Protect Your Practice Against Information Security Threats

CA Pranay Kochar

B.Com, F.C.A, P.G.D.I.T., CISA, DISA (ICAI), CEH, ISO 27001 LA, Dip. Cyber Law"

KOCHAR CONSULTANTS

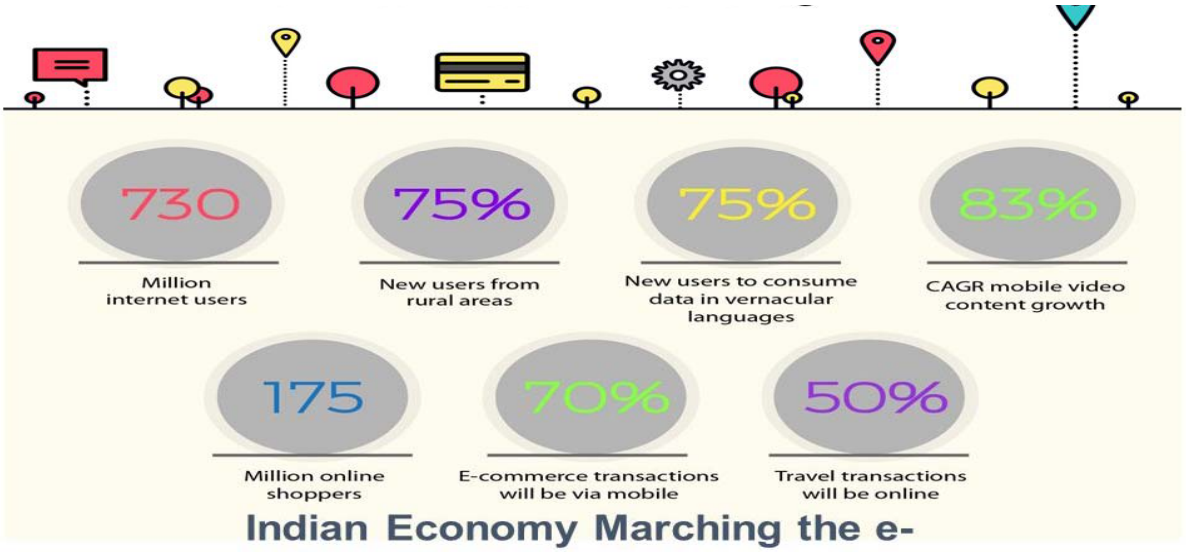
Essence of IT Security

INFORMATION SYSEM AUDIT | IT CONSULTING | IT GOVERNANCE & COMPLIANCE

DISCLAIMER

- This presentation is made on a best effort basis. No representation or warranties are made by J.B. Nagar CPE Study Circle with regard to the speakers presentation.
- Views expressed by the speaker are his own views and do not represent the views of J.B. Nagar CPE Study Circle.
- The logos, domain names and service marks are the registered and unregistered marks of their respective owners and are used only for representative purpose.
- The audience is expected to perform their own due diligence before taking any action based on the discussion during the sessions.

THE INTERNET IN INDIA BY 2020



DSCI PROMOTING DATA PROTECTION

3

Source: The Future of Internet in India, NASSCOM

A NASSCOM® Initiative

IT REVOLUTION

IT has extremely revolutionized:

- The way business is being done : e-payments, advertisements, online purchases.
- Retail businesses done across the globe : Amazon, Flipkart
- MIS reporting
- The way business correspondence is being done
- Methods of information exchange between the firms and their clients: email, chats, blogs..

This has led to increased risk of data theft and associated cyber security risks.

