Seminar on Internal Audit

EMERGING TRENDS IN FRAUD PREVENTION AND DETECTION IN CYBER WORLD

CA S. Swaminathan

29/12/2019

Topics covered in Seminar

- ✓ Session 1 : Applying Data Analytics within Internal Audit
- ✓ Session 2 : Enterprise Risk Management
- ✓ **Session 3 : Emerging trends in fraud prevention and detection in cyber world**
- ✓ Session 4 : Soft Skills and Stakeholder Management

What is Cyber

- The word “CYBER” is derived from the word “CYBERNETICS”, which means, “*the scientific study of communication and control, especially concerned with comparing human (and animal) brains with machines and electronic devices*”

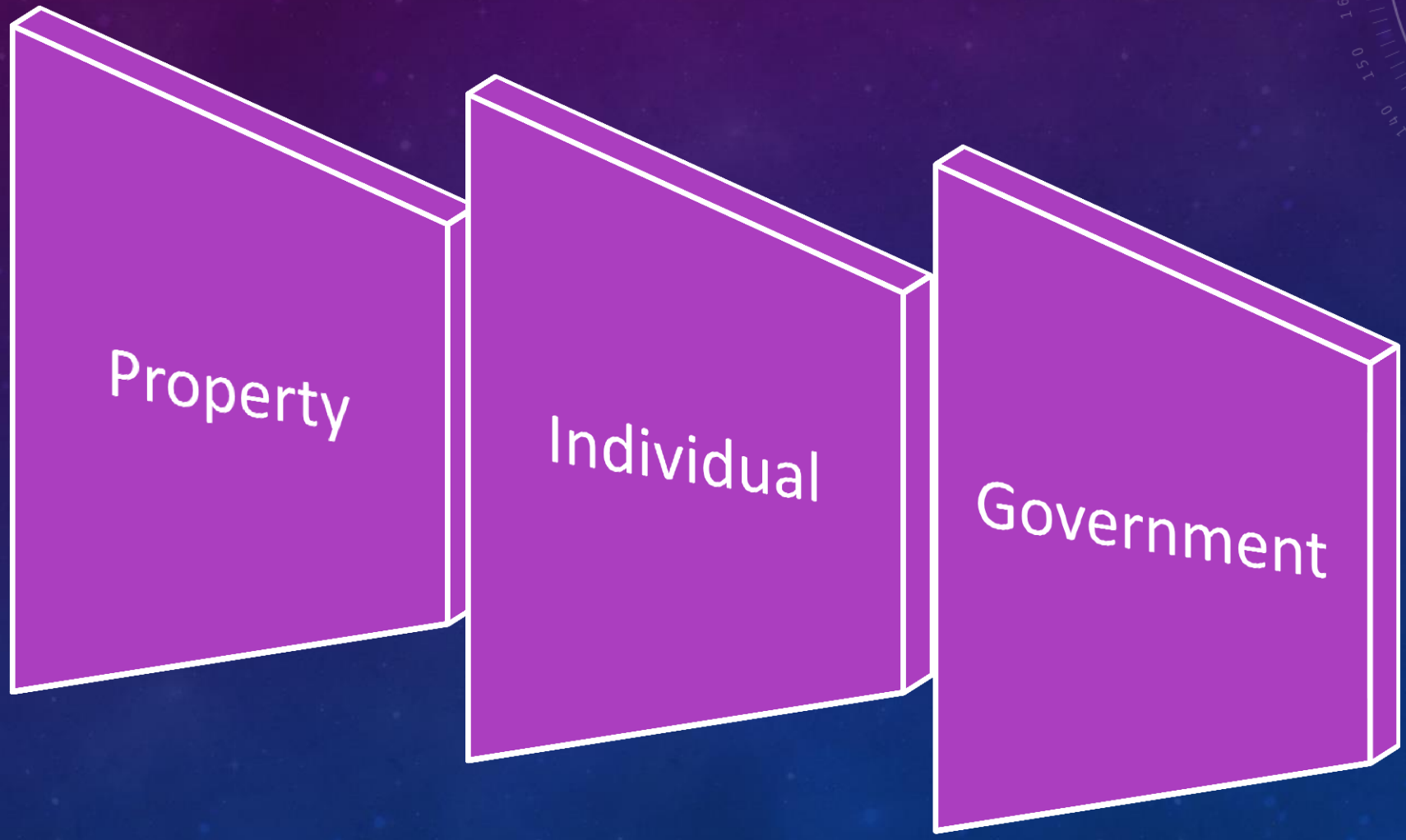
What is Cyber crime

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offence.

A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online.

Categories of Cyber Crime

There are three major categories that cybercrime falls into:

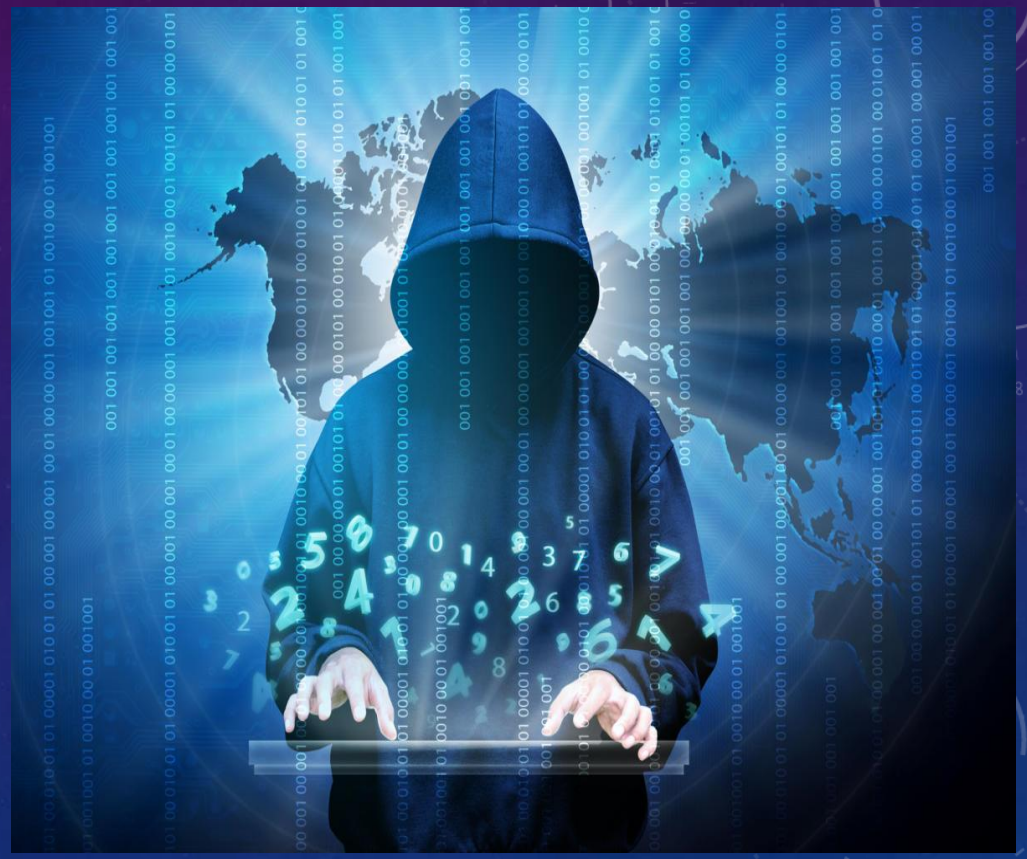


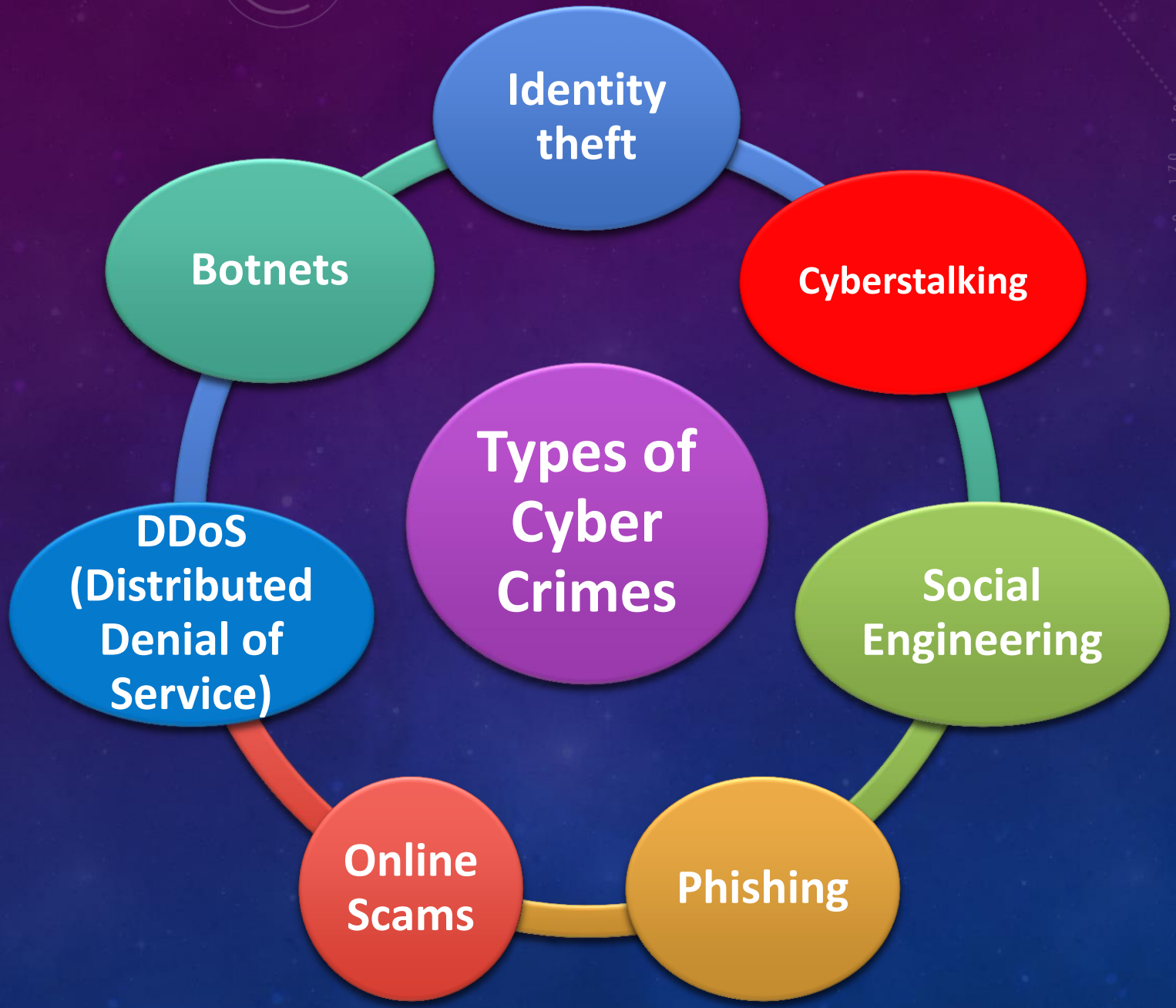
Categories of Cyber Crime

- **Property:**
  - ✓ Hacker stealing a person's bank details or card details thereby making purchases online without individual's knowledge.
  - ✓ Using a malicious software to gain access to a web page which contains confidential information.

- **Individual:** This category of cybercrime involves one individual distributing malicious or illegal information online. This can include cyberstalking, and trafficking.

- **Government:** This is the least common cybercrime, but is the most serious offence. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. which are usually done by terrorists or enemy governments of other nations.




