CHALLENGES OF CYBER SECURITY AND DATA PROTECTION AMIDST DISRUPTIVE CHANGE – THE ROLE OF BANKERS AND FINANCE PROFESSIONALS

Bhanu Wijayaratne
Assistant General Manager - Risk
HNB Finance Ltd

INTRODUCTION

Cyber security and data protection is of vital importance to all financial institutions, as they carry very confidential and sensitive information about their customers as well as relate to their own business strategies. On the other hand, in the present environment data is considered as one of the most expensive commodities which is essential for effective decision making in business, and equally needed to drive business strategies efficiently.

As a result, data hackers and various undesired elements are trying out all their avenues to access such data and make attempts towards unauthorized use of data which in turn necessitate the financial institutions (FIs) to have robust cyber security systems in place, in order to ensure that such FIs are safe from various vulnerabilities that can turn detrimental to them.

Among such vulnerabilities, breaches in the FIs duty of secrecy can lead towards loss of customers' confidence that can end up as a serious reputational issue which can trigger regulatory repercussions as well.

The fact that FIs are undergoing dramatic changes in their business models and strategies, with the transformations taking place across the industry resulting from deployment of a series of technological innovations such as Cloud Computing, Big Data Analytics, Artificial Intelligence and Machine Learning, Robotic Process Automations, Distributed Ledger Technology, Block Chain etc, it is extremely important and essential that all Banks and other FIs pay due attention to protect their data and ensure cyber security.

As per the website www.techopedia.com, Data Protection is defined as "the process of protecting data which revolves around the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding such data", which aims to strike a balance between individual privacy rights whilst still allowing data to be used for business purposes.

This article attempts to address the areas such as,

- The threats posed towards data protection and the ways and means of identification of them.
- The controls that can be introduced towards data protection and cyber security.
- The regulatory regime that governs cyber security and data protection.
- The measures that can be taken to effectively & efficiently manage issues relating to cyber security and data protection.

CHALLENGES AND THREATS TO CYBER SECURITY

Challenges or threats to cyber security may occur in form of attempts to expose, alter, disable, destroy, steal or gain unauthorized access to data. In the given attempts, data hackers would capture control of the computer systems and demand ransom to release such controls.

Cyber attacks

Cyber attacks can be broadly categorized into two types namely, web-based attacks and system based attacks.

System-based attacks can be explained as attempts to compromise a computer network or a computer.

In addition, it is commonly observed that phishing attacks are also used by data hackers to fraudulently obtain sensitive information such as user names, passwords and credit or debit card details by disguising as trustworthy entity in an electronic communication.

Further, if the attackers require extra interaction from the user to access data, same is known as "click jacking". The motive of the attackers under click jacking is to open the targeted website in an invisible frame and get the user to click the frame, without even him knowing that he is clicking the hacker's website.

Drive –By Downloads are another sophisticated web attack that hackers perpetrate against online users. This method requires no user action to download malicious content onto a legitimate website.

Spams

Spams can be described as the use of electronic messaging systems to send out unsolicited e-mails, often of a commercial nature to multiple mailing lists, individuals or news group postings. According to Sophos's Internet Security Threat Report, spams are all on the rise across networks together with malware & phishing attacks. Spam is more than annoying, and can be really

dangerous, if it is part of a phishing scam initiated to obtain your passwords, credit card details, bank account details etc.

Spams can be of different types, namely Image Spam, Blank Spam, Back scatter Spam etc. Common implications of spams can be cited as follows:

- Degrades the internet speed significantly.
- Steals useful information such as details in a contact list.
- Alters search results on search engines.

Trojan Horse

A Trojan Horse or a Trojan is a malicious computer programme which can mislead users of it's intent, as it's software looks legitimate and genuine but can take control of your computer. Users are deceived and misled by some form of social engineering into loading and executing Trojans on their systems, which could enable cyber criminals to spy on and steal sensitive data and gain unauthorized access to your system, inclusive of actions such as deletion, copying, modifying and blocking of data in your system.

There are different types of Trojans currently seen. Backdoor Trojan enables malicious users to control the targeted computer, whilst Trojan Banker would support to steal account information on online banking systems. The Trojan Downloader can download and install new versions of malicious programmes on to the computer.