TRADITIONAL ROLES OF A CA

- Accounting
- Auditing
- Direct Tax Compliances
- Indirect Tax Compliances
- Company Law Compliances
- Consultancy services

INFORMATION TECHNOLOGY AND TRADITIONAL ROLES

Accounts & Compliance
- On software like Tally or SAP or Excel
- Robotic Process Automation
- Block Chain
- Cloud Accounting

Taxation
- E-filing income tax returns
- E-filing GST returns
- Online tax payments

Auditing
- Computer Aided Audit Techniques
- Artificial Intelligence / Machine Learning

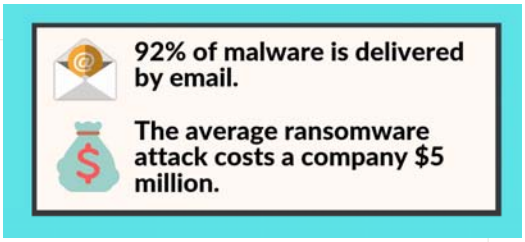
IMPORTANCE OF CYBER SECURITY

- Firms are trusted with some of the most intimate personal and financial information of their clients
- Hackers are continually trying to get their hands on such critical, private information
- Understanding cyber security basics ensures not only the safety of client information, but also the longevity of the firm

Can your firm get hacked in the same way that any larger financial institutions may have been?

The short answer is YES!

IMPACT OF CYBER ATTACKS

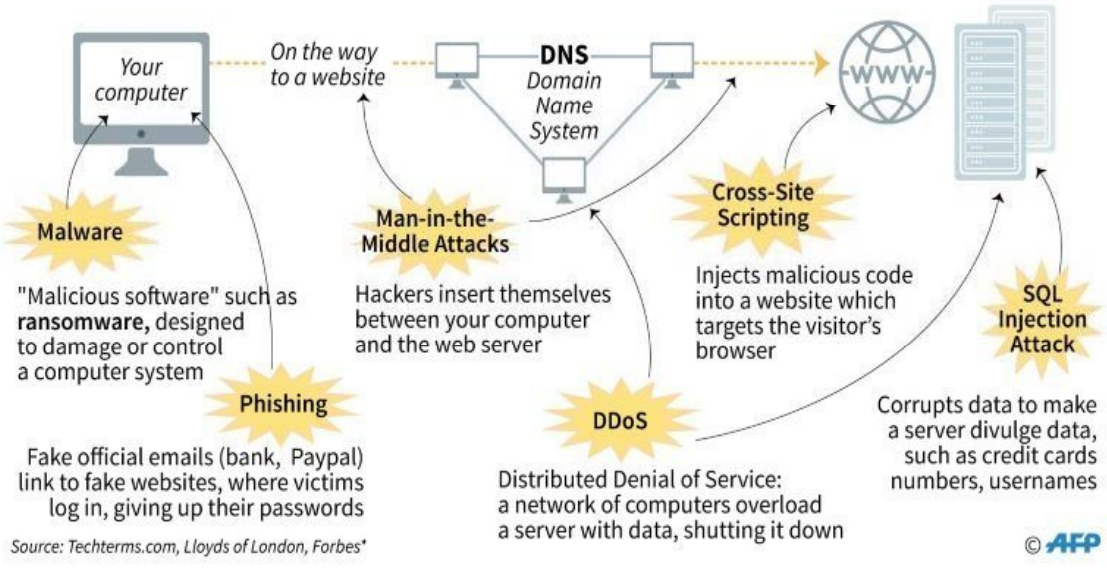


Cyber-attacks may impose:

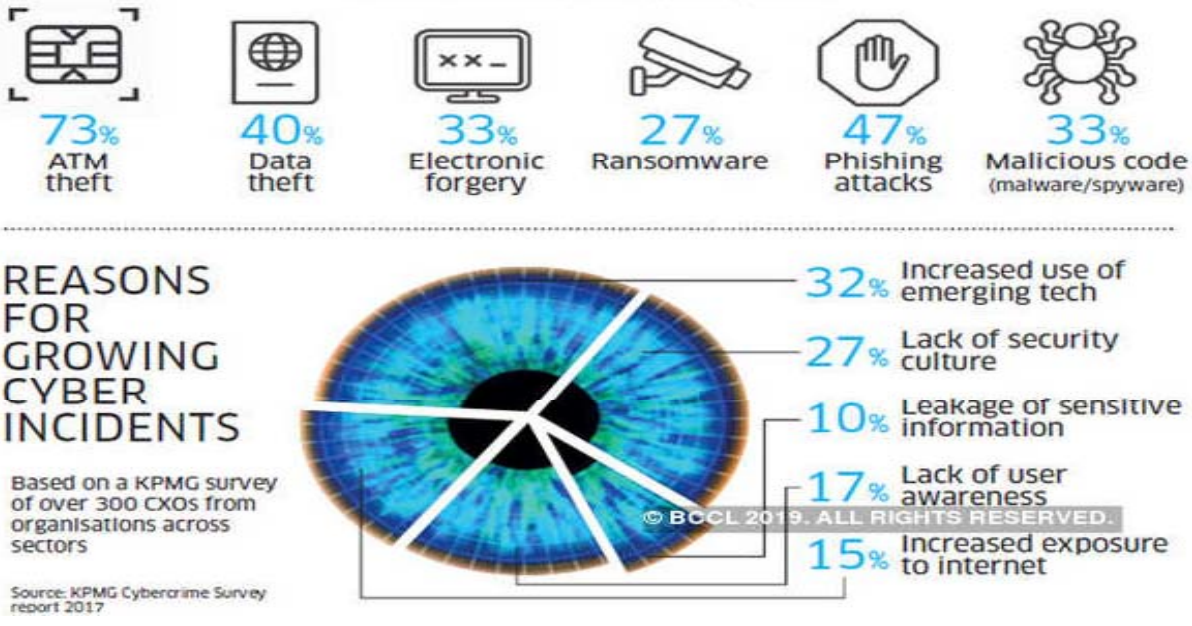
- Regulatory actions,
- Negligence claims,
- Inability to meet contractual obligations
- A damaging loss of trust among clients and stakeholders.
- Commercial losses,
- Loss of reputation,
- Disasters,
- Disruption of operations and sometimes even business closures.
- Small breaches if not addressed adequately could lead to un-surmountable disasters

TYPES OF CYBER ATTACKS

Cyber crime worldwide cost $400 billion in 2015 and is forecast to reach $2 trillion in 2019*



TOP CYBER CRIMES IN INDIA



Why CA firms are at high risk for Cyber Attacks

THE CHALLENGES

Cybercriminals usually target small and medium sized accounting firms:

- They give relatively lesser emphasis to data security, controls, and risk evaluations; they are therefore more vulnerable than bigger firms.
- They don't have enough staff in the IT function, and not all staff have the mastery to spot these issues, which can prompt further risks.
- The senior partners are especially at risk since they are both effortlessly identifiable on the web, and are most likely to conduct online banking transactions for their practices.

Firms Hold Massive Private Data

- Firms hold top to bottom information as privileged data from HNI clients or organizations.
- Tax documents, financial records, PAN, and direct-store data, accountants may also serve as sources for years of private data.
- Some firms hold virtually complete individual accounts of their customers, transforming these practices into important targets.

Firms Have Productive Corporate Information

- Firms deal exclusively with financial and tax documents, and related personal and business documents, different practices handle high-stakes corporate issues.
- Firms that deal with mergers, acquisitions, and corporate rebuilding frequently, hold data that might be of considerably more noteworthy enthusiasm to cybercriminals.

FIRMS DO NOT ASSESS SECURITY RISKS

- Unlike large accounting businesses, small and medium firms often do not implement robust security strategies.
- Cyber criminals execute malware attacks by targeting small and medium accounting firms by taking advantage of inadequate data security.
- The security risk assessment will help the firm to check the nature of client data being accessed by each employee and assess the effectiveness of the employee's device to prevent targeted security attacks.
- Risk assessment will help the firm to evaluate and improve its security strategy according to the security vulnerabilities.