Types of Cyber Crimes
Identity theft
Cyberstalking
Social Engineering
Phishing
Online Scams
DDoS (Distributed Denial of Service)
Botnets

Identity Theft

- This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information.
- They can also open an internet account in your name, use your name to plan a criminal activity or can claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.

Cyberstalking

- This involves online harassment where the user is subjected to a plethora of online messages and emails.
- Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety

Social Engineering

- Involves criminals making direct contact with you usually by phone or email to gain your confidence and usually pose as a customer service agent so that you'll give the necessary information needed.
- Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

Phishing

- Involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer.
- Cybercriminals are becoming more established and many of these emails are not flagged as spam.

Online Scams

- Usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are “too good to be true” and when clicked on can cause malware to interfere and compromise information.

DDoS Attacks (Distributed Denial of Service)

- Used to make an online service unavailable and take the network down by flooding the site with traffic from multiple sources.
- The hacker then hacks into the system once the network is down

Botnets

- Botnets are networks from compromised computers that are controlled externally by remote hackers.
- The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.
- Cybercriminals initially gain access to these devices by using special Trojan viruses to attack the computers’ security systems

Cybersecurity Statistics

- ✓ Warren Buffet says that cybercrime is number one problem of mankind, bigger than nuclear weapons.
- ✓ Total cost of a Cybercrimes in 2021 - approx. $ 6 trillion. (more than the global trade of drugs).
- ✓ Cybersecurity spend - $96 Billion in 2018, to reach $ 1 trillion in 2021.
- ✓ Global Ransomware alone cost $5 billion

Technology Landscape

- ✓ Pace of digitization of financial transactions in India continues to gather pace.
- ✓ Estimated that noncash payment transactions, which today constitute approximately 22 % of all consumer payments, will overtake cash transactions by 2023. It is estimated that the total payments conducted via digital payment instruments will be in the range of USD 500 billion by 2021, which is approximately 10 times of current levels.
- ✓ Technology infrastructure continues to build up, with 100 Crore mobile connections in the country, of which 24 Crore are of smartphone users. The number of smartphones is expected to increase to 52 crore by 2021.
- ✓ Approx 90 percent of all devices are internet enabled and the number of internet users is set to double to nearly 650 million by 2020 from the erstwhile 300 million in 2015.

Cyber Security Issues

- ✓ Sharing and transmitting personal information repeatedly by individuals for various activities making it vulnerable to misuse their data. Aspects such as the purpose for collecting personal information, how will this information be used, security mechanisms put in place for protecting such information, for how long will this information be stored and what will be the procedure for destroying such information, are not known
- ✓ Affect businesses across sectors and irrespective of sizes
- ✓ Consequences include business disruption, regulatory fines, and most importantly reputational damage. If “T” becomes silent in “TRUST”, “R” is on stake. “T” here means “Technology” and “R” means “Reputation”.
- ✓ Potential risk is not just within a single business but in the whole supply-chain
- ✓ Potential risk is from round the globe and may involve organized criminals, as well as careless employees.

Factors impacting cyber security

Less awareness amongst individuals: Awareness amongst internal employees remains the first line of defense. However, not many firms invest in training and improving the cyber security awareness levels within the enterprise.

Budget constraints and little support of Top Management support: Budgets are usually driven by business demands and low priority is accorded to Cyber security. Top Management focus also remains a concern, support for cyber security projects are usually given low priority. This is primarily due to the lack of awareness on the impacts of these threats.

Social Media: Growing adoption of social media leads to more potential for hackers to exploit. Many a user puts the data out for anyone to see, which can be potentially exploited to attack the user's organization. Use of social media to propagate fake news can impact reputations in an insidious manner.

Poor Identity and Access Management: Identity and access management is the fundamental element of cyber security. In an era where hackers seem to have upper hand, it requires only one hacked credential to gain entry into an enterprise network. Despite some improvement, there remains a lot of work to be done in this area.

