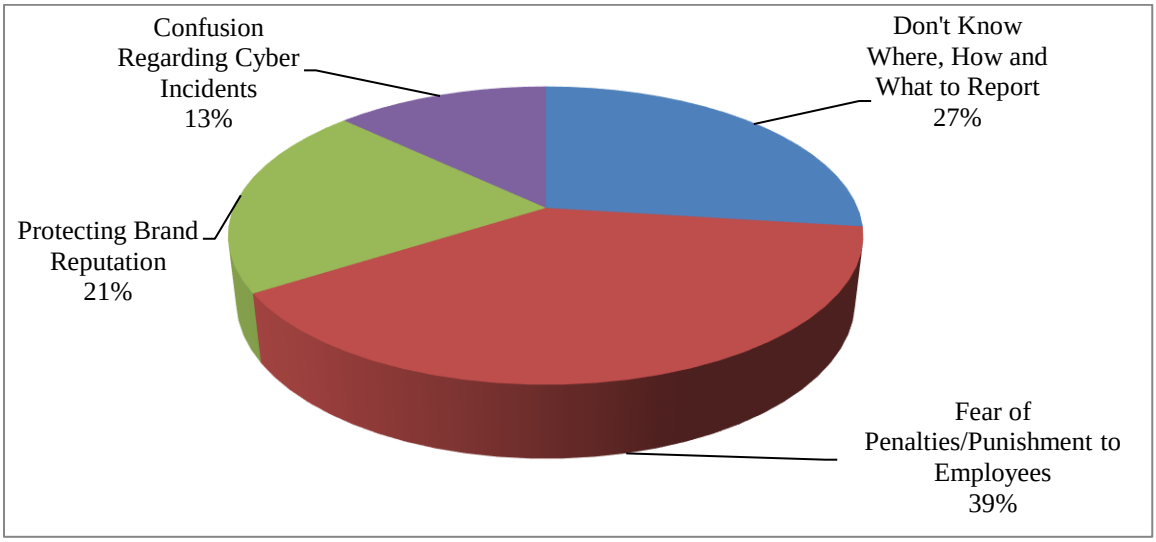
4.2.10 Data Leakage Prevention (DLP)

In order to discover probable data breach/data exfiltration and protect data from any types of malicious activity, Data Leakage Prevention is used in banks. Through mischievous intent or unintentional error confidential data is revealed to unauthorized personnel in data leakage incidents. Such sensitive data may include private or business information, intellectual property (IP), economic data, credit-card data, and other information depending on the business environment. DLP is a plan that protects end users to send sensitive or critical information outside the company network. It is very much alarming that, 78% banks do not have DLP solution. To protect sensitive data, banks should introduce Data Leakage Prevention solution as soon as possible.

4.2.11 Reporting

In many cases, employees tend to hide cyber incidents from management. According to the employees of 27 percent banks, lack of responsiveness is the main reason behind this attitude. Again, professionals of 39 percent banks fear that they will be punished if the cyber incidents are known by their management. And 21 percent banks think that reporting of cyber breaches will create a negative impact on their reputation.

Figure 27: Reasons for Not Reporting Cyber Incidents



Source: BIBM Survey

29 percent banks do not feel the urge to report the cyberattack incident to LEAs (Law Enforcement Agencies) as they think it is not a serious issue. In almost all instances, banks those experienced a cyber-security incident did not notify law enforcement and/or the regulator. Cyber is such a concept that is unlikely bound by geographic restrictions and this causes the crime to be borderless. In case of a trans-border cyberattack, 71 percent banks are perplexed to detect to whom they will go and report the crime. 66 percent of the banks are aware about the legal impact of cybersecurity incidents. However, 34 percent said that they are not familiar with the technics that should be put in place to address such legal hazards. Again, a mere 3 percent banks have reported cyber-incident to LEA after becoming victimized.

Now banks are strengthening their resistances against cyberattacks. But at the same time implementation of cyber laws and regulations are very essential to handle cyber risk. 73 percent banks feel that LEAs are not adequately prepared to tackle problems related to cyber-crime.

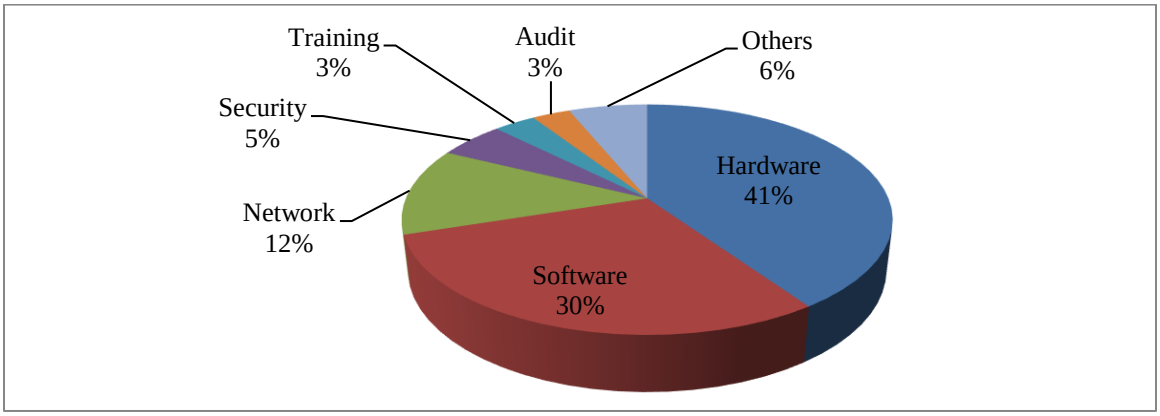
4.2.12 Cyber Insurance

In case a cybersecurity incident happens, a bank can shift its liability to that company which gives Cyber Insurance service. It is not like that a cyber-insurance can secure an organization against cybercrime; but it can reimburse for losses due to cybersecurity incidents. The study shows that the concept of 'cyber insurance' is not well understood till now in our country and it is still at a budding phase.

4.2.13 IT Budget

In 2017, approximately, Tk. 2035 crore was invested for IT System in the banking sector (Figure-28).

