Ransomware and Related Cybersecurity Matters - Impact on Audit

Cyber security in today's day and age is a matter of utmost importance and necessity with internet touching all aspects of our life. The recent ransomware attacks are a glaring reminder of how vulnerable our systems are to these breaches. In such a scenario, Chartered Accountants have an added professional duty to analyse the cyber risk faced by an audit client like any other business risk. Read on to know more….

Ransomware- Evolving Effects of Cyber risk

On May 12, 2017, a massive ransomware cyber attack caused major business impact across the globe, affecting organisations in almost every sector. Ransomware is a type of computer malware that encrypts files, disks and locks computers. The hacker then demands a ransom for decryption tool which has to be paid within a stipulated time in the form of bitcoins.

WannaDecrypter2.0 ransomware is a fast spreading ransomware that started its assault against hospitals across the UK before spilling across the globe.

The frequency and severity of such cyber attacks are continuing to increase. Cyber security is not just an "IT issue" or a matter that results only in information loss. It affects an entity's reputation and has resulted in theft of protected or sensitive information (e.g., intellectual property, credit card information, personally identifiable information [PII]) and disruption of computer-controlled operations or access to online systems, and can require significant financial costs to remediate the breach. It is a broad business risk affecting most entities.

As these attacks continue to evolve, so will their effect on the organisation as a whole. While many of the recent, highly publicised attacks/breaches do not appear to have been directly targeted at financial systems, the access gained by the attackers provided them the ability to:

- Manipulate or modify financial records, such as billing/cost/ interest rates
- Modify key automated business rules
- Modify automated controls relied upon by the management.

Market Response to Growing Cyber Risks and Assessing Auditor Responsibilities

Various interested parties are concerned about entities' abilities to appropriately deal with cyber attacks and breaches:

- **Various organisations** are issuing guidance to help improve cyber preparedness (e.g., FFIEC, FISMA, ISACA, NERC, NCSC and MeiTY in India, etc.)

(Published by Digital Accounting and Assurance Board (DAAB) of ICAI with contributions from CA. Sanjay Vasudeva and CA. Subh Ghosh. Comments can be sent to gdaab@icai.in.)

- **IS Auditing Standards** provide audit professionals with necessary guidance and information in this respect. Examples – ISO 27001, NIST, COSO framework, COBIT, etc.
- **Securities regulators** across the world continue to highlight the importance of the issue in announcements:
  - **Securities Exchange Board of India (SEBI)** has set up a panel on cyber security to suggest measures to safe guard the capital markets from such attacks.
  - **Securities Exchange Commission (SEC), US**, has stated that "Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cyber security events and have clear procedures in place rather than waiting to react once a breach occurs." (SEC, US September 2015)
- Audit committees/Boards are expected to have an appropriate understanding of the business implications of cyber risks.
- Significant investors and customers/consumers are asking for more transparency into an entity's cyber risks and processes as well as privacy and how Personally Identifiable Information (PII) is handled.
- Business partners want to understand the adequacy of entities' cybersecurity risk management program before connecting systems.

Assessing Auditor's Responsibilities

From audit perspective, the primary focus continues to be on access controls and changes to systems and data that would impact the financial statements and the effectiveness of internal control over financial reporting (ICFR).

Auditor should consider whether cyber risk (like other business risks) represents a risk of material misstatement to the financial statement as part of the audit risk assessment activities. Focus should be on understanding the cyber risks affecting the entity and the actions being taken to address these risks.

In relation to cyber security threats which could impact the IT systems of the entity, the key focus for auditors should be on controls and systems, which directly impact the data that is used and relied upon in the audit. In situations where material cyber security related breach is discovered, the auditor would need to consider the impact on financial reporting, including disclosures, and the impact on ICFR.

Cyber Security Breach and Audit Risk Assessment Strategy

Auditor may adopt following audit risk assessment strategy for cyber risks -

- Obtain a high-level understanding, primarily via inquiry, of the processes and controls implemented by the entity to manage cyber risks, including:
  - Privileged account access
  - Governance/Risk management program
  - Security monitoring/Incident management program
  - Security awareness program
  - Threat and vulnerability management program
  - Patch management program
  - Vendor risk management program
  - Data classification program
- Evaluate the information obtained to assess the risk of material misstatement to the financial statements.
- Communicate relevant observations for strengthening the cyber control environment, as appropriate to the management and Audit Committee.