SMALL FIRMS TEND TO HAVE INSUFFICIENT SECURITY

- Cyber Criminals particularly target small accounting firms since they have implemented much lesser security systems.
- When they get access to an organization's system, cybercriminals can regularly steal virtually any type of documents, from financial records to emails.

Small Firms May Not Recover From Hacks

- For small firms, recovery may prove fairly hard to achieve if not impossible.
- Clients pay accountants for their skills, however, they likewise expect trust and tact.
- If the firm cannot guarantee customers' data protection, the organization may never have the capacity to come back to its earlier level of business.

Action Plan to Protect Your Firm from Cyber Attacks

KNOW THE APPLICABLE LAWS

- Every firm is expected to protect it's clients' Personally Identifiable Information (PII) or details.
  - PAN
  - Aadhaar Number / Data
  - Digital Signatures
  - Bank Account Number
  - Residential Address
  - Residential or Mobile Phone Number
  - Date of Birth
  - Place of Birth
  - Mother's Maiden Name
  - Financial Records

SECTIONS OF IT ACT RELATED TO DATA PROTECTION

The Information Technology Act, 2000 have two sections relating to Privacy:

- **Section 43A**, which deals with implementation of reasonable security practices for sensitive personal data or information and provides for the compensation of the person affected by wrongful loss or wrongful gain.
- **Section 72A**, which provides for imprisonment for a period up to 3 years and/or a fine up to Rs. 5,00,000 for a person who causes wrongful loss or wrongful gain by disclosing personal information of another person while providing services under the terms of lawful contract.

IT RULES RELATED TO DATA PROTECTION

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- Applies to bodies corporate and persons located in India
- Duty to draft a privacy policy and make it easily accessible to the provider of the information.
- The policy should be clearly published on the website and should contain details on the type of information that is being collected, the purpose for which it has been collected and the reasonable security practices that have been undertaken to maintain the confidentiality
- Obtain consent in writing or by Fax or by e-mail before collecting such sensitive personal data.

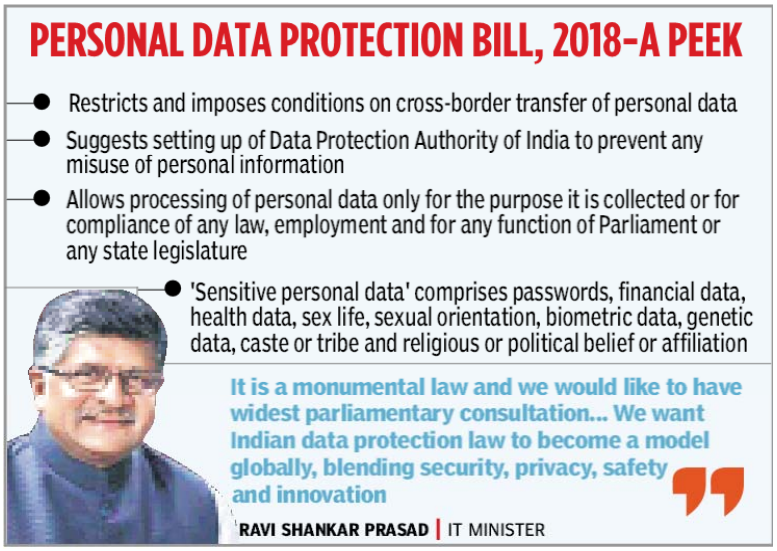
IT RULES RELATED TO DATA PROTECTION

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- The information collected shall be used only for the purpose for which it is collected
- Retain the information for no longer than is required for the purposes
- Seek prior permission of the information provider before disclosing such information to a third party
- Maintain the security of the information provided

LAW IN PIPELINE SINCE 2011

- **The Privacy Protection Bill**, proposed legislation for a privacy and personal data protection regime in India.
- This law when passed would regulate the collection and use of personal data in India, as well as surveillance and interception of communications.



