White Paper on

Cyber Risk Management and 10 Essential Security tools

Published on 1st July, 2016

Bharat Panchal
Head - Risk Management
National Payments Corporation of India

This white paper is authored by Mr. Bharat Panchal, who is currently working as Head – Risk Management at the National Payments Corporation of India (NPCI) since 2011. At NPCI, he is responsible to evaluate, implement and monitor improvements pertaining to Risk Management, controls and governance areas like Enterprise Risk Management (ERM), Operational Risk Management (ORM), Information Security, Internal Audit and Fraud Management. He has established a sound risk management framework across the organisation and has partnered with functions and member banks to ensure efficiency and effectiveness of operations, safeguarding tangible and intangible assets, accuracy and integrity of transactions and processes.

Author can be contacted via email: bharat.panchal@npci.org.in

This White Paper

This paper will discuss the current cyber security challenges in the banking and financial institutions in India. It will also provide information about the major threats indicators and the risk of data loss. It will present some governance framework to help you maintain compliance with the many regulations governing your business. Finally, it will talk about the best possible controls by way of deploying essential tools to prevent the organisations from potential cyber security threats which can help organisation to defend against threats and mitigate risks.

Overview

Securing technology systems and protecting the data and assets of customers remains one of the highest priorities for any financial institution. Evolving security threats, both internal and external, require the use of new controls, latest methods and sophisticated advanced security tools to protect all transaction activities and data. Multifaceted and layered security tools and procedures strengthen any institution's efforts in combating against these threats by providing multiple automated barriers at different levels. Hence it is important to ensure that security practices are stringent by utilising a strong, multi-layered security strategy, including the use of firewalls, proxy servers, SEIM (Security Incident and Event Management) 2 factor authentication with tokens, PIM (Privilege Identity Management), FIM (File Integrity Management), WAF (Web Application Filtering), APT (Advanced Persistent Threats). In the banking and payment system network like NPCI, a strong security strategy requires that all high-risk transactions be reviewed and authorised by the customer, and that the payment system networks uses industry-standard practices to validate the legitimacy of those transactions. A layered security policy should also take into consideration where sensitive data is stored, human resources, and the physical assets of the organisation, including laptops, tablets, printers, scanners, mobile phones, WiFi and access to all other facilities.

Cyber Risk Management

Cyber risk management is a complex problem which needs complete sponsorship from the executive management, forward thinking governance, advanced techniques, threat correlation and collaboration throughout the organisation. The goal of cyber risk management is to build cyber resiliency, where the organisation's systems and operations are designed to detect cyber threats at very early stage and respond to such events to minimize business disruption and financial losses. A cyber risk management program must be one of many components of overall business risk environment as a part of enterprise risk management framework. The top management team should recognise its leadership role in setting the proper tone and structure for enabling cyber resiliency throughout the organisation. They should also recognise the importance of identifying and mitigating cyber risks as an essential task in maintaining the on-going success of their institution. It is very essential that executive management take the following steps to implement successful cyber risk governance:

This step should include improving cyber intelligence gathering techniques, leveraging cyber insurance options, and upgrading cyber security technologies time to time to align with emerging cyber threats. The top management team must ensure that a program exists within the organisation to manage cyber risks to reduce potential harm to their business and improve their cyber resiliency and it is updated regularly to align it with emerging threats and its mitigation. It may essential to re-evaluate cyber risk priorities and investments to ensure that the financial institution's cyber business risk perimeter is fully protected at regular interval.

a. Establish cyber risk governance – The foundation of any cyber resilient organisation is a strong governance framework for managing cyber risks. This is established by well-defined and unambiguous roles among teams, well documented operating processes and a clear reporting structure. Other risk programs such as disaster recovery, business continuity, and crisis management must be well inter-linked with the cyber risk program.

b. Define cyber risk boundary – An organisation's cyber vulnerabilities extend to all possible places where its data is stored, transmitted, and accessed — which may be employees themselves, its trusted partners, member institutions and customers. Apart from this, nowadays, lot of data goes into big data, analytics, and social media. Organisation must take this into cognizance while deciding the boundaries.

c. Identify critical business processes and assets – Organisations should very precisely identify what are their most valuable revenue streams,

business processes, assets, and facilities. After these are identified, understand where they are located, how it is performed and who are authorised to use or access the same.