Common features of a Trojan Horse are:

- Weird messages and pop ups
- Slowness in computer
- Interrupted internet connection
- Unusual applications
- Missing files
- Malicious windows

Pharming

Pharming can be defined as modifying DNS entries, that would direct the users to a wrong website instead of accessing their intended website. It is a fraudulent initiative to mislead internet users towards a bogus website, in order to obtain personal information such as passwords, account numbers etc. This is done by installing a malicious code on the personal computer or server.

Pharming though carrying similar characteristics to phishing attacks, is somewhat different to same as phishing involves getting the user to enter personal information via a fake website. Pharming can be identified as vigilant as the URL is different from that of the genuine website.

Spyware

Spyware is another threat to cyber security which enables hackers to gain access to information of the activities of another person's computer by transmitting data covertly from the hard drive. Using spyware, one can gather vital information of the target user, which includes internet surfing habits, user logins, bank detail etc. but not limited to same. It can also compromise the genuine user's control of the computer by installing additional software and re-directing web browsers.

There are different types of spyware such as Adware & Commercial Spyware etc. Adware is commonly used by advertisers to catch the web surfing habits of users and also to gather details of sites visited by users.

Commercial spyware on the other hand is not unauthorized at all times. The service provider who supply free software and social networking platforms use this method to monitor the usage of their software by the market.

Spyware can be identified with following observations.

- Unusual number of pop-up advertisements.
- Slowness of the computer when opening programmes & saving files
- Appearing of new tool bars on the web browser
- Failure of certain keys in the browser

Computer Viruses

As per Wikipedia, a computer virus is a type of malware that when executed replicates itself by modifying other computer programmes and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus. Attackers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to firstly infect systems and then to spread the virus. Viruses are often found in file downloads and E-mail attachments. When downloading a file or opening an attachment the virus gets activated.

There are different types of viruses such as Boot Sector Virus, Direct Action Virus, Multipartite Virus and Polymorphic Virus etc., depicting different characteristics as a result of which one might suddenly experience situations such as the mails being hijacked, files going missing, sudden lack of storage and space, slow startups and performance, which could be signs of the computer and network being infected by a virus.

Worms

A computer worm is another form of a threat to a computer or a network. It is a standalone malware computer programme that replicates itself in order to spread to other computers. Such software is very sophisticated, thus can collect and dispatch data to specified locations, using information about the network of its own.

E-mail worm is another type of a worm which uses the e-mail to spread itself. On the other hand, internet worms are completely autonomous programmes, which use the infected machine to scan the internet for other vulnerable machines.

Two other commonly seen types of worms are Site-sharing Network Worms and Instant Message Chat Room Worms. If one observes scenarios such as slow performance of the computer, programmes opening and running automatically, irregular levels of performance in Web browser, firewall workings and missing or modified files etc., they may be signs of the computer being attacked by worms.

Key Loggers

Keystroke logging, often referred to as key logging or keyboard capturing, is the action of recording the keys struck on a keyboard, typically covertly, so that persons using the keyboard are unaware that their actions are being monitored. Data can then be retrieved by the hacker who operates the logging programme. Accordingly, it should be noted that key logging is a serious threat to users and their data.

There are two main types of key loggers, namely software based key loggers and hardware based key loggers. Software based key loggers are essentially programs that aim to monitor the operating system of the computer, thus are really more dangerous. Hardware based key loggers on the other hand do not need any additional installations, as they are already within the physical system of the computer.

In order to identify the key loggers, one may be watchful and vigilant on scenarios such as slow computer performance, strange delays in the computer, new desktop icons, excessive hard drive or network activity, if experienced on your computer.

DATA PROTECTION CONTROLS

Due to the growing number of threats as mentioned above all computer users and data owners, specially the Banks and other Financial institutions need to be mindful of the subject vulnerabilities and ensure that appropriate action is taken towards protection of data and cyber security.

As per the standard information security principles, there are three types of controls, namely

- Preventive controls
- Directive controls
- Responsive / Corrective controls.

Within the above three types of data protection controls, same can be further classified into three types depending on its method of application.

- Automated controls
- Manual controls
- Partially automated controls

Automated Controls

Automated controls can be described as technical controls as well, which facilitate measures that are intended to cater to the protection requirements of the system. Such controls are executed through the computer system itself which provide automated protection from unauthorized access or misuse. It also facilitates detection of security violations and support security requirements for application and data. However, it should be noted that implementation of security controls requires significant operational considerations. Effective enforcement of technical controls merits attention and focus on following key areas.