Figure 28: Distribution of IT Budget



Source: BIBM Survey

We found that a major portion of the IT budget was used to procure hardware. Second highest budget is spent for software purchase. It is also found that budget allocation for security, training and audit was very poor. About 81% of the banks demanded at least 10% of the total IT budget to ensure cyber security and mitigate technological risks.

4.2.14 Managing Service Provider and Outsourcing Risk

A risk management module that is created by third party can help a bank to identify, access and mitigate risks. But this can also produce some threat if not monitored properly. Time to time onsite assessment should take place for the outsourced activities to detect risks that can arise due to outsourcing.

Signing SLA (Service Level Agreement) with vendors for support and services are very important aspect of maintaining proper service-oriented relationship. Inclusion of clauses in SLA regarding right to inspect/audit vendor's institute ensures the accountability of vendors for providing reliable supports to banks.

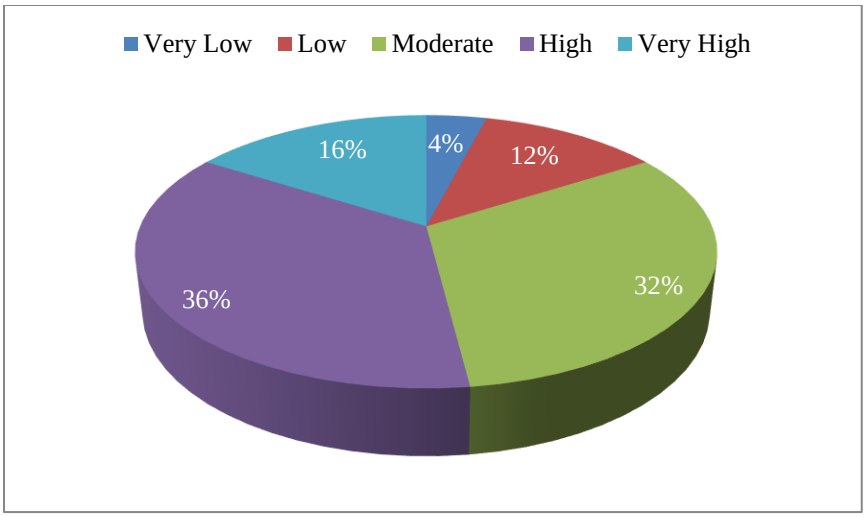
78 percent of the banks feel that before outsourcing or taking any support from service providers, cyber security risk assessment should be addressed first. It is found that 52% banks put audit clauses in SLA and 48% banks don't do it. All banks should add this clause in the SLA for banks' own safety as well as for regulatory compliance. Among the banks those put audit clauses in SLAs, very few (13%) of them audit third-party vendor's institute and their activities as per the signed SLA and 87% banks did not visit vendors at all according to the SLA. Now-a-days, a lot of services are outsourced by the banks. To

mitigate outsourcing risk, banks should conduct audit to see the strengths and weaknesses of their vendors as per signed SLA.

4.3 Risk Perceived by the Banks

BIBM survey tried to find out the perceived degree of risk from the responding banks. Some 16% banks mentioned that current situation of information security is not enough to prevent any virtual or physical damage of information management system, perceiving the highest risk. Around 36% of the surveyed banks believe that they are in high risk of information loss at any moment. 32% banks reported that they are under moderate risks, whereas 12% and 4% banks feel that their risk is low and very low, respectively, as shown in the following figure.

Figure 29: Information Security Risk of Banks



Source: BIBM Survey

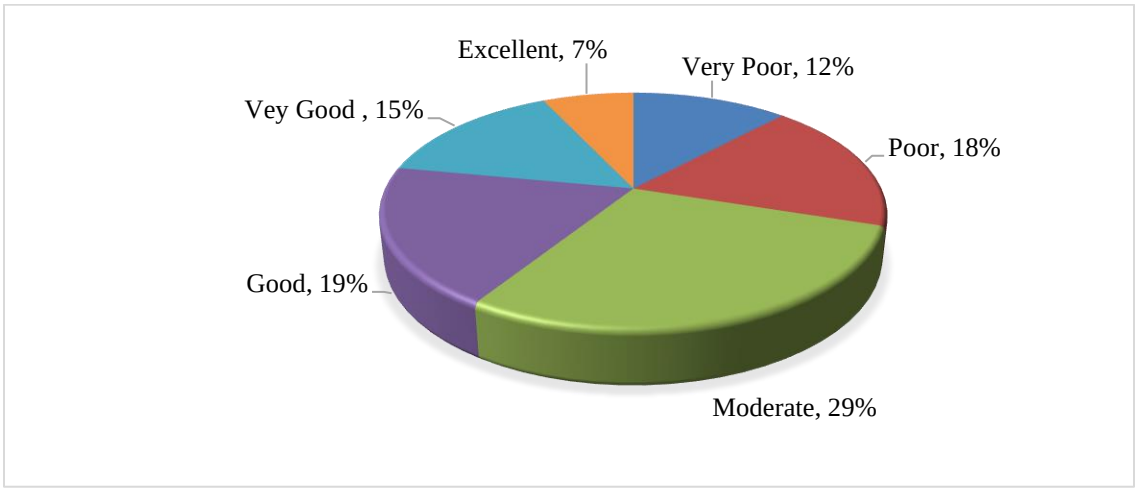
4.3.1 Why are Cyber Risks perceived?

Financial businesses and corresponding technology are varying quickly, in accordance with this IT risks are also increasing. The study indicates that 60 percent banks believe that the implementation of emerging and innovative technology (FinTech) is exposing banks to newer cyber risks. Presently network security is considered as one of the top strategic concerns for banks, while errors in existing software is considered as top internal threat. Future threats must be considered and addressed by senior managers in coming days. An alarming finding is that, only 21% banks consider cyber threats as one of the top three risks to the business. This reflects a very low awareness of security among top level executives in banking sector of Bangladesh.