d. Assess cyber threats – Effective cyber risk monitoring focuses on building a sustainable and resilient approach to putting early warning inputs from various teams in collective manner to quickly correlate threats in real time. Financial institutions should establish a robust threat-analysis capability built on shared intelligence, data, and research from internal and external sources.

e. Collection, analysis, and reporting of information – Financial institutions should ensure that their cyber risk operations team or SOC (security operations center) supports three primary functions i.e. collection and management, processing and analysing, and reporting and action to build robust cyber and advanced cyber threat intelligence capabilities.

f. Plan and respond – The development of prepared responses is a necessary step in adequately planning and preparing responses to cyber events. Based on cyber intelligence gathered throughout, a clearly defined process must be developed which depicts who should take action, what their responsibilities are, and exactly what they should do. Executive management should also frequently revisit cyber intelligence gathering techniques, refresh or upgrade cyber security technologies and review their cyber insurance arrangement.

Cyber Risk Governance

The cyber risk governance process should be designed to help the senior management and the Board to get better visibility on cyber risks. A cyber risk management capability should be well interlinked and should be a key component of the enterprise risk management program. The governance process is established by deciding who will be on each of the teams, and setting up operating processes and a reporting structure. A team of senior management i.e. Chief Operating Officer, Chief Technology Officer, Chief Risk Officer, Heads of Operations, security, business should be part of the steering committee which should be the driving force in the organisation for cyber risk governance. This committee must monitor the organisation's cyber risk position and reports it to the senior management and the board of directors. They also review reports from the cyber risk oversight and operations teams and helps prioritise emerging cyber threats and accordingly review strategy to adapt the program as the cyber risk threat profile. Cyber Security or Information Security team under Risk Management should continuously assess the cyber risk the organisation faces, the people behind them, and the assets they threaten. They must be in position to identify new threats and improves how information assets are protected on continual basis. This is because business changes has an impact on the cyber perimeter as well for example new service offerings, major change or revamp on existing services, introduction of new suppliers, vendors, or business partners etc. The security operations team should produce reports for the cyber risk steering committee, which gives number and type of cyber events, origination and duration of events, which assets have been targeted, kinds of fraud or cyber attacks attempted, comparison of cyber events to industry trends, incident and response reports, threat assessments, and intelligence reports etc.

Define cyber risk boundary

Identify and define the boundary that organisation has to protect from any cyber threat. An organisation's cyber vulnerabilities extend to locations where its data is stored, transmitted, and accessed, both by organisations and its service providers. Any weakness in the perimeter becomes organisation's vulnerability. This challenge will continue to increase as the organisation's cyber security perimeter continues to expand as customers increase their demands to allow access to their information irrespective where it is stored.

Identify critical business processes and assets

It is very important to identify the assets you need to protect and the level of protection needed for such asset. Asset classification is second most important activity. It should be determined what comprises their most valuable business assets, where these assets are located at any given time, and who has access to them. They should also determine which business processes, if compromised, would lead to significant hardship to the business. Finally, they should identify key facilities that house or support key data elements or business processes. We refer to these collectively as "crown jewels" — those information assets or processes, which if stolen, compromised, or used inappropriately would render significant hardship to your business.

Most organisations' threat analysis efforts inhabit a disjointed environment spread across several functions, physical locations, and systems. This disjointed nature and lack of common methods to consume intelligence is a significant barrier to establishing a robust cyber risk intelligence capability. To close this deficit, organisations should establish a robust threat analysis capability that is built on shared intelligence, data, and research from internal and external sources. To build a robust cyber intelligence infrastructure, financial institutions should ensure their cyber risk operations team supports the organisation by correctly analysing cyber risk data, providing leadership with the cyber risk information it needs to make informed decisions, and proactively and quickly responding to attacks.