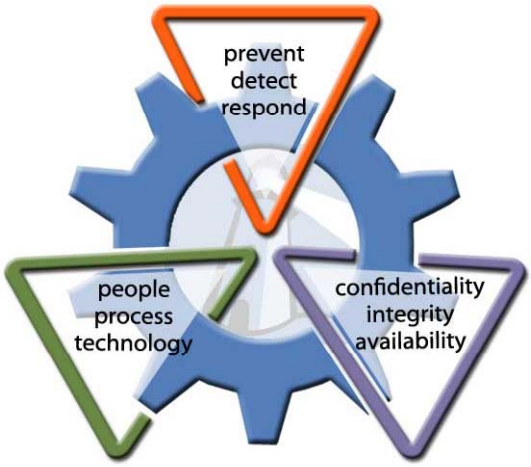
PERFORM REGULAR RISK ASSESSMENTS

- A review of the client information, categorizing which are regulated PII and sensitive data
- Identification of new laws that your firm need to fulfill for compliance
- Partner with a Managed Services Provider to make sure your risk is limited and make sure your systems are protected and secure.
- New developments in the regulatory and business environment
- New technologies that your firm could be maximizing

Likelihood severity occurs	Potential Severity Rating: Minor	Moderate	Significant	Catastrophic
Very Likely	Moderate	High	Extreme	Extreme
Likely	Low	Moderate	High	Extreme
Unlikely	Very Low	Low	Moderate	High
Rare	Very Low	Very Low	Low	Moderate

CREATE A CYBER SECURITY POLICY

- It's easier for your employees to follow cyber security protocols if it's a:
  - Formal Policy Document,
  - Part of your employee handbook, or
  - Clearly outlined in your standard operating procedures.
- A written cyber security policy can also help in training employees.



Cyber Security Triads

UPDATE THE OPERATING SYSTEM

- Buy Genuine Operating Systems
- The operating system requires frequent or continuous updates for strengthened security
- System updates are especially significant for server operating systems.
- Regular updates of OS, upgraded firewalls and anti-virus in your workstations can provide for more trusted protection against threats.
- Harden your operating systems as per manufacturers guidelines.

EMAIL SECURITY

- More than 90% of cyber-attacks begin with a phishing email.
- Majority of people open an email from an unknown individual's name, without browsing or verifying the actual sender's email address.
- Encryption of Email is the key.
- Default Gmail encryption protects emails. Google encrypts emails both when they're stored (data at rest) and while in motion.
- Gmail encryption does have its limits, but can be easily strengthened with an additional layer of client-side encryption, via third-party add-ons.

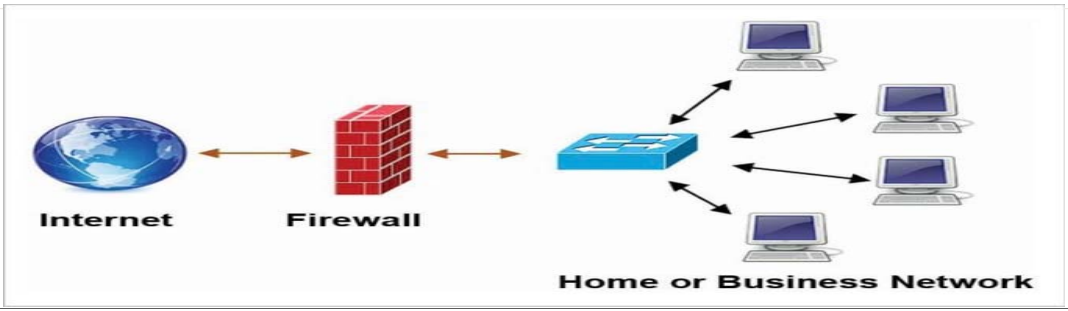
ANTIVIRUS UPDATES

- Use genuine anti virus software
- Antimalware applications should check for updates frequently,
- Scan the devices on a set schedule, along with any media that is inserted.
- In bigger firms, having a central antivirus server is recommended.

