Practice Management

How to protect your firm against hacking and cyber crimes

Presented by Nestene Botha (CA)SA RA

Proud #ProTechMentor at www.protechaccounting.com

How to protect your firm against hacking and cyber crimes

Presented by:

- Chartered Accountant (SA), Registered Auditor
- Masters in Accounting Education
- Top 35 under 35 *2
- Founder of the first virtual audit firm in South Africa
- Managing director & founder of Coloring4Covid, Born2Count, The Audit Pro, ProTech Accounting Solutions, ProTech Sales Solutions, ProTech Training Solutions

Check out my profile at www.protechaccounting.com

How to protect your firm against hacking and cyber crimes

Housekeeping:

- Questions in the Chat Box :)
- Recording available for download from SAAA website
- Slides pre-distributed, but can also get a copy on the SAAA website

How to protect your firm against hacking and cyber crimes

Importance of Topic:

- information theft is the most expensive and fastest rising consequence of cybercrime
- (Ninth Annual Cost of Cybercrime Study)
- Significant Business Risk
- Risk Management Strategy

https://www.techrepublic.com/article/ransomware-attack-why-a-small-business-paid-the-150000-ransom/

How to protect your firm against hacking and cyber crimes

Importance of Topic:

British Airways

- Skimming credit card details from website
- 500,000 customers
- Reputation impact
- GDPR case
- Class action

Wannacry

- Ransomwear attack
- 200,000 computers across 150 countries
- Business disruption

Hairdresser in Glasgow

- Ransomwear attack
- SME
- Business disruption

How to protect your firm against hacking and cyber crimes

Importance of Topic:

IFAC Guidance

- Get the basics right (80% of cyber attacks can be prevented according to IFAC by just getting the basics right!)
- Protect Key Informational Assets
- Consider Cyber in all Activities
- Accept that security will be breached

https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

How to protect your firm against hacking and cyber crimes

Accountant’s risks:

- Loss of data
- Loss of customers
- Fines
- Legal Action
- Reputational Damage
- Operational Disruption

How to protect your firm against hacking and cyber crimes

Accountant’s role in cyber security:

- using their skills and expertise to protect data and information
- reporting on a company’s cybersecurity risk management program and controls

How to protect your firm against hacking and cyber crimes

What should the accountant do?

- Comprehensive business-led approach
- Holistic risk management
- Involving all levels of an organization
- Ongoing
- Respond to new standards and regulation
- Understand the weaknesses in legacy systems
- Identify where investment in technologies can help
- Ethical duties
    - e.g. might be necessary to make a public disclosure

How to protect your firm against hacking and cyber crimes

What should the organisation do?

- Identify key informational assets
- Identify gaps
- Target resources to deal with key threats
- Broaden cyber security activities beyond prevention to include:
  - Intelligence
  - Detection
  - Response
- Understand cybersecurity roles and capabilities
- Identify, mitigate & monitor key risk areas
  - Map out major processes
  - Assess risk remediation plan
  - Assess control

How to protect your firm against hacking and cyber crimes

Example Basic Key Risk Areas to Consider:

- boundary firewalls
- internet gateways
- secure configuration
- access control
- malware protection
- patch management

How to protect your firm against hacking and cyber crimes

Service Offering Opportunity:

- Helping clients assess their governance and risk management
    - smaller businesses tend not to have strong risk management and control expertise
    - Accountants can ensure adequate business continuity and disaster recovery planning
        - For example recovery from ransomware threats
- Helping clients quantify risks and return on investment based on cost of breaches and stolen data and factors that impact cost
- Helping to mitigate risks with effective controls
- E.g. https://www.bdo.co.za/en-za/services/advisory/cyber-innovation-assurance-and-analytics

How to protect your firm against hacking and cyber crimes

Guidance available to accountants:

- The ICAEW provides simple cyber security steps for smaller firms.
- AICPA’s System and Organization Controls (SOC) for cybersecurity
- National Institute of Standards and Technology (NIST) Cybersecurity Framework

How to protect your firm against hacking and cyber crimes

Security best practices for small businesses

Employee Training

- Training employees to detect malicious links and emails is an efficient and cost-effective way of preventing malware attacks.

Secure Data Storage

- Opting for an efficient cloud-based storage solution, followed by regular data back-ups to the cloud, is an affordable way of boosting data security. It’s also one way of mitigating the effects of possible ransomware attacks.

How to protect your firm against hacking and cyber crimes

Security best practices for small businesses (continued)

Basic System Security

- Optimise password protection (including two-step authentication)
- Update hardware and software
- Secure all business devices
    - Website vulnerability and intrusion-detection scanning
    - Virtual private network (VPN)
    - Managed firewall and antiviral services & anti-malware software

Build a shield around hardware and end-points with policy

- All employees should:
    - use only dedicated business devices to conduct business
    - dispose of data and equipment in the proper manner
    - securely send and receive information
    - encrypt all backed-up data

How to protect your firm against hacking and cyber crimes

Security best practices for small businesses (continued)

Cover all your bases from a solutions perspective and ensure you and your staff understand what each is for:

- **Firewalls** are software (and also hardware) designed to protect the system from attack from people accessing the organization’s systems via both internal and external communication links.
- **Malware/spyware and web proxy protection solutions** protect the system from software code that may be from pop-up windows or have more insidious intent, such as logging usernames and passwords for fraudulent purposes.
- **Anti-spam software** protects email inboxes from being clogged by unwanted broadcasted email.
- **Anti-phishing software** protects users visiting websites that are designed to trap user information that can then be used for fraudulent purposes.

How to protect your firm against hacking and cyber crimes

Outsource

https://www.jmark.com/

https://theoutsourcedaccountant.com/how-we-help/

How to protect your firm against hacking and cyber crimes

Thank you for Listening!!!

Any Questions?:)

Pop your email in the chat if you’d like to be notified of my future events :)