4.4 IT Security Awareness of Employees' and Customers'

We developed a questionnaire on IT security containing 100 marks to measure the security awareness of both employees' and customers' (Grading System: 0-20 = Very Poor, 21-40 = Poor, 41-60 = Moderate, 61-70 = Good, 71-80 = Very Good, 81- 100 = Excellent). It is expected that bank employee should have basic knowledge about IT security and they should score above 60.

Figure 30: IT Security Awareness of Employees'

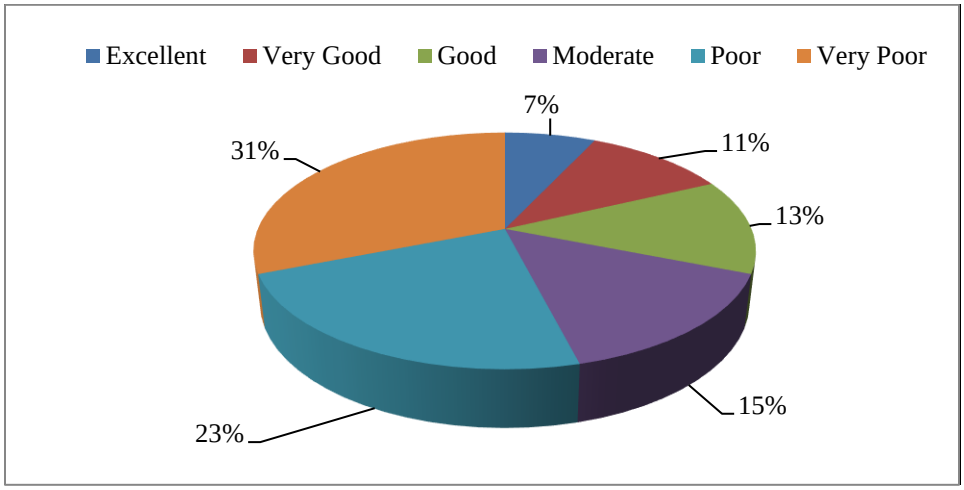


Source: BIBM Survey

We collected data from 450 employees of banks covering the whole country. We can see from Figure-30 that, 59% employees scored below 60 (Very Poor 12%, Poor 18% and Moderate 29%), i.e. they have not enough understanding about IT security. Only 41% (Excellent 7%, Very Good 15%, Good 19%) employees scored above 60. This finding indicates that banks have to take a lot of effort to create security awareness among their employees.

Same process is followed to measure the IT security awareness of customers'. Figure-31 shows the status of IT security awareness of customers' in our banking sector. Data is collected from 750 customers covering the whole country. As seen from the graph, only 31% customers (Excellent 7%, Very Good 11% and Good 13%) have very clear idea about IT security and threats. Most of the bank customers (69%) scored below 60 which indicates a poor IT security awareness among them.

Figure 31: IT Security Awareness of Customers'



Source: BIBM Survey

4.5 Gap Analysis

In this section 'Security Gaps' were assessed purely on the basis of each standard comparing with a reference score '100', which was considered to be the maximum and that any organization should like to achieve for excelling. A gap of close to 30 and more was considered to be highly critical area for the improvement of the performance dimensions. A gap of between less than 30 and more than 20 was considered as critical and further needs for improvement and gap below 20 is treated as less significant.

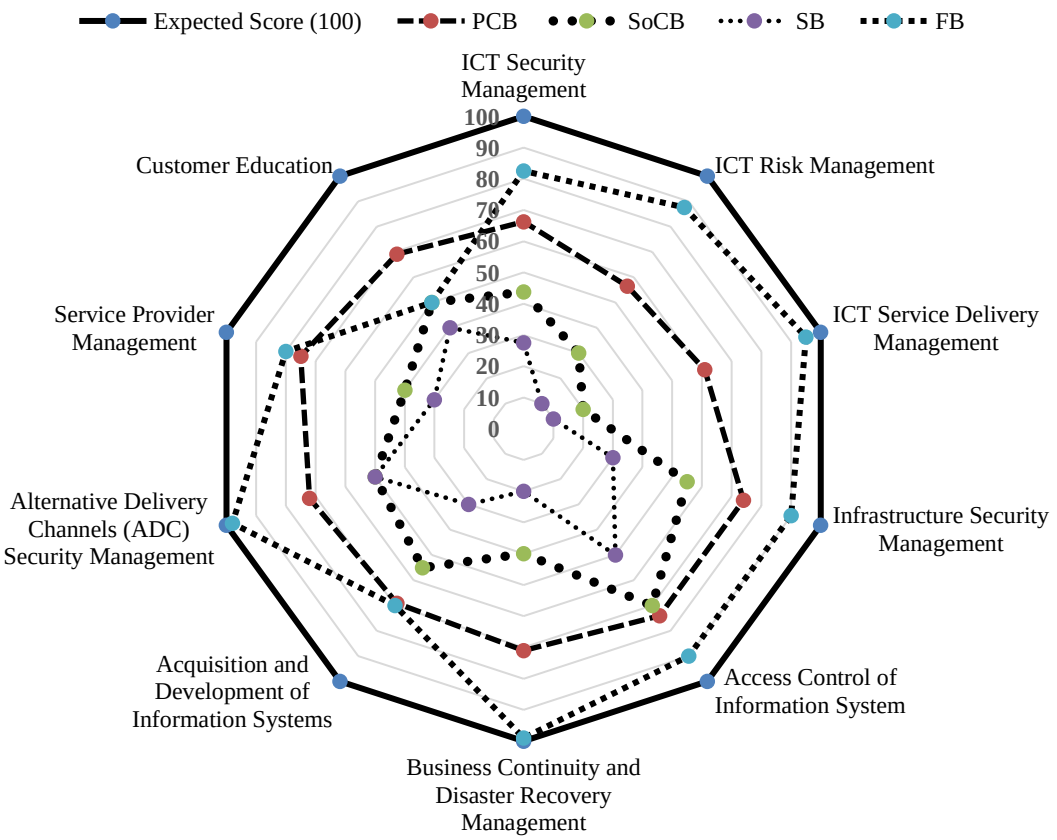
4.5.1 Gap Analysis under BB ICT Security Guidelines

Following figure shows the gap between the current situation and highest expectation (100) under BB ICT Security Guidelines. This will help the management to reduce the gap between the real scenario and expectation.