VIPRE from SUNBELT SOFTWARE · TREND MICRO · pctools · McAfee · KASPERSKY lab · ca · eset · AVG · G DATA · PANDA SECURITY · AhnLab · avast! · Norton from symantec · F-Secure · Microsoft Security Essentials · webroot · Quick Heal · RISING · bitdefender

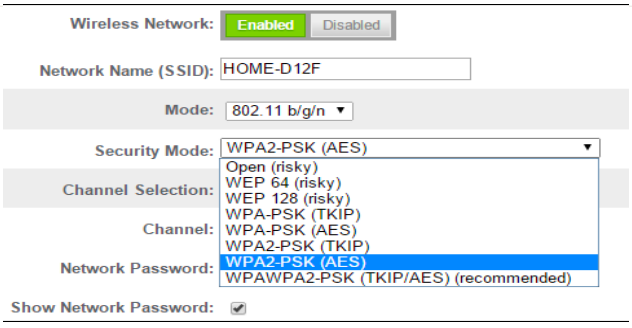
INTERNET SECURITY

- Internet searches can lead you to compromised websites, which infect your network with viruses and malware.
- Install a hardware firewall router with gateway antivirus, gateway anti-malware, and intrusion protection system.
- Use Proxy Servers / Content filtering to prevent employees accessing certain websites



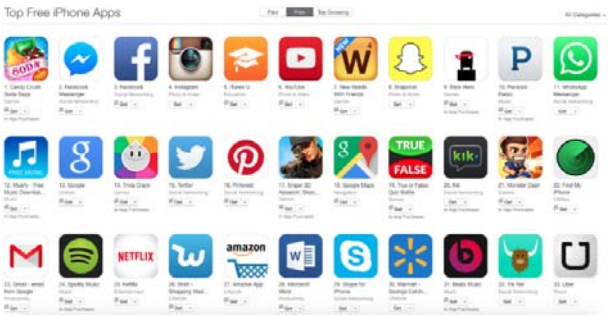
WIRELESS SECURITY

- Secured remote / wireless access into your network system planned, tested, and then implemented.
- Deploy a strong password policy for accessing the Wireless Network.
- Have a guest network for visitors that need internet access via your wireless network system.



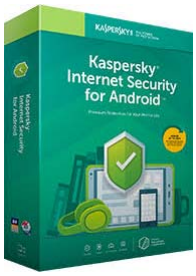
PROTECTION FOR MOBILE DEVICES

- Data used on mobile devices should be encrypted.
- Devices should be password protected
- Using only genuine and trusted mobile apps.
- Using the latest security apps on the phone.



Google Play Store

App Store



PROTECTION FOR USB DEVICES

- Any device that plugs into a USB port including Mobile Phones, iPods, and cameras can be used to spread malware.
- When an infected USB drive is plugged into a computer, the malware infects that computer.
- An organizations's biggest weakness is an employee who simply doesn't understand the potential security risks of using USB drives.

