Hackers set their sights on accountancy firms – 7 steps to minimize risk

Joe Collinwood, CEO at CySure explains why accountancy firms are targets for hackers and what steps they can take to minimize their exposure.

LONDON, UK, July 25, 2019 /EINPresswire.com/ -- When it comes to cyber crime, small accountancy practices are not exempt from the disruption that affects large organizations. In the USA for example there has been an explosion in fraudulent W-2 filings and in the UK with more filings now on-line risk is increasing. So why are accountants being targeted?

•They hold large amounts of private data
•They have the information cyber criminals want – corporate financial data, social security numbers, Tax IDs, bank accounts, payroll data.
•Accounting firms use similar software so if a criminal finds a vulnerability they have lots of potential victims
•Typically there is inadequate technical protection, policies and procedures
•A lack of incident response and business continuity procedures means accountants are more likely to pay a cyber criminal money for fear that the firm's reputation will be tarnished.

Many accountancy firms are making it easier for hackers by underestimating the threat they face from cyber attacks. There were 438 separate data security incidents reported to the Information Commissioner's Office (ICO) in Q2 2018/2019 alone in the finance, insurance and credit sector. The cost to launch cyber attacks is negligible and the most likely method of breach is phishing ie human error. It's time to think again.

Gateway to Information
Self-employed accountants and accountancy practices are on the radar of cyber criminals because of the amount of valuable data they hold. This information enables hackers to pull off complex frauds at a later date. Cyber criminals view accountancy firms as a "gateway" to client information and are perceived as a soft target with few security barriers, limited cyber security tools and little or no in-house expertise.

Additionally, as many firms use the same software systems, hackers are motivated to seek vulnerabilities in the software knowing there will be a substantial pay day by exploiting the weakness to attack multiple businesses.

Minimize Risk – 7 simple steps to cyber resilience
No business is too small to be attacked, however with the right approach to security, accountancy firms can pave the way to cyber resilience by following these top cyber-security tips:

•Invest in effective firewalls, anti-virus and anti-malware solutions and ensure any updates and patches are applied regularly,
•Ensure business critical data, such as customer data and financial information, on all company assets is securely backed up and can be restored at speed
•Have simple, clear policies in place to create a cyber-conscious culture in the workplace
•Have regular awareness training for reminders of potential scams or tactics
•Review contracts and policies with suppliers to ensure they have an accredited standard for

cyber-security and their partners to protect the supply chain
•Have