ICT Security Management: ICT security management ensures that the functions and operations related to ICT are efficiently and effectively handled. In case of this standard, FCBs scores the highest (82.5), followed by PCBs (66). SBs are far behind in meeting the standard.

ICT Risk Management: It covers Risk governance, Risk assessment and Risk response which are vital for the existence of any organization. But the overall situation of our banking industry is not satisfactory in this regard. Here also, FCBs holds the leading position by achieving 87.5 marks. It is clear that PCBs (56) and SOCBs (30) are very weak in this particular field.

Figure 32: Security Gap Analysis under BB Guideline



Source: BIBM Survey

ICT Service Delivery Management: The objective of this standard is to set controls to achieve the highest level of ICT service quality by minimum operational risk. In this standard, FCBs is much more matured than other categories of banks in Bangladesh. FCBs (95) bypassing PCBs (61) with a clear difference in achieving this standard. The other two categories of banks are far behind to meet the expected score.

Infrastructure Security Management: Secured infrastructure shall be implemented to protect sensitive or confidential information which are stored and processed in systems. In case of this standard, PCBs ranked 2nd by scoring 74. SOCBs and SBs are not in a good position in this standard.

Access Control of Information System: Access control of information system plays a very important role in overall IT security. PCBs and SOCBs are almost in the same level by scoring 74 and 70 respectively.

Business Continuity and Disaster Recovery: Business Continuity and Disaster Recovery is a key aspect of any financial organization. But the condition of our banks in meeting this standard is not so satisfactory except FCBs. FCBs (99) almost touches the expected score. It is evident from the data that, SBs (20) should give utmost priority in this regard.

Acquisition and Development of Information Systems: To implement any new business function, banks require rigorous analysis to confirm that business necessities are met in an effective and well-organized manner. Though the score of FCBs (70) and PCBs (69) are somewhat satisfactory in this standard but the condition of SBs (30) and SOCBs (55) is quite unacceptable. Especially SBs should give more emphasis to attain a minimum score.

Alternative Delivery Channels (ADC) Security Management: ADC ensures higher customer satisfaction at lower operational expenses and transaction costs. In case of ADC security management, FCB (98) is clearly in a remarkable position, followed by PCBs (72). The score of SOCBs and SBs are same.

Service Provider Management: Now a days in our country, banks are increasingly reliant on third party service providers as partners to achieve the development targets. It is also an effective cost alternative. But it is clear from the graph that no bank in our country is pleased with the service of vendor/third party. The score of FCBs (80) and PCBs (75) is almost same in this case.

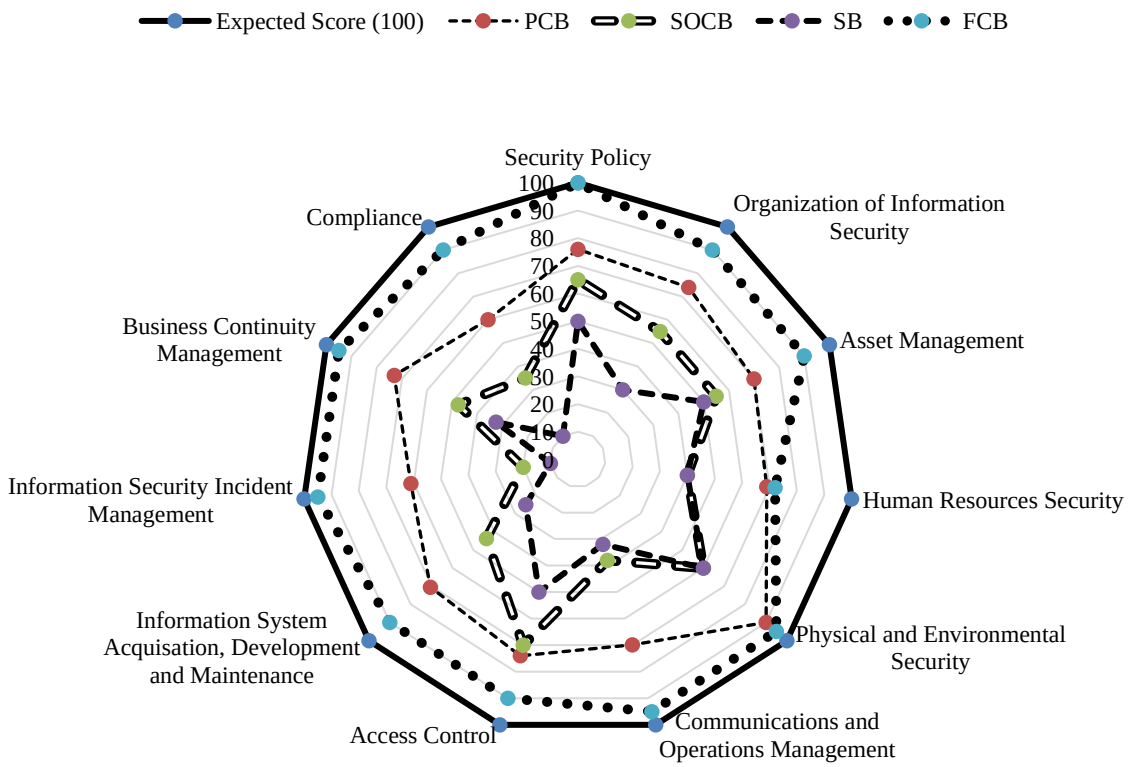
Customer Education: It is often said that awareness of customers is the best resistance against frauds. But the real scenario is quite opposite in our country. It is obvious from the data that this particular field is very much neglected by our overall banking sector. PCBs (69) score the highest and SBs (40) scores the lowest in meeting this standard.