- Identification and Authentication
- Logical Access Control
- Audit Trails.

a). Identification and Authentication

Under identification and authentication requirements, the following areas need to be given due focus and attention.

- Frequency of password change
- Who changes the password (user/system administrator etc.)

- Characteristics of password such as,
  - √ Length of the password (Minimum and maximum characters)
  - √ Allowable character set
  - √ Password aging time frames and enforcement approach
  - √ Number of generations of expired password disallowed for use
  - √ Procedure to be followed for password changes
  - √ Procedures for handling password compromise
  - √ Procedures for training users and the content to be covered.

- The level of enforcement of the access control mechanism (i.e. network operating system etc.)
- How the access control mechanism supports individual accountability. (eg ; passwords associated with a user ID that is assigned to an individual)
- Self-protection techniques for the user authentication mechanism (password encrypted while in transmission, automatic generation of passwords etc.)
- Individual access attempts for a given user ID.
- Whether passwords are IP specific, i.e. access location restricted or not
- Ensuring that all system provided administrative default passwords are changed
- Policies that provide for bypassing user authentication requirements, single sign on technologies etc. (eg:- host-to-host, authentication servers, user-to-host identifiers or group user identifiers)
- Use of digital or electronic signatures and the standards used.
- How biometric controls are used and implemented.

Actions taken when the above requirements are not met or ignored need to be documented and implemented.

b). Logical Access Controls

In the process of ensuring cyber security and data protection, it is also important to ensure that there are controls in place to authorize or restrict and monitor the user activities within the system. Accordingly, the features of both hardware and software need to be looked at in terms of its design to permit only authorized access to or within the system. This is done in order to ensure that users are restricted to authorized functions and transactions, thereby to detect unauthorized activities and transactions performed.

In order to ensure effective and efficient logical access controls, following areas need to be given due consideration.

- How are access rights granted?
- Are privileges granted based on the job function?
- Has segregation of duties been given due attention when granting access rights?
  Eg - System developers should not be granted permission to deploy systems, version upgrades etc. in production or live system.

- System capabilities in generating access control lists etc.
- Whether users are restricted from accessing operating systems or other system resources are not required in the performance of their duties.
- Controls to detect unauthorized transaction attempts by both authorized and unauthorized users.
- Any restrictions to prevent users accessing the system outside normal working hours or on weekends, unless their respective job roles require them to do so.
- Is there a time bar for the system to automatically blank the associated display screens in the event such users have been inactive for a considerable predetermined time period?
- After what period of user's inactivity, does the system require the user to enter a unique password before reconnecting.
- Whether encryption is used to prevent access to sensitive files as part of the system access control procedure.
- Availability of policies and logical access controls to regulate how users are granted access permission or make copies of the files or information accessible to other users.
- What other hardware or technical controls are used to provide protection against unauthorized system penetration and other known internet threats and vulnerabilities, if the system is connected to internet or any other wide area network. (WAN)
- Whether any port protection devices are used to require specific access authorization to the communication ports, including the configuration of the port protection devices.

c). Audit Trails

In the initiatives of data protection, it is important to ensure that the system is enriched with effective audit trails to support accountability by providing a trace of user actions. Accordingly, audit trails should be designed in such a way that they provide appropriate information that can assist in intrusion detection and remediation. In other words, audit trails should include sufficient information to establish what events occurred and who initiated them. (eg: type of event, when the event occurred, user IDs associated with the event or transaction etc.)

The following controls should be embedded into the audit trails and related procedures to ensure effective checking of audit trails:

- Should capture information to assist in intrusion detection;
- How audit trails are used as online tools to help identify problems other than intrusions as they occur;
- How separation of duties has been established between the personnel who administer the access control function and those who administer the audit trail and its operational function;

- How the appropriate system level or application level administrator would review the audit trails, upon known system or application software problems, a known violation of existing requirement by a user or any unexpected system or user problem etc.
- How effectively audit services and analytic tools are used in a real time or near real time fashion.

Manual Controls

The controls that are manually performed by individuals are known as manual controls, where no IT generated reports or techniques are used.