Suggested approach when a breach comes to attention are as follows :

- Gain an understanding of management's approach to investigating the breach;
- Evaluate the actions taken by management in response to the investigation;
- Assess the effect of the breach on the audit.

Notification of Cyber Security Breaches

Management should establish protocols to provide auditors with timely notification of a cyber security breach with potential material implications to the financial statements. They should consider updating the incident response plan to include a step to notify auditors and disclosure committees responsible for public filing.

Breach Significant to the Entity's Financial Statements

It is not necessary that all breaches are significant to the entity's financial statements. A breach that results in either or both of the following may potentially be significant:

(i) *Extraction of Protected or Sensitive Information*
Breaches that could result in impairment of assets; fines, penalties and lawsuits requiring the recording of material liabilities and/or commitment and contingency disclosures in the financial statements. Examples include information related to intellectual property, credit card, PII, customer data.

(ii) *Modification of Financial Applications or Information*
This would include breaches that could affect the accuracy and/or integrity of financial information. Examples include changes to key business rules, automated controls or billing, cost or interest rates.

Common Areas Exploited in Cyber Attacks

In evaluating the root cause/attack approaches being used by attackers in a number of recent highly publicised attacks, some common themes were identified as follows:

Common Attack Approaches	Cyber Risk Area	Effects
Privileged accounts were not adequately protected (especially system accounts)	Privileged account access	Facilitated the attacker's ability to deepen and broaden the breach
Exposure to social engineering attacks	Security awareness program	Enabled attackers to gain a foothold in a target's system
Depth and quality of event monitoring did not keep pace with evolving attack vectors	Security monitoring/ incident management program	Attackers structured their attacks to avoid detection via historical controls (e.g., violation monitoring)

Common Attack Approaches	Cyber Risk Area	Effects
Quality of threat and vulnerability management programs not keeping pace with evolving risks	Threat and vulnerability management program	Lack of effective responses to address new/evolving threats
Lack of timely, comprehensive patching of technologies	Patch management program	Issues are being exploited to deepen and broaden the breach (e.g., initiate a ransomware attack)
Inadequate evaluation and testing of vendor access to client systems	Vendor risk management program	Excessive/extraneous vendor access being exploited (weakest link)
General lack of clarity and prioritisation around the higher-risk areas of the entity and the level of protection needed	Data classification program	Critical information was not being adequately protected

Understanding Action Taken By Management

Cyber risk area	Example considerations when understanding the actions taken by management in developing audit strategies

Privileged Account Access	• Determine the controls for account provisioning (system and human accounts)
	• Determine how management assesses ongoing appropriateness (system and human accounts)
	• Determine management's process for identifying whether:
	  • An account with privileged access has been hijacked (e.g., monitoring behavior)
	  • Fictitious accounts with privileged access have been established (system and human accounts)

Cyber risk area	Example considerations when understanding the actions taken by management in developing audit strategies
Governance/ risk management program	• Determine how management periodically assesses and evaluates its cybersecurity program for effectiveness • Determine whether management engages third parties to perform attack and penetration or other cyber assessments and understand how management evaluates and responds to results
Security monitoring/ incident management program	• Determine how management would know if the entity was under a cyber attack, if a breach significant to the entity had occurred, or if a user's account had been hijacked • Determine whether a security incident response plan has been developed and tested
Security awareness program	• Understand what programs are in place (audience, frequency, topics, trainings, etc.)
Patch management program	• Determine how management identifies, evaluates, prioritises and implements software patches issued by software vendors • Determine how management monitors the patch status of key technologies to work towards consistent deployment
Vendor risk management program	• Determine how vendors connected to the IT environment are identified • Determine how the risk associated with each vendor connected to the IT environment is assessed
Data classification program	• Determine how data classified as "most critical" to the entity is protected • Determine how management would know if information critical to operating its business and/or maximising its advantage in the marketplace was accessed, stolen or destroyed