4.5.2 Gap Analysis Considering ISO Standards

FCBs: As seen from the graph, out of 11 standards of ISO Guideline, FCBs outshines in 10 standards. In these 10 standards, the score made by FCBs is between 90 and 100. The only standard that is somehow overlooked by FCBs is ‘Human Resources Security’. FCBs scores 72 in this field, which indicates that FCBs should give more attention to their workforce to attain high mark.

PCB: Overall condition of PCBs is satisfactory in these 11 ISO standards. Though this category of bank scores between 60 and 90, it is clear from the graph that PCBs gives attention in meeting most of the standards. But two major standards (Information Security Incident Management and Compliance), that are vital for the sustainability for any organization especially for a financial institution are somewhat ignored.

Figure 33: Security Gap Analysis Considering ISO Standards



Source: BIBM Survey

SOCBs: Performance of SOCBs is not up to the mark. Their score ranges between 20 and 70. Three fields that require special attention are: Information Security Incident Management (20), Compliance (35) and Human Resources Security (40). If they cannot improve the overall condition in these 3 standards, then it will be a threat for their longevity.

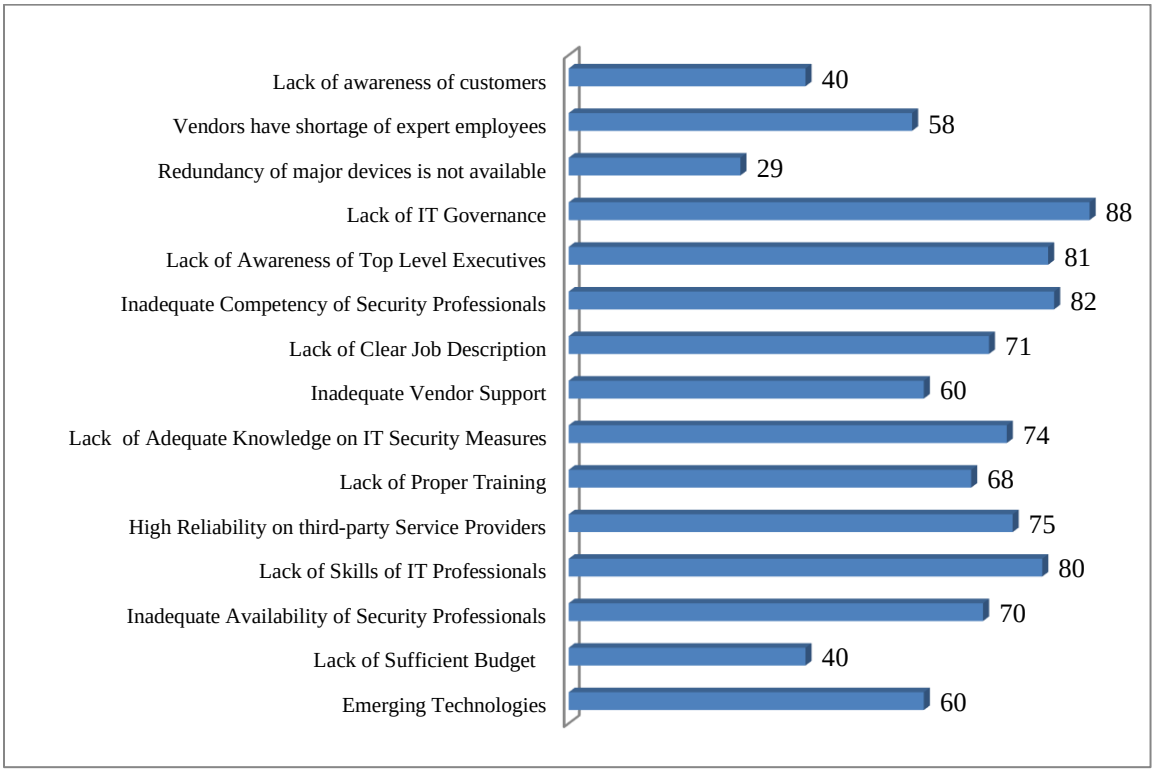
SBs: Condition of SBs is not pleasing at all. They are far behind to reach a minimum level. They score between 10 and 60 in these eleven standards, which is not an acceptable mark. They are very weak in Information Security Incident Management (10) and Compliance (10). In other 8 standards also, they are not in a good position. SBs should give utmost attention to create an overall satisfactory condition.

5.1 Challenges to Implement IT Security

5.1.1 Views of IT Heads of Different Banks

IT department have been facing different challenges or obstacles to manage IT system in banks efficiently. The opinions of HOITs of sampled banks are shown in the following graph (Figure-34). Most banks have pointed out that external factors pose the greatest challenge for constructing a satisfactory cyber security program. According to IT heads, the main obstacles they have faced to safeguarding information security were the lack of IT governance (88%), lack of awareness of top-level executives (81%), inadequate security professionals (70%), absence of segregation of duties (71%), lack of skills of IT employees (80%) and shortage of knowledge regarding emerging technologies (60%). Although reported less commonly, lack of hardware, inadequate vendor support and lack of sufficient budget were also mentioned as hindrances in some instances.