Assess cyber risks:

Largely, all information security tools are designed and implemented to identify unusual patterns or traffic types and alert security and operations teams about possible abnormality. The typical IT-centric response is to deploy additional tools and personnel to put it all together. While these generic tools can be quite useful in correlating known types of activities, they are incapable of automatically identifying and reacting to new threats. Effective cyber risk monitoring focuses on building a sustainable and resilient approach to putting intelligence inputs from various functional teams together under a common lens to quickly correlate and dynamically adjust the risk posture of the organisation to these threats in real time. Its important to design appropriate actions based on threat landscape. Most organisations' threat analysis efforts inhabit a disjointed environment spread across several functions, physical locations, and systems. Lack of common methods to consume intelligence is a significant barrier to establishing a robust cyber risk intelligence capability. Such gap can be bridged by establishing a robust threat analysis capability that is built on shared intelligence, data, and research from internal and external sources. To build a robust cyber intelligence infrastructure, it is important that financial institutions ensure their cyber security team supports the organisation by using appropriate tools, correctly analyzing cyber risk data, providing leadership with the cyber risk information it needs to make informed decisions, and proactively and quickly responding to attacks. This papers will talk in detail about some essential tools which financial organisations should implement to protect cyber threats.

Plan and respond:

A strong governing team, with the right level of knowledge, tools, expertise, and involvement at all levels of the organisation is must to efficiently respond to cyber threats. The team must thoroughly understand the risks to their organisation, the tools and its capabilities, and their options in responding before a cyber event occurs. The development of Cyber Incident Response Plan is a necessary step in adequately planning and preparing responses to cyber events. The plan must be very clearly defined for who should take action, what their responsibilities are, and exactly what they should do.

To deal with a cyber security incident, one of the most important actions is to be properly prepared. This helps to recover systems more quickly, minimize the impact of the attack, and increase confidence in organisation customers and even save organisation money in the long term. This first phase is crucial, but can easily be overlooked because of a lack of awareness, support or resources.

To be effectively prepared, organisation should be able to determine the criticality of organisation's key assets; analyse threats to them; and implement a set of complimentary controls to provide an appropriate level of protection. Considering the implications of people, process, technology and information; organisation can then update their cyber security response capability and review its state of readiness in cyber security response.

Protection of assets

A financial organisation should implement adequate protective controls that are in line with best practices of cyber resilience standards to reduce the likelihood and impact of a successful cyber attack on identified critical business functions, information assets and data. Protective controls should be proportionate to and consistent with the organisation's risk tolerance and its threat landscape.

The organisation should consider cyber resilience from the ground up during system and process design, as well as service and product development, in order to minimize the probability of a successful cyber attack. A process to embed resilience by design should ensure that all software, network configurations and hardware, databases etc. are subject to rigorous testing against related security standards. The security tools must be implanted in a way that attack surfaces are limited to the extent practicable.

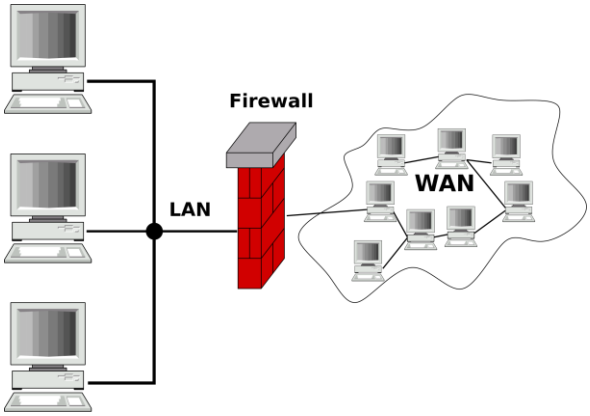
Ten Essential Security tools

Technology towards information security is getting advanced at rapid speed. Forbes has predicted that worldwide Cybersecurity Spending Increasing To $170 Billion By 2020. There are all possibilities that this estimate may increase as the spending is being driven by government initiatives, increased legislation and high-profile data breaches in current year and in future. The security posture of any financial organisation must be well designed and controlled. Its utmost necessary to evaluate all potential threats and surrounding controls in today's dynamically changing cyber environment. By implementing following tools, it will enhance the information security of any financial institution:

1. Firewall
2. Network Access Control (NAC)
3. Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)
4. Advanced Persistent Threat (APT) prevention
5. Anti-Virus / Anti Malware protection
6. Web Proxy & Content Filtering:
7. Security Incident & Event Management (SIEM)
8. Anti - Distributed Denial of Service (DDoS)
9. Data Loss Prevention (DLP)
10. Data Backup and Recovery Solution

I. Firewall:

The primary purpose of a firewall is to filter traffic. Firewalls inspect packets as they pass through, and based on the criteria that the administrator has defined, the firewall allows or denies each packet. Firewalls block everything that you haven't specifically allowed.