Protection For USB Devices

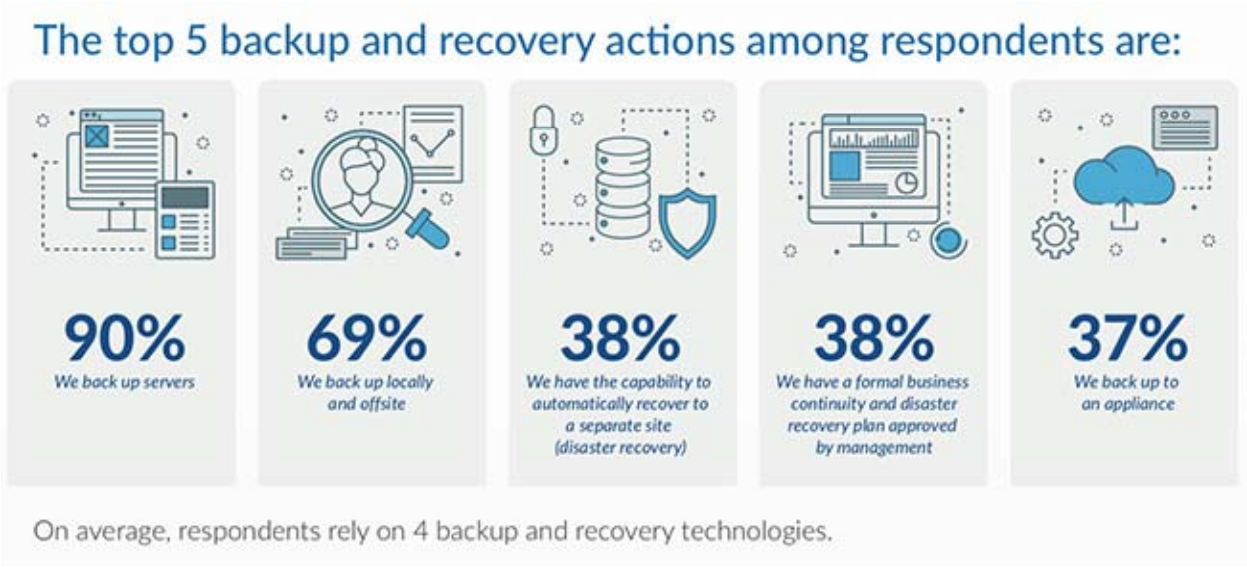
Steps to protect the data on your USB drive and on any computer:

- Use passwords and encryption on your USB drive
- Keep personal and business USB drives separate
- Use a firewall, anti-virus software, and anti-spyware software to make your computer is less vulnerable to attacks
- Do not plug an unknown USB drive into your computer
- Disable Autorun
- Develop and enforce USB drive-related policies

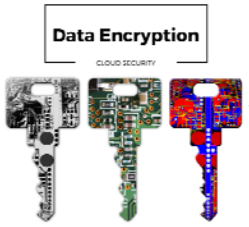
Backing Up Data Religiously

- If all your data is in one place, it is nowhere.
- Back up all of your most important data on a regular basis.
- Backup stored at an off-site server it drastically minimizes chances of a breach or data loss.
- Currently one of the best methods of security.

SURVEY CONDUCTED BY KASEYA



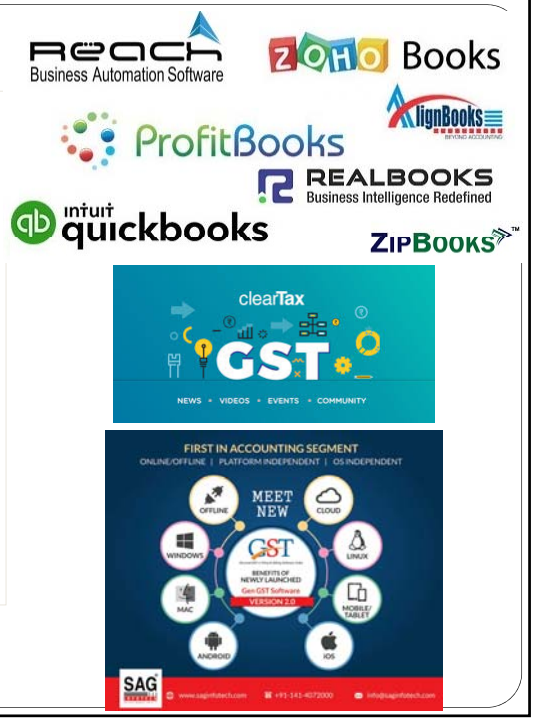
ENCRYPT BACKUP DATA



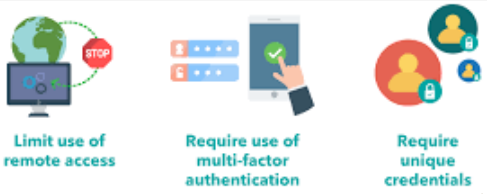
- As a professional, your responsibility is to ensure that data is secure when it's in your custody.
- Encrypt any backup media that leaves the workplace, and also validate that the backup is complete and usable.
- Frequently review backup logs for completion, and restore files randomly to ensure they will actually work when required.
- Hiring an IT specialist is advisable to set up your firm's network, and ensure your data is encrypted and secured.