Figure 34: Views of IT Heads of Different Banks



Source: BIBM Survey

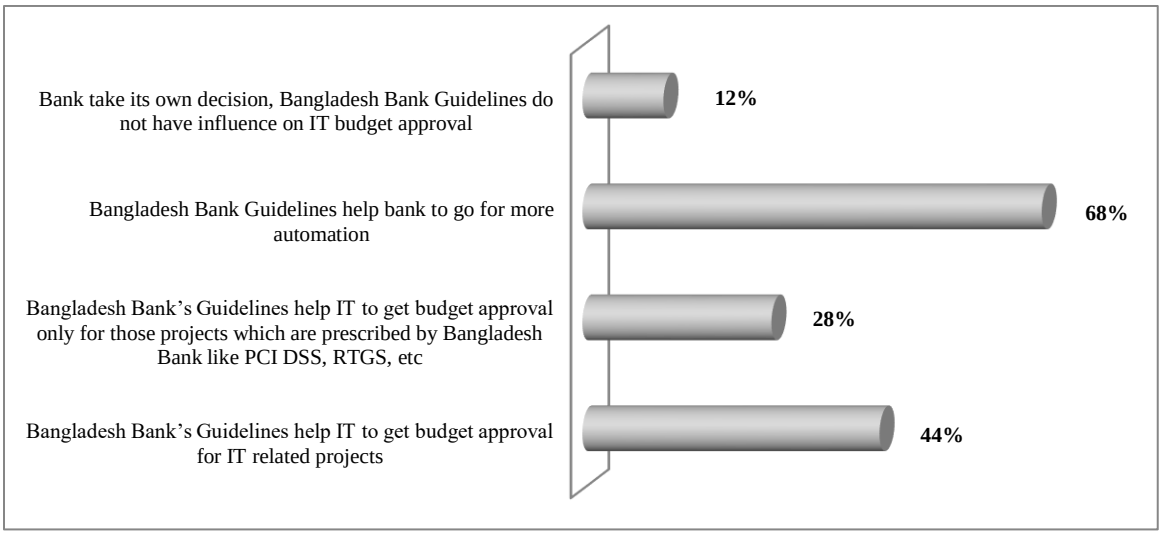
A wide-ranging IT security framework should be embraced by banks because adoption of emerging technology at a fast speed is leading to a dynamic risk profile. According to the views of IT Heads of different banks, we are trying to find out the factors that create a barrier to construct an effective information security in our banks. As the advances in technology is happening, on the other side sophisticated attacks on system is also increasing. And

sometimes it is very difficult to suspect a possible attack if security professionals do not have proper/enough expertise. ITG framework is essential for the sustainability of banks' IT. But 88% Heads of IT think that proper ITG structure is not build up yet in our banking sector. If top level management is not aware about the importance of IT in banks, then it is very difficult for IT division to achieve their goals. 81% Heads of IT face this problem. High reliability on third-party service providers sometimes poses a great risk to banks. If the service providers are not readily available in time of a disaster then a bank may fall in great catastrophe. 58% banks face this challenging situation.

5.1.2 Role of Bangladesh Bank

Bangladesh Bank is playing a vigorous role in the automation of banking sector. As per Figure-35, 68% of the respondents indicate that Bangladesh Bank guidelines help banks to go for more automation, 12% indicate that banks took its own initiative for the IT automation. In addition to that, 44% respondents say that Bangladesh Bank's guidelines help IT to get budget approval for the automation and 28% respondents say that Bangladesh Bank's Guidelines help IT to get budget approval only for those projects which are emphasized by Bangladesh Bank like PCI DSS, RTGS, etc.

Figure 35: Guidance of Central Bank to Develop IT Competency in Banks



Source: BIBM Survey

Bangladesh Bank can take more proactive approach to bring all the banks at the same level of IT automation, manage IT related risks and implementation of IT Governance through IT Governance Framework standardization and guidelines.

As a regulatory body, Bangladesh Bank (BB) has been playing prominent role to uphold smooth and secured e-banking operations. Besides, due to rapid growing of state-of-the-art e-banking products and services, banking community expects more contributions from

BB. Opinions and expectations of banks regarding the role of BB are summarized and presented in the following table (Table-6).

Table 6: Possible Roles of Central Bank (% of Banks)

Sl. No.	Expectations of Banks from the Central Bank	% of Banks
1	Bangladesh Bank (BB) may form a committee headed by a GM of Bangladesh Bank taking members from the scheduled banks. The committee may conduct a meeting once a year and formulate a guideline for ICT development for the bank. BB may circulate this guideline for compliance.	82
2	BB may review its ICT guideline in each year by the mentioned committee.	74
3	BB may form a team of ICT inspection for the banks and each team may inspect and monitor certain number of banks and the banks will always communicate with its team for compliance instead of communicating once in a year.	63
4	BB inspection team should be trained for its purpose and should include only expert having adequate academic and professional qualification.	63
5	BB may provide necessary assistance to BIBM to equip with more ICT related manpower and resources so that the role of BIBM is more pragmatic.	62
6	Each year BB may conduct a day long ICT conference under the leadership of the Governor where all the MDs and IT Heads of banks and the CEOs of Vendors will participate. In each year a particular subject like ICT security, IT based new products etc. may be focused. Three banks and three vendors may be rewarded based on their contribution in the ICT development of the banks.	81
7	Banks have severe weakness in regular DRS testing. BB may increase the frequency of effective audit and inspection to ensure instant activation/running of DRS operation at the time of any disaster.	53
8	Banks should have immediate plan to set up DRS at separate seismic zone and BB may take proper initiatives to provide infrastructure for reliable DRS.	67
9	Banking industry should set up a common center for sharing electronic banking experiences, threats and frauds, difficulties and probable resolutions. In this regard BB can take initiatives with the aid of BIBM, BAB and CTOs forum. An institution like IDRBT (Institute for Development and Research in Banking Technology) which is established by the Reserve Bank of India, can be formed immediately in Bangladesh.	88

Source: BIBM Survey

5.2 Findings and Recommendations

1. The security of the information flow both inside and outside of the bank should be focused. There is a big challenge for the banks having Internet connection to their corporate Intranet. It is the security issue that must be addressed properly with adequate hardware, software and manpower. Every bank should strengthen its ICT security department in ICT division. Recruitment of ethical hacker; placing a proper IT security control and monitoring system etc., are the crying need of banks. Surprisingly, 62% of the banks have no security expert in the IT team. Immediate actions should be taken by top level management of those banks to recruit proper

security experts or to develop security experts quickly by providing high quality training.

2. Security awareness of both bank customers' and employees' is a great concern for banking sector. Customers' awareness can be increased by counseling, advertising and distributing leaflets/brochures. Specialized training on IT security and fraud prevention can be provided to employees of banks.

