Marg
The Business Backbone
Marg ERP 9+

You Want Your Customer's Business To Grow

We want you to be empowered

Ease out Accounting & Auditing with Marg

- Statistical Financial/ GST Return reports for Internal Audit
- Data Freeze Management
- Automatic RCM Entry in one click
- Frequent Voucher Entry Option
- Get 100% Customised GST Invoice and returns in Excel/ CSV and JSON format
- Auto-Update of GST amendments

Now With

BANKING INSIDE ERP

A Single Interface for Accounting, Inventory & Banking

www.margerp.com | 9599 336 503 | info@margerp.com

Cyber Security and Accountants

The monetary administrations part of any organisation has customarily been seen as exceptionally developed with regards to cyber security activities. In recent times, the money related division had the most astounding Security Rating of all inspected enterprises. However, despite the fact that organisations in the monetary division have been talking about the need of observing cyber security for a long while, the danger scene is continually advancing—prompting a more intricate digital biological community consistently. This makes everything the more basic to be proactive with regards to cyber security issues. While financial services' is seen as a mature sector when it comes to cyber security, it's also a major target due to the nature of the relevant data. With that in mind, it's important for those in the industry to be well-versed on those areas with the greatest threat potential. Of those—including third-party risk—are outlined in this article.

Credible Cyber Security Threats to the Financial Service Sector

1. **Third Party Cyber security Risk:**

   The danger of outsider cyber security—and the subject of how proportional your cyber security program to all the more nearly screen your sellers' security stances—poses a potential threat in the budgetary administrations segment of any organisation. Does your association have the capacity to consistently screen every merchant you work with? Do you have a framework for teaming up with sellers (and working together inside) on cybersecurity measures and figuring out what should be possible to secure your information? It's important to have the capacity to quickly recognise and remediate issues if required. So, having a non-stop observing instrument will give you genuine feelings of serenity.

2. **Widespread Business Operation Risk:**

   For budgetary administration associations that work at a global level—or just work

CA. Sachin Dedhia

(The author is a member of the ICAI. He can be reached at eboard@icai.in)

eMerge

A robust software solution

Financial consolidation

Statements as per IND-AS, IFRS and other GAAPs

Financial performance analysis and graphs

Budget vs Actual reports

Quick implementation

For more features and case studies, please visit www.emergeconsol.com
To set up a demo, call Prakash +91 99604 77889 or
send email to sales@emergeconsol.com

across the geographic territory—the risk of cybersecurity issues increments. Huge finance related organisations around the globe need to consider extra cybersecurity hazards over their centre points of business.

3. **Open Ports:**

   Open ports are generally not risky by nature; however, when touchy data exists, is overseen, or is exchanged through those ports, the potential for a break rises. One of the establishments of the WannaCry ransomware assault was the open port 445.

   While essentially having great system cleanliness is imperative, it is basic to have a strong arrangement set up for port administration. Money related administration ventures specifically have a great data to lose on the off chance that they are not watchful with open ports on their system or the system of their trusted third parties.

4. **Fourth Party Cyber Security Risk:**

   It has been recently uncovered in a number of cases that the finance related divisions of many organisations were not sufficiently checking their fourth parties. Fourth-party cyber security—observing the security of your sellers' outsiders—is a dependable risk to each association.

   Suppose one of your fourth parties is influenced by a ransomware assault that makes them disconnected for a significant period of time. In that case, much of the issue with this risk is that numerous associations will not be aware of their fourth parties.

   Since cyber security dangers like these can possibly affect the impact of your organisation, your techniques for overseeing them should be considered all the time. To keep away from the above-mentioned cyber security dangers, you should comprehend and consider the cybersecurity ramifications of the sellers you work with (and the merchants they work with), the spots you work together in, and how well your system security is arranged.

Threats to Mid-Size & Small Firms

One of the threats that have gained prominence is *Ransomware attacks* with even small & mid-size firms falling prey to such attacks. Ransomware attacks happen because of the use of open source free software whose servers are infected. It also happens when an employee opens an unwanted excel file which has got macros enabled in it, thereby infecting the entire network. One of the best solutions to Ransomware attack is to have a good back up strategy thereby ensuring the availability of the data even if there is a Ransomware attack.

One of the threats that have gained prominence is *Ransomware attacks* with even small & mid-size firms falling prey to such attacks. Ransomware attacks happen because of the use of open source free software whose servers are infected. It also happens when an employee opens an unwanted excel file which has got macros enabled in it, thereby infecting the entire network.

A chartered accountant firm will need to arise and secure against the dangers of cyber-attacks as a CA's firm has a lot of data of their clients. Genuine software, updated anti-virus & a good backup solution will help mitigate this risk to a great extent.

Regulators like RBI, SEBI & IRDA are demanding cyber security audits to be conducted on a regular basis for companies. A DISA qualified CA can easily undertake such audits.

A chartered accountant firm will need to arise and secure against the dangers of cyber-attacks as a CA's firm has a lot of data of their clients. Genuine software, updated anti-virus & a good backup solution will help mitigate this risk to a great extent. Regulators like RBI, SEBI & IRDA are demanding cyber security audits to be conducted on a regular basis for companies. A DISA qualified CA can easily undertake such audits.

In future, in case of war between two countries, it is said that it will also be a cyber-war where countries instead of sending soldiers will first attack the financial stability of the countries, bank balances will be changed and BFSI will come under pressure. Hence, we are now seeing regulators like RBI, SEBI & IRDA demanding cyber security audits to be conducted on a regular basis for companies. ■