Cyber risk area	Example considerations when understanding the actions taken by management in developing audit strategies
Threat and vulnerability management program	• Determine how new and evolving threats to the IT environment are identified • Determine whether the adequacy of the response procedures to those threats deemed credible • Understand what processes exist to classify and remediate vulnerabilities

Developments in IT framework and Changing Audit Response

Following are some examples of suggested changes in audit response with regard to developments in IT framework -

Areas	Example considerations in developing audit response
Blockchain A distributed database/ ledger that maintains a continuously growing list of data records (public and private) put together in encrypted blocks. The technology creates a concrete transaction record and transaction integrity.	Working across the organisation on helping entities understand the impact of blockchain. Assessing the audit impact of blockchain and developing new techniques to audit a blockchain.
Artificial Intelligence (AI) Application of IT security and computing systems that exhibit some form of human intelligence.	Investigating the use of AI in the audit process and related research capability.
Ethical hacking and related IT based strategies	Internal and external penetration testing, Limited vulnerability assessment, Social Engineering.
Data Analytics	Helps identify trends and anomalies in processes and controls helping direct investigative effort in the right areas.

Cyber Attestation

Cyber Attestation should be based around development and issuance of:

- A framework for cyber risk management program reporting, including principles and criteria for evaluating entity-wide cyber risk management programs;
- An attestation guide for engagements related to those programs;

This would contribute to improved management communication of and confidence in information about entities' cyber risk management programs.

This could potentially provide principles and criteria that can be used by:

- Practitioners who will be providing attestation reporting services and also to those who will be providing advisory services to entity's that require remediation assistance.
- Entity officials in developing its cyber risk management programs and assessing the effectiveness of its existing programs.
- Auditor and other stakeholders for developing materials to build on the implicit cybersecurity aspects.

Suggested areas to be considered are as follows:

- The form and content of the report
- Intended users of the report–may change over time
- Balancing flexibility with comparability
  Guidance and criteria are expected to evolve; especially as the materials are further vetted by various stakeholders (e.g., regulators, industry associations, IT groups).

As a next step, entities should consider the following:

- If not already occurring, establish a process to actively monitor cyber-related legislative and regulatory activities that affect the entity directly – as well as those affecting its clients and business partners, as such requirements may ultimately pass through to the entity.
- Consider having a pre-assessment of the cyber risk management program performed, especially of those areas that have not been subject to previous audit scrutiny.
- For some companies, significant remediation activity may be required to address identified gaps.
- Early identification of these gaps is essential to plan and execute remediation activities in an efficient, balanced and cost-effective manner.

Conclusion:

The auditor while drawing conclusion from the audit procedures conducted should consider the following scenarios:-

Conditions affecting the entity, and business plans and strategies that may not affect the risks of material misstatement:

- If anything significant [not affecting the risk of material misstatement] comes to the notice of the auditor with regard to breach of cyber security, the auditor should provide those charged with governance with timely observations arising from the audit that are significant and relevant to their responsibility to oversee the financial reporting process.
- The communication should clearly state the details of deficiencies observed in internal control with regard to cyber security and recommendations for improving the same.
- Reference in this regard may be drawn to the Auditing Standards, SA 260 and SA 265.

Conditions affecting the entity, and business plans and strategies that may affect the risks of material misstatement:

- If anything significant [affecting the risk of material misstatement] comes to the notice of the auditor with regard to breach of cyber security the auditor should modify the opinion in the auditor's report if he concludes that, based on the audit evidence obtained, the financial statements as a whole are not free from material misstatement; or he is unable to obtain sufficient appropriate audit evidence to conclude that the financial statements as a whole are free from material misstatement.
- The auditor should also provide those charged with governance with timely observations arising from the audit with regard to breach of cyber security that are significant and relevant to their responsibility to oversee the financial reporting process; and the circumstances that led to the expected modification and the proposed wording of the modification.
- Reference in this regard may be drawn to auditing standards SA 260, SA 265 and SA 705. ■

Just when the caterpillar thought the world was ending, he turned into a butterfly. - Proverb