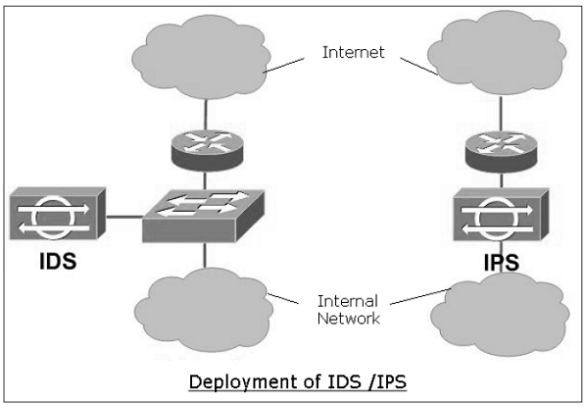
The network level security is managed by state of the art Firewall technology. There are two layers of network security using Multi-layer Firewall Security Architecture. Generally two firewalls deployed in all network i.e. enterprise level Firewalls at the core & perimeter level.

II. Network Access Control (NAC)

Network access control (NAC), is a method to strengthen the security of the network by restricting the availability of network resources to endpoint devices that comply with a defined security policy. A network access server (NAS) is a server that performs authentication and authorisation functions for potential users by verifying logon information. In addition to these functions, it could also implement centralised server system for pushing anti-threat applications such as end-point firewall policies, antivirus software, and Malware and spyware detection programs. NAC also regulates and restricts the things individual subscribers can do once they are connected.

III. Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)

Vulnerability/exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.



IDS and IPS are similar in detection of anomalies in the network. IDS is a 'visibility' tool whereas IPS is considered as a 'control' tool.

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability and exploits. The IPS often sits directly behind the firewall and is provides a complementary layer of analysis that negatively selects for dangerous content.

Intrusion Detection System (IDS) sit off to the side of the network, monitoring traffic at many different points, and provide visibility into the security state of the network. In case of reporting of anomaly by IDS, the corrective actions are initiated by the network administrator or other device on the network.

IV. Advanced Persistent Threat (APT) prevention

An APT is a highly organised, well-coordinated attack against a specific target by usually a large group of people working together and each bringing their own specialized skills to perform the attack. The people behind an APT have an intended purpose for wanting to target a particular entity. Using different methods (either internal or external), the attackers relentlessly attempts to gain access to the network and stay there until they have achieved their objective.

The main targets of an APT attack are commonly those organisations with a large amount of sensitive information (e.g. source code, trade secrets, personally identifiable information (PII), etc.) that will usually help the attacker gain a competitive advantage, identify a weakness or somehow gain an upper hand over the victim of the attack. Financial sector is one of the most attempted sector as attackers can steal vital information to gain financial advantages by using such information for fraudulent purpose.

Various solution available in the market that detects and blocks attacks across Web and email

threat vectors as well as malware resident on file shares. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats. Zero-day, targeted malware enable advanced persistent threats (APTs) to breach IT security, steal/alter/destroy sensitive data, and exploit network resources.

V. Anti-Virus / Anti Malware Protection

A virus is a program or piece of code that is loaded onto the computer without your knowledge and runs against user's wishes. Connecting or surfing the Internet without proper antivirus security can allow unknown viruses, which can infect and damage your computer. Usage of unprotected system, which is connected to the Internet or an email, allows viruses to be spread at lightning speed in a matter of hours; and a single virus is enough to infect your whole network. Malware is an abbreviated term meaning "malicious software." This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner.

Anti-virus security is the prevention that protects a computer from the infection of viruses. A computer and in turn the network has to be armed to protect itself from the attacks of viruses. Antivirus security comes in many different forms. There are antivirus programs, which can help detect and prevent viruses from coming in. Antivirus programs are quite popular in the computing world for their abilities to protect a computer from viruses.