3. Regular monitoring and auditing the access log and commands being given by admin users to various Applications, Databases and critical devices may reduce the security concerns. However, according to our survey only 48% of the banks have formed this unit. Other banks should form this unit to reduce the IT risk arising from the attempt of unauthorized access and/or undesirable command. The survey shows that only 75% of the banks are checking the access log of IPS/IDS. That means, the rest 25% of banks do not know how many external attacks are being attempted to their system. Banks should engage some officers in the IT security department who might be dedicated for monitoring and checking ACL. It also should be included in the IT security policy so that the IT audit from ICCD can ensure its proper implementation. Our survey shows that 60% of the banks do not prepare report showing total number of unauthorized attempts to access critical systems. Yearly review of the most critical activities is a common mechanism to ensure its security controls. Various solutions are available in the market for effective execution of monitoring and auditing ACL. Such a solution is Security Information and Event Management (SIEM). It enables security/network supervisors to gather log data of all events from a wide variation of network devices across the entire network to detect and report on security threats and doubtful behavior. Not only that it also simplifies forensic investigation and carefully manage the collection, storage and archiving of all log data produced by multiple network devices over a long period of time.

4. It is observed that the level of appreciation by most of the banks' management regarding the skills development of IT personnel through Training and Workshop participation is not at very good stage. Near about 3% of total IT budget goes to training purpose and CTOs are not satisfied regarding this issue. Bank management should increase their level of understanding and appreciation that there is no alternative to develop IT skills in banks because ICT is rapidly changing platform and more critical and devastating cyber-attacks/frauds are also increasing. As per face-to-face discussion, majority of the Heads of IT indicated that budget approval for IT skills development is a challenge for them. Management approves IT budget for system implementation but they are reluctant on training for IT skills development. IT executives may improve their capacity to influence CEO and Board that there is no

alternative to develop ICT skills (especially on IT Governance, IT Project Management, IT Audit, IT Risk Management and IT/Cyber Security) with a view to maintain e-banking system with reliability and security. Blending program can be arranged jointly by software and hardware vendors (IBM, Oracle, Microsoft, Cisco, etc.), expert IT professional of different banks and academicians from different institutes and BIBM. Specialized training, certification and post graduate program for both general bankers and IT professionals of banks may be conducted by BIBM or other related organizations.

5. It is seen that 16% banks have insufficient (less than 2) or no IT auditors which could be one of the IT risk factors related to operation and finance in banking system. The study shows the same weak status of Information Security Officers. This is a serious issue and need to be addressed as soon as possible. But most of the banks don't have sufficient IT auditors to audit their back-offices and branches. We found that 45% of the officers related to IT audit and security have no certification in this regard. Most of them are not internationally certified having inadequate training and experience. That's why they are not confident and efficient enough for conducting fruitful audit. Although small number of IT professionals have certifications, but they are not equipped with relevant banking knowledge. As a result, audit observations and respective recommendations are not focused according to business dimensions. It is clear that poor auditing system of those banks may create another risk for security if auditors fail to identify security holes. Bank management should give special attention to this issue.

6. It is found that 52% banks put audit clauses in SLA and 48% banks don't do it. All banks should add this clause in the SLA for banks' own safety as well as for regulatory compliance. Among the banks those put audit clauses in SLAs, very few (13%) of them audit third-party vendor's institute and their activities as per the signed SLA and 87% banks did not visit vendors at all according to the SLA. Now-a-days, a lot of services are outsourced by the banks. To mitigate outsourcing risk, banks should conduct audit to see the strengths and weaknesses of their vendors as per signed SLA.

7. We have found that data center of all banks are built in Dhaka. However, 54% DCs and 18% DRSs have been established in high-rise buildings having risk of earthquake and fire. On the other hand, DRSs of maximum banks are also established in Dhaka within an average air distance of 12.5 kilometers from the DC, showing very high risk of natural disaster like earthquake. Most of the CTOs of Bangladeshi banks strongly agree that the distance is not enough to avoid natural disaster like earthquake. Banks

should have immediate plan to set up DRS at separate seismic zone and both Govt. and BB may take initiatives to provide infrastructure for reliable DRS.

Regular and periodic testing of a DRS is an important and crucial issue for a centralized online bank. This type of testing increases confidence and expertise of recovering data and business operation in case of any disaster. Research findings reveals that only 72% banks tested live operation from DRS in 2017. Among them, most of the banks tested the live operation in holy days – Friday or Saturday (after 4 p.m.). About 45% of the banks are afraid of testing the disaster recovery site by shutting down the data center any time. This finding indicates the poor quality and readiness of the technology including proper management of data center and disaster recovery site. Frequency and duration of live testing is also unsatisfactory.

BCP/DRP plays an important role to ensure that essential business functions continue to operate during and after a disaster. Only 61% banks have approved guidelines of BCP/DRP. About 28% banks have separate BCP team but team size of this department is very small and team members are not properly trained. Special decision can be taken by all banks including Bangladesh Bank in this regard. This finding indicates the poor quality and readiness of IT disaster recovery management. Banks should have proper policy and guidelines of business continuity and disaster recovery management. Bank authority should have active participations and close monitoring to ensure effectiveness of the policy related to ITDRP.

8. According to our survey, only 32% banks have ITG framework, indicates severe weakness of management's active involvement in IT system management in banks. With a view to enhance the level of understanding on the importance of ITG for effective business development, proper discussion forum or roundtable discussion may be arranged for top management (BoDs and Senior Management). Bangladesh Bank and BIBM may play vital role in this case. Research findings indicate that implementation status of ITG in banks is very weak. Still 8% banks did not initiate ITG implementation process and 60% banks though initiated they have no definite target date to complete the process. Banks should give proper attention and follow appropriate guidelines, standards and frameworks (such as COBIT, ISO/IEC *38500:*2008) to successfully implement ITG.

9. Bangladesh Bank may take initiatives to develop an Information Sharing and Analysis Centers (ISACs) where all the members can discuss and share their opinion regarding the various issues of IT audit and security to mitigate the risks and increase awareness among them about the latest security threats. Moreover, Bangladesh Bank can set up a Data Bank for all of the commercial banks. That will help to collect and share up-to-date information regarding current status, growth, frauds, threats, security

issues and problems of the banking sector of Bangladesh. IT Heads of 88% banks agreed that banking sector should have a center for sharing electronic banking experiences, problems and solutions. An institution like IDRBT (Institute for Development and Research in Banking Technology) which is set up by the Reserve Bank of India can be formed immediately in Bangladesh. Moreover, a Computer Emergency Readiness Team may be formed for disaster recovery of the banking sector.