Mobile phones and Apps: As organizations move towards adopting mobile phones as its preferred channel for doing business, it also becomes the ideal choice for hackers to exploit as the base increases. Since financial transactions can be done on mobile apps, the mobile phone is becoming an attractive target leading to an increase in mobile malware.

Probable Solutions

- ✓ Become vigilant when browsing websites.
- ✓ Flag and report suspicious emails.
- ✓ Never click on unfamiliar links or ads.
- ✓ Ensure websites are safe before entering credentials.
- ✓ Keep antivirus/application systems up to date.
- ✓ Use strong passwords with 14+ characters.
- ✓ Moving towards integrated security, where all components communicate and work together, is essential.

Probable Solutions

- ✓ **Protect information**: The traditional approach has been to protect systems which hold the data. With data being available in different forms (structured /unstructured) and being stored on multiple devices and in the cloud it becomes imperative to change the paradigm. In addition to keeping systems secured, it is recommended to secure the information/data such that the security remains and travels with it at all times.

- ✓ **Investing in technology to ensure protection:** Organizations must invest in technology that can recognize and prevent the practices and actions used in exploits.

- ✓ **Security as a cost vis-a-vis to security as a plus:** The mindset of seeing security as a cost needs an overhaul. The risks associated with security threats and the potential impact to business should make organizations see the benefits of proactive security.

- ✓ **Prioritize risk based security:** Risks are dynamic and 100% prevention is not possible / not realistic. A risk-based approach gives a clear roadmap for the organization to focus its effort and investment where it matters. It is prudent to classify the risk associated with each system and focus on the efforts accordingly.

Initiatives

Cyber Security: To enhance the trust and reliability of Organization's infrastructure for assurance and resilience

Research and Innovation: To empower Organization through creative technology solutions based on research, and by tapping the synergy among key stakeholders

Systems Audit: To support validation and enforcement of regulatory guidance on cyber security, through excellence in audit, analytics and forensics

Project Management: To leverage lean and agile development capability for creating and operating reliable and empowering systems, and delivering delightful user experience.

Cyber risk - Roles and Responsibilities

First Line of defense (with Business and IT Functions}

- Include risk informed decision making into daily operations
- Define accepted risk level and escalate risks outside tolerance level
- Perform risk mitigation procedures as appropriate

Second line of defense (IT Risk Management function)

- Establish risk governance including policies and standards
- Implement risk mitigation tools, procedures and monitor
- Provide risk oversight

Third line of defense (Internal Audit)

- Assess program effectiveness independently
- Report to Board on risk management effectiveness
- Comply with Security and Exchange Commission requirements and disclosure obligation related to cyber security risks

Cyber risk - Steps by Internal Audit

- ✓ To develop a cyber security strategy and policy by working with Management and Board of Directors.
- ✓ Identify and act on opportunities to improve the organization's ability to identify, assess and mitigate cyber security risk to an acceptable level.
- ✓ Assess and mitigate potential threats that could result from the actions of an employee or business partner by recognizing that cyber security risk is not necessarily only external
- ✓ To heighten awareness and knowledge on cyber threats by leveraging relationships with the Audit Committee and Board thereby ensuring that the Board remains highly engaged with cyber security matters and up to date on the changing nature of cyber security risk.
- ✓ Ensure that cyber security risk is integrated formally into the audit plan.
- ✓ Develop and keep current an understanding of how emerging technologies and trends are affecting the company and its cyber security risk profile.