One of the most important factors in the successful protection of your network against viruses is how fast you get new virus engine signature files – those files released by antivirus labs that help to identify a virus when there is a virus outbreak. Then, a critical factor is how fast the signature files of your antivirus solution are updated when a new virus emerges. In every virus attack there is a time differential between the outbreak of the new virus and the release of signatures to defeat and eliminate it. The faster a signature file is created, the less likely the chance of an infection.

Antivirus products often use a mix of technologies to detect and prevent any damages from viruses. The three most common approaches are:

a) Signature files which are prepared and released by antivirus product lab on a regular basis and contain details that help identify a latest virus. Signature files are the usual way antivirus engines are updated on very frequent basis.
b) Heuristics are used to detect viruses and other threats that have not yet had signature files or any vaccination developed for them. Essentially they look at different characteristics of a file, assess the characteristics and flag those that appear to be viruses. This method helps to detect and catch viruses that can mutate which are resistant to signature files.
c) Sandboxing isolates and executes suspicious code in a virtual machine isolated from the rest of the IT infrastructure to determine if it's malicious or not.

While some antivirus or anti malware products combine two or more of these technologies, there is no single best solution. The only effective way to assure the highest level of safety and security is by a multi-layered in-depth defence which can be achieved by using multiple antivirus engines.

VI. Web Proxy & Content Filtering:

A proxy server is a computer that acts as an intermediary between the user's computer and the Internet. It allows client computers to make indirect network connections to other network services. If proxy server is used in the network, client computers will first connect to the proxy server, requesting some resources like web pages, any other resources, which are available from various servers over Internet. Thus it protects internal systems from direct exposure to the external (internet) world.

The content filter analyses all web traffic and blocks selected websites or sites containing viruses. Forbidden sites are selected from a list of categories, which in turn must be downloaded from external sources and stored on the system.

The content filter system allows to create an various user role profiles. A profile is composed by three parts:

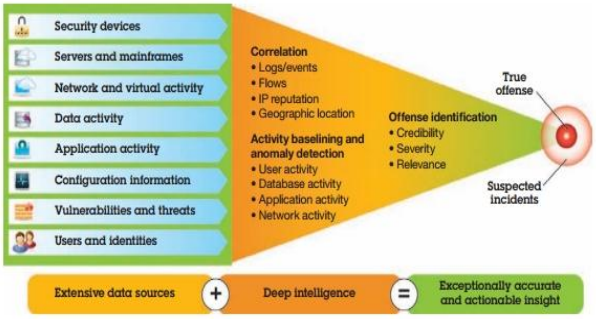
- ***Who:*** the client associated with the profile. Can be a user, a group of users, a host, a group of hosts, a zone or an interface .
- ***What:*** which sites can be browsed by the profiled client..
- ***When:*** the filter can always be enabled or valid only during certain period of times.

VII. Security Incident & Event Management (SIEM)

Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event

collection and the ability to correlate and analyze events across disparate sources.

A SIEM system collects logs and other security-related documentation for the purpose of analysis. Most SIEM systems work by deploying multiple collection agents in a cohesive manner to gather security-related events from end-user devices, servers, network equipment and even specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies.



SIEM combines the essential functions of SIM and SEM products to provide a comprehensive view of the enterprise network using the following functions:

- **Log collection** of event records from sources throughout the organisation provides important forensic tools and helps to address compliance reporting requirements.
- **Normalization** maps log messages from different systems into a common data model, enabling the organisation to connect and analyze related events, even if they are initially logged in different source formats.
- **Correlation** links logs and events from disparate systems or applications, speeding detection of and reaction to security threats.
- **Aggregation** reduces the volume of event data by consolidating duplicate event records.
- **Reporting** presents the correlated, aggregated event data in real-time monitoring and long-term summaries.

VIII. Anti - Distributed Denial of Service (DDoS)

A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

In a typical DDoS attack, the attackers begin by exploiting vulnerability in one computer system and making it the DDoS master. The attack master, also known as the botmaster, identifies and identifies and infects other vulnerable systems with malware. Eventually, the assailant instructs the controlled machines to launch an attack against a specified target.

As DDoS attacks increase both in volume and sophistication, they are increasingly difficult to stop. DDoS perpetrators have shifted their focus from the network layer to the application layer, where DDoS attacks are harder to detect. DDoS attacks are often used as decoys to divert the attention of IT teams away from other simultaneous attacks. Even the largest enterprises today find it nearly impossible to build out sufficient infrastructure to scale in response to a large DDoS attack.