10. Bangladesh Bank conducts ICT inspection in commercial banks on sample basis once in a year. The duration of inspection is generally very short (two to three days) which is not well enough as ICT is a very vast area and all of its components have direct impact on business. In practice, IT Audit should be comprehensive, not based on sample. Bangladesh Bank may increase the frequency of audit/inspection to ensure a better banking information system. Supervision and monitoring need to be made stronger. More stringent and specific audit mechanism aligned with international standards should be incorporated in supervisory review/inspection by BB. Also, BB may conduct system and functional audit. More skilled ICT audit personnel of BB may be sent for onsite supervision. They might be equipped more with VAPT tools to get the real scenario of the banks IT system. BB may develop Ethical Hackers so that they can identify security holes of commercial banks by sitting their head office and aware the banks.

    Bangladesh Bank may propose a unique organogram for all the banks covering all the areas of IT Services like Software, Network, IT Security, IT Assurance and Compliance, System, Support and Services, Payment Services, DBA, IT Administration and Data Centre Management, Planning and Innovation, Business IT.

    Bangladesh Bank may define IT standards for all Financial Institutes, set a roadmap in the following areas so that the shareholders get the value of their investment.

Table 7: Proposed Standards for different areas of Banks/FIs:

Areas	Standards
Strategic IT Alignment	COBIT
IT Governance	COBIT, ISO 38500
Architecture & Information Management	ISO 20022, TOGAF
Service Delivery	CMMI, ISO 15504, PRINCE 2, PMBOK, ITIL
Service Management	ITIL, ISO 20000, OHSAS 18001, ISO 22304
Information Security	ISO 27001, PCI DSS
Workshop & Resource Management	SFIA

References

Alam M.R., Mehdee T., Yesmin R. and Hossain M. Z. (2017), "Alternative Delivery Channel: Opportunities and Challenges of the New Banking Environment", *Banking Research Series*, BIBM, Dhaka, Bangladesh.

Bangladesh Bank, *Financial Stability Report*, Various Issues (2015-2017), Department of Off-Site Supervision, Bangladesh Bank.

Bangladesh Bank (2015), *Guideline on ICT Security for Banks and Non-Bank Financial Institutions*, 2015, Dhaka, Bangladesh.

Bhasin T. M., (2008), *E-commerce in Indian Banking*, India: Authors Press.

Centre for Advanced Financial Research and learning (2016), "*Cyber Risk and Mitigation for banks and FIs",* International Seminar Paper.

University of Cambridge (2018), "*Cyber Risk Outlook 2018*", Center for Risk Studies, University of Cambridge, 2018.

Ernst & Young (2017), *Responding to cyber incidents in India*, Ernst & Young, 2017.

Ernst & Young (2017), *Confronting the New Age Cyber Criminal*, Ernst & Young, 2017.

Habib, S. M. A, Khan, M. S. U, Alam, M. R., Rabbi K. and Bahauddin, K. M. (2011), "Implication of the use of Information and Communication Technology in Channeling Workers' Remittances to Bangladesh", *Research Monograph 001*, BIBM, Dhaka.

Internet Crime Complaint Center (IC3), (2017), *Internet Crime Report*, IC3, 2017.

Kaspersky (2017), *Ready or Not? A global survey into attitudes and opinions on IT security*, Kaspersky, 2017.

KPMG (2016), *Cybercrime Survey Report: Insights and Perspectives.* KPMG, 2017

KPMG (2016), *Global Profiles of the fraudsters*, KPMG, 2016.

Laudon K., Laudon J. (2016), *Management Information System*, India: Pearson

Ministry of Information (2010), *ICT Act, 2006*, Bangladesh Government, Dhaka

Net Guardian (2017), *Digital Banking Fraud*, Net Guardian, 2017

PwC (2017), *The Cyber threat to Banking*, PwC, 2017.

Rahman, M. (2008), 'Innovative Technology and Bank Profitability: The Bangladesh Experience', *Working paper series 0803*, Policy Analysis Unit (PAU), Bangladesh Bank.

RSA (2018), *RSA Quarterly Fraud Report*, RSA, 2018.

Shirin A.K. (2011), *Information Technology in Financial Services*, 1st Edition, 2011, Tithy Printing & Packaging, Dhaka, Bangladesh.

Sim G. (2018), *Cyber Security*, ASEAN Bankers Association, April, 2018.

SWIFT (2017), *The evolving cyber threat to the banking community,* SWIFT, 2017.

Symantec (2012), *Banks likely to remain top cybercrime targets*, Symantec, 2012.

Uddin M. S., Alam M. R., Rabbi K., Hasan M. F. (2017), "IT Operations of Banks", Various Issues (2015-2017), *Banking Review Series*, BIBM, Dhaka, Bangladesh.

Uddin M. S., Alam M. R., Rabbi K. (2014), "Information System Security in Banks: Bangladesh Perspective", *Research Monograph 007*, BIBM, Dhaka, Bangladesh.

Uddin M. S., Alam M. R., Rabbi K. (2011), "Mobile Banking in Bangladesh", *Banking Research Series*, BIBM, Dhaka, Bangladesh.

Uddin M. S., Alam M. R., Rabbi K. (2010), "IT Readiness of Banks for Business in Cyber Space", *Banking Research Series*, BIBM, Dhaka, Bangladesh.

World Economic Forum (2016), *World Economic Forum Global Risk Report,* World Economic Forum, 2016.

Bangladesh Institute of Bank Management (BIBM)
Plot No.-4, Main Road No. -1 (South), Section No. -2, Mirpur, Dhaka-1216
Tel: 9003031-5;9003051-2, Fax: 880-2-9006756,E-mail bibmresearch@bibm.org.bd; Web: www.bibm.org.bd

Price: BDT 300.00
USD 8.00