Accordingly, manual controls include some of the following activities which fall within part of IT General Controls (ITGC) as well.

- Controlling physical access to unauthorized areas.
- Prohibiting the use of cameras, mobile phones, recording devices in restricted areas.
- Keeping back-up tapes in a secured off-site location.
- Keeping hard copies / back-up tapes containing important data in a fire-proof vault under dual control.
- Placing a screen cover on the monitor that reduces the viewing angle.
- Requesting customers/visitors to remove helmets, caps, jackets etc. when entering ATM cubicles, banks etc.

Partially Automated Controls

There are certain controls that can be enforced on data protection which are partially automated but need manual intervention to complete the procedure, which are known as partially automated controls.

a). Two Factor Authentication

In order to perform a transaction by a user upon a system, it pauses the person halfway down and requires the user to input a password, commonly known as “one-time password” (OTP), which is sent by the system itself to the user either on his mobile phone, e-mail or to a special device outside the system, with which only the transaction is allowed to be continued towards completion. This is a partially automated control used to ensure that only the authorized users are given access to perform certain transactions.

b). CCTV Monitoring

Real time monitoring or monitoring of the recording of CCTV images would ensure detection of unauthorized access or wrong practices.

PREVENTING CYBER ATTACKS

i. Preventive Controls

This can be achieved by taking various steps and some of which are as follows.

- Refrain from opening emails from unknown sources from outside.
- Virus guards to be daily updated.
- Lock the functioning of USB Ports and CD Drives of the computers of users.
- All updates to the system be done from a central point.

Data Encryption

Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as cipher text, appears scrambled or unreadable to a person or entity accessing without permission.

Data Destruction

Data destruction in the process of legitimately destroying data stored in devices, tapes, hard disks and other forms of electronic media, preventing unauthorized persons accessing such data.

Data destruction is an umbrella term for the legitimate destruction of data which includes both hard drive destruction and software destruction and are put into practice in the following scenarios.

- When replacing a computer with a new one, the data in the hard disk needs to be destroyed before disposal, by running a destruction software.
- Data backup tapes to be burnt when the backup tapes are to be disposed.
- Non-disclosure agreements (NDAs) to be signed when obtaining services by third parties and ensure that they agree to permanently delete the data available with them at the end of the service agreement or contract.

Data Masking

Masking a particular portion of data can protect it from being fully disclosed to an internal unauthorized party or a malicious source as well as to internal personnel who could potentially misuse such data. This is also known as "Anonymization". Example: The last 8 digits of a credit card may be masked in the data base.

Tokenization

When you issue an acknowledgement or a receipt to a customer or a third party on a transaction performed by way of a printed receipt or by way of an electronic notification (SMS), you may indicate only part of the account number leaving the rest denoted with characters. eg. 7811 XXXX 8516 XXXX

Protecting e-mail data

Controls should be in place on transmitting data and information via e-mails.

The capacity of information that can be transmitted via an e-mail should be restricted depending on a need basis and also using the level of the password that has been assigned to the user, keeping in line with the responsibilities and the job role assigned. Also, further controls can be enforced by restricting the attachments to PDF files, coupled with data classification initiatives by which users will be permitted to transmit only certain classified data categories, linked to the level of password assigned.

Data Classification

Data classification is an initiative to secure the organization's information.

It is the process of identification of data classified into different categories in terms of its importance and sensitivity and assigning access of such data to users depending on its importance based on predetermined levels of sensitivity and relevance.

Accordingly, it must be noted that a proper data classification allows your organization to install appropriate controls based on the predetermined category of data, which enables different level of controls, rather than having same level of control for all types of data, which is known as a risk based approach, that can save your time and money whilst ensuring that your most sensitive data is given high level attention and focus towards better security and protection.

ii. Detective Controls

Detective controls are a key component of cyber security and data protection which provides visibility into malicious activity, breaches and attacks on an organization's IT systems.

Financial institutions, specially banks given their legal duty of secrecy towards their customers, coupled with the sensitivity of business information available in their data bases, need to be geared with fully fledged monitoring and detection tools that are commensurate with the importance and sensitivity of the business information held by them and the level of usage of technology, in terms of its vastness and complexity.