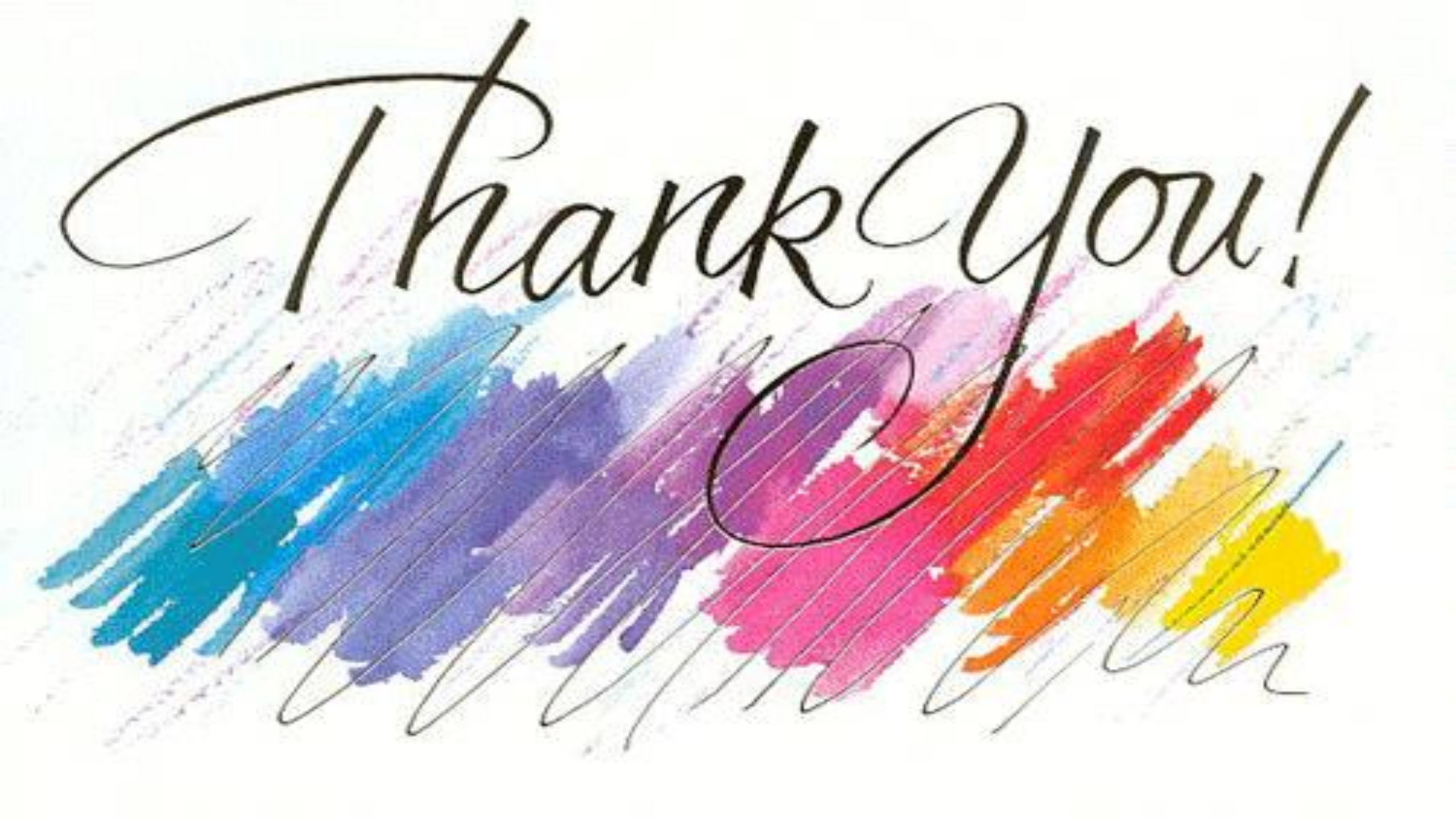
Cyber risk - Steps by Internal Audit

- ✓ Emphasize that cyber security monitoring and cyber incident response should be a top management priority; a clear escalation protocol can help make the case for—and sustain—this priority.

- ✓ Address any IT/audit staffing and resource shortages as well as a lack of supporting technology/tools, either of which can impede efforts to manage cyber security risk

Conclusion

In this competitive world, there are challenges of securing information and protecting financial assets of the citizens. This is a battle to be fought on various fronts and it is essential to plan well, exercise rigorously and execute flawlessly by taking a collaborative approach, which will reduce the cost of business without compromising quality, trust and reliability.


Thank You!