There are solutions available which offers built-in scalability to help the enterprise fend off the largest DDoS attacks, as well as attacks against web applications and direct-to-origin attacks.

Such solutions help to maintain site performance and availability even when confronted with fast-changing threats. Such powerful solution enables enterprises to easily scale to deflect and absorb the largest DDoS attacks, reducing downtime, business risk and costs.

So solutions for DDoS provide real-time network visibility in addition to detection and prevention of Distributed Denial of Service (DDoS) attacks. It helps to protect internet-facing infrastructure from threats and service disruptions by surgically removing network and application-layer DDoS attacks. It defends critical on-premise and cloud infrastructure from attacks while relying on sophisticated filtering technologies to allow legitimate traffic to continue to flow.

IX. Data Loss Prevention (DLP)

Data loss prevention (DLP) is critical to stop accidental and intentional data leaks—whether it's customer information, financial data, intellectual property or trade secrets. Today's enterprise must be able to identify, track, and secure all confidential data at rest, in use, and in motion. This is increasingly difficult due to growing risk factors, including mobile workers and the widespread use of USB drives, webmail, IM, social media and CDs/DVDs.

In addition to obvious data loss methods such as the loss of physical assets such as laptops or USB carrying such data, many data loss incidents are due to accidental disclosure through electronic transmissions. In most cases, end users do not realize the risks associated with sending sensitive data through unencrypted emails, social media sites i.e. Facebook or WhatsApp, webmail and file transfer tools over an Internet. Increased use of mobile devices heightens the risk that unauthorized parties could gain access to sensitive data which has become relatively easy to engage in the spreading of such data.

From a data loss perspective, three standard terms related to the states in the data lifecycle are as below:

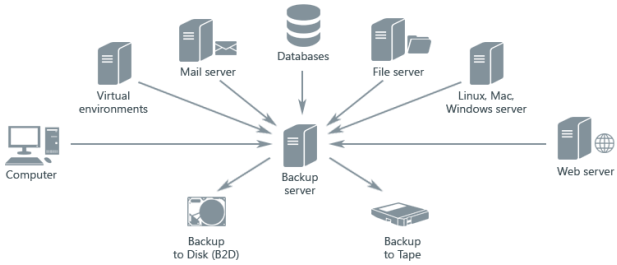
- Data at rest is data that is stored within the IT infrastructure and on media. Common components containing data at rest are servers, databases, file shares, intranet sites, workstations, laptops, mobile devices, portable storage, backup tapes, and removable media. Data at rest can also be stored externally with third parties or through external extensions of the IT infrastructure, such as cloud storage.
- Data in motion is data that is in transit, flowing across internal networks and to the outside world (i.e., data on the wire and in the air).
- Data in use is data that is being accessed or used by a system at a point in time. Examples include data in temporary memory on a local machine, an open report or running query on a workstation, an email that has been drafted but not sent, a file being copied to a USB drive, and data being copied and pasted from one local document to another.

Establishing, maintaining, and demonstrating control over sensitive information assets begins with visibility into where it is stored and how it is being used. Safeguarding classified and designated information requires an integrated effort including solid security policy, sound operational practices and a high level of security awareness in addition to powerful data loss prevention tools.

There are various highly advanced tools available in the market which can be deployed for data loss prevention. These tools work well in blocking unintended releases of sensitive information, and also work just fine in an environment where there are stringent IT controls implemented over the types of email systems and browsers that are being deployed by end users.

X. Data Backup and Recovery Solution

Data is the core currency in today's digital economy. Organisations need to take every practical measure to protect their data. The wealth of the enterprise and the most precious is data, in order to ensure the enterprise's sustainable development and operation, is to protect the computer based information. Human error, the loss of the hard drive, computer virus, natural disaster and so on are likely to cause data loss, cause inestimable losses to the enterprise. For financial system, due to the particularity of the industry, computer systems business data loss is a disaster, can lead to system files, the loss of customer data, business data, business will be difficult to normal. At this time, the key question is how to restore the computer system as soon as possible, make it can run normally.