MOVE YOUR DATA TO THE CLOUD

- Data stored on the cloud has greater protection than data that is stored on company servers.
- The move to such cloud services can change business habits that help ensure a much secure accounting firm.
- Cloud accounting can make your business more efficient.
- It's not that hard to migrate your practice to the cloud, and it will improve your efficiency, save money and make your clients feel safer



REMOTE WORKING



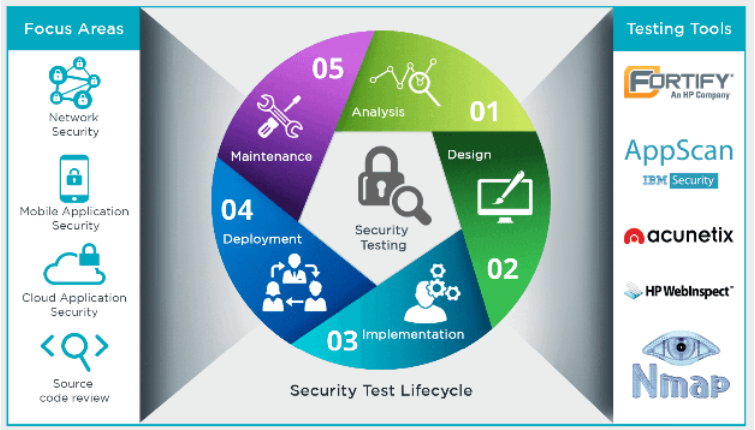
- Remote data access makes it easier for hackers to steal and misuse sensitive financial data of clients.
- Employees should access the computers and business solutions over a secure Virtual Private Network (VPN).
- Use genuine and trusted software solutions, like Microsoft Remote Desktop, Licensed Team Viewer for remote access.
- Implement multi-factor authentication to ensure that any unauthorized user does not access the data stored in the cloud.

BYOD POLICIES

- Bring your own device (BYOD) trend has seen grow rapidly in offices throughout the nation.
- Since employees get to access Company and Client data on their personal devices, it is essential for firms to have policies in regards to Cyber-Security for such individual devices.
- One can decide to completely prohibit the utilization of personal gadgets for organization matters or impose limitations to the data that can be accessed on them.
- It is for the best interest of the accounting firms not to allow BYOD so that the data never leaves the office.

TEST SECURITY MEASURES

- Hire Security specialists for proper configuration when implementing firewalls and security-related features such as remote access and wireless routers.
- External resources can be called upon to do Vulnerability Assessment / Penetration testing of your applications or networks.



EDUCATE EMPLOYEES

- Most breaches occurred because of un-aware employees.
- Security education is a must and should be conducted once a year.
- Employees should be regularly instructed on current cyber security attack techniques such as phishing and dangerous threats including ransomware, and social engineering
- Review IT / computer usage policies, and provide reminder training to employees for all the new and updated policies.

IN CONCLUSION

- **Isn't technology a crucial factor in cyber security for accounting firms?**
- **Is technology at fault for all these modern-day data espionage?**
- It's not technology per se, but the poor implementation of the technology which is at fault.
- It would be best to partner with a managed services provider to take care of your cyber security and tech management needs.

Thank You

CA Pranay Kochar

9819846198

pranay@kocharconsultants.com

KOCHAR CONSULTANTS

Essence of IT Security

INFORMATION SYSEM AUDIT | IT CONSULTING | IT GOVERNANCE & COMPLIANCE