Fire Walls

As per Wikipedia, a Firewall, in computing is a network security system that monitors and controls incoming and outgoing network traffic based on pre-determined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network such as the internet.

Privileged Access Management (PAM)

Privileged Access Management is a solution that helps organizations restrict privileged access within an existing Active Directory environment. (AD)

In the present environment, it is not so difficult for attackers to obtain credentials of domain administrators. The objective of PAM is to curtail opportunities for malicious users to get access to your system, whilst increasing the internal controls. PAM makes it harder for the malicious attackers to penetrate into a network and obtain privileged account access. It also facilitates higher level monitoring, more visibility and more fine-tuned controls, which allow the organizations to ascertain who their privileged account users are and what activities they have performed etc. In other words, PAM gives more insights into how administrative accounts are used in the environment (Wikipedia – docs.microsoft.com)

Periodic Access Reviews and System Audit Logs

User access reviews covering all users need to be conducted periodically at a pre-determined frequency to detect any unauthorized access by users.

System audits too are required to be conducted frequently, through which system log reports need to be carefully reviewed and analyzed to detect any breaches, wrong doings, malpractices etc., should there be any.

iii. Corrective Controls

Corrective controls are designed to correct errors, breaches or to mitigate risks and prevent recurrence of further errors or wrong doings.

However, it must be noted that in practice corrective controls are often coupled with preventive and detective controls. Corrective controls facilitate remedy on undesirable outcomes that have occurred and reduce risks to an acceptable level when other controls fail or are not cost-effective.

Network Security Vulnerability Assessment

Network vulnerability assessment is the process of reviewing and analyzing a computer network for possible security vulnerability and shortcomings. It is used by network administrators to evaluate the security architecture and defense of the network against possible vulnerabilities and threats.

Among the assessments to be conducted under network security vulnerability assessment, following are some key areas which merit attention but not limited to same.

- Internal Security Vulnerability Assessment
- External Security Vulnerability Assessment
- Web application Security Vulnerability Assessment
- Firewall security configuration Assessment
- Wireless network security Vulnerability Assessment
- Switch security Vulnerability Assessment.

REGULATORY FRAMEWORK AND GLOBAL IT SECURITY STANDARDS AND BEST PRACTICES

General Data Protection Regulations (GDPR)

Regularly new regulations and international best practices are introduced which impact organizations across the globe. In 2012 European Union implemented General Data Protection Regulations (GDPR), which enables the customers to view, limit and control, how Banks and other companies collect and process their personal data.

The underlying concept of GDPR reforms was to initially make Europe fit for the "digital age". Over a space of four years, agreements were reached on how same would be enforced, as a result of which GDPR implementation deadline was fixed as 25th May 2018.

Applicability of GDPR

GDPR applies to organizations and entities operating within European Union (EU) as well as those who operate outside EU, provided they transact business with companies or organizations within EU. This resulted in GDPR becoming applicable to all major business entities throughout the globe who deal with EU.

Accordingly, all Sri Lankan corporates who deal with personal data of EU residents shall be required to comply with GDPR, even though such laws are not extraterritorial, and not directly enforceable on persons outside EU. However, the authorities have enforced such law on EU counter parties dealing with entities and persons outside the EU, compelling the EU counterparts to drop their trade or business ties with other countries unless such third parties are compliant with the GDPR.

Accordingly, GDPR compliant Banks in Sri Lanka would benefit by being able to open accounts for residents and businesses incorporated in EU, which include cross-border transactions, maintaining of correspondent banking relationships and other international trade related business activities.

How to be compliant with GDPR

GDPR has taken initiatives to provide customers with the right to know, in the event their personal data are being hacked. Entities who hold such data are required to notify regarding such data secrecy breaches to appropriate national bodies no sooner such incidents occur, in order to ensure that the subject EU citizens can take measures as appropriate to prevent their data being misused and abused.

The following requirements need to be met in order to be compliant with GDPR:

- Need to organize your data in such a way that in the event a person inquires as to what information on him is in your possession, as the data holding entity you should be in a position to provide such information as quickly as possible.
- Need to ensure that the data held in their possession is well secured.
- Need to ensure that data is not held unnecessarily.
- Need to have a fair processing policy.
- Need to have an efficient process to provide information to the person concerned, free of charge, if requested.
- Need to have a clear process for deletion of data.
- Need to obtain written consent of the consumer, if their personal data is to be used for marketing purposes.
- Need to appoint a Data Protection Officer.