The data backup is in order to guarantee the data consistency and integrity, eliminate worries about the system users and every stakeholder. Different applications require different solutions to adapt to, in general, a complete backup system solution, need to meet the following principles:

a) **Compatible stability**.
Backup solution's main function is to provide a data protection method, and the stability and reliability of the product which is one of the most important aspects. Firstly, the backup software solution must be 100% compatible with operating system, secondly, when the accident happened, can recover data quickly and efficiently.

b) Solution Support
In a today's complex IT environment, the computer network may include a variety of operating platform, such as UNIX, Windows, VM, and installed a variety of applications, such as ERP, database, and cluster system and so on. Any backup solution must support various operating systems, databases, and typical applications.

c) Real-time performance
Some of the key tasks is non-stop running for 24 hours, and it is likely possible that at the time of backup, there are some files
may still is in a state of opening. So at the time of backup, to take measures, the solution must be capable to to ensure that all the files in the backup system correctly.

With the continuous development of business and multiplication of data every moment, it is utmost necessary that the backup system solution must be capable to use the method of multiple concurrent back up operation of tape recorders or SAN to maintain the effectiveness of business systems.

d) Level of Automation

Many systems due to the nature of work, takes too much of time to finish backup and sometime there are certain restrictions i.e. backup window, time zone issues in distributed network etc. which makes the entire backup process more complex and tedious. So, backup solution should be able to provide a scheduling facility for automatic backup, and use the technology of tape library to automatically change the tape. In large enterprise, Storage Area Network (SAN) is made available to store data backup. The solution should be compatible to take backup and store it in SAN automatically as per defined schedule.

Database systems are the most critical components to safeguard, yet often the most complex to back up and restore properly. Taking very regular backups with definite schedule offers other advantages as well. The backups can be used to create new environments for development, staging or QA without impacting production or even re-creating a fresh production environment in case of massive data loss in production.

Conclusion:

With the verity of actions taken by the Government and Reserve Bank of India, proliferation of banking and financial system had been expanded exponentially in India in recent years. Financial inclusion, Pradhan Mantri Jan Dhan Yogna, Interbank ATM Transactions through National Finance Switch (NFS), Immediate Mobile Payment Service (IMPS) etc. have brought the banking at customer's door step and customers are enjoying greater benefits. Along with the growth in this sector, cyber criminals are now moving beyond computers and deploying very sophisticated techniques and attacking critical networks, websites, mobile handheld devices, such as smartphones and tablets. Cyber attackers have now taken advantage of the increasing popularity of Internet and mobile phone applications by embedding malware into them. Despite the increasing cyber threat risks, many institutions are failed to ascertain risks associated with their technology infrastructure. Cyber threats can be hard to quantify in terms of likelihood and business impact. As a result, many organisations do not fully understand the nature of the threat and tend to inaccurately assume that cyber security is technical issue.

This paper provides essential insights for management to get the basics of cyber security threats, necessary governance and essential tools which any organisation may want to deploy.

Adopting a preventive approach to tackling cybercrime related risks could help to enhanced security with improved value. However, typically requires a cultural shift that starts with high level governance strategy to incorporate cybercrime related risks into the enterprise risk strategy. That will help to start to identify gaps in the current cybercrime risk management strategy and encourage an organisation-wide approach to countering cyber threats. Further, along with the strategic governance, a strong deployment of tools is very much necessary as a preventive approach towards cybercrime risk management. A suggested framework for building a sustainable model for cybercrime risk management is outlined in this paper. There are many tools available in the market today which organisations deploy to prevent cyber risk based on their need and nature of business they are into. However, there are 10 essential tools described in this paper, which any financial organisation must implement to ensure minimum level of cyber security.

References:

1. www.pwc.com/us/en/financial.../cyber-resilient-financial-institution.html
2. http://www.youngzsoft.net/ccproxy/use-proxy-server.htm
3. http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM
4. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sbaSIEM_deployG.pdf
5. http://www.satisnet.co.uk/content/new-year-new-threats-for-q1-labs-to-fix/
6. https://www.akamai.com/us/en/resources/ddos-attacks.jsp
7. www.atlantis-press.com/php/download_paper.php?id=24072
8. http://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#9d11dc876f80