Global Standards

Payment Card Industry Data Security Standards – (PCI-DSS)

PCI-DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data. In other words it is a set of security standards designed to ensure that all companies that hold such data maintain them in a well secured environment.

PCI standards are mandated by the card brands administered by the Payment Card Industry Security Standards Council. Such standards were created to establish controls to reduce credit card frauds. Validation of compliance needs to be performed annually or quarterly as per pre-determined frequencies, either by external Qualified Security Assessor (QSA) or by a firm specific Internal Security Assessor (ISA), who should present a report on compliance.

Under PCI-DSS, entities are required to protect card related data by implementing the following control measures.

- Install and maintain a firewall configuration to protect cardholder data.
- Not to use vendor supplied defaults for system passwords and other security parameters.
- Protect stored data
- Encrypt transmission of card related data
- To have in place effective anti-virus software
- Develop and maintain secure systems and applications
- Assign a unique ID to each person with access rights to computer
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

The Sri Lankan Regulatory Regime

Following are the key regulatory requirements applicable to information security under the Sri Lankan regulatory regime.

- Computer Crimes Act No. 24 of 2007
- Baseline Security Standards for Information Security Management
- Guidelines on Minimum Compliance Standards for Payment related Mobile Applications
- Finance Companies Direction No. 4 of 2012 on Information System Security Policy

Computer Crimes Act No. 24 of 2007

This legislation was passed by the Sri Lankan Parliament as a result of numerous initiatives taken and contributions made by sources such as the CINTEC Law Committee, a Sub Committee of the Law Commission and Ministry of Justice of Sri Lanka. It is no doubt a timely enaction, when advancements were being made in the field of Information Communication Technology (ICT) in Sri Lanka, through several initiatives such as e-Sri Lanka Project etc.

Computer crimes consist of three main components.

- Crimes committed using computers as tools for such criminal activity
- Hacking offences which affect integrity, availability and confidentiality of a computer system or network.
- Content related cyber crimes, where computers together with internet resources are used to distribute illegal data.

The Computer Crimes Act No. 24 of 2007 primarily addresses computer related crimes and hacking offences whilst content related offences are being handled through a series of changes to the Penal Code and other statutory provisions.

Baseline Security Standard for Information Security Management

As per Banking Act Direction No. 4 of 2014 of 26.06.2014, all banks are required to implement the Baseline Security Standard for Information Security Management which came into effect from 01.07.2015.

According to Baseline Security Standard, Information Security Management can be explained as "The preservation of confidentiality, integrity and availability of information by the appropriate and systematic application of security controls in order to manage the risk of exposure to a threat, which arises due to the existence of vulnerabilities in information assets."

CONCLUSION

The purpose of cyber security and data protection is to help prevention of cyber attacks, data breaches, leakage of valuable information etc which can also support effective risk management.

As cyber crime is constantly on the rise, IT security and data protection initiatives and solutions are essential for all kinds of businesses, specially for Banks and other Financial Institutions, given the high importance of the internet and the digital systems they use, compelled with the dire need to strictly comply with the "duty of secrecy", thereby upholding customer confidence on them.

As per the Cyber Security Breaches survey of 2017 of United Kingdom, more than 46% of UK businesses experienced a cyber attack of some sort and many of these businesses have suffered as a result loss of customers confidence and even the actual theft of personal and business information. Although one cannot lay hands to such authentic information in Sri Lanka, the issues and risks faced by Sri Lankan Banks and other Financial Institutions cannot be underestimated.

Accordingly, it is essential that we train our employees on cyber security principles and ensure necessary preventive, detective and responsive action is taken as detailed in this article, if we are to safeguard the business of banking towards a better tomorrow.

References

- Consultation paper for CBSL on technology risks resilience for licensed banks.
- Guideline on minimum compliance standards for payment related mobile application No 01 of 2018
- Finance Company Directives No 4 of 2012 on Information System Security Policy.
- Insights and Recommendations for cyber security professionals from ISCA.
- Baseline Security Standards for Information Security Management
- Wikipedia
- cisco.com
- checkpoint.com
- techopedia.com
- cybergrx.com
- blog.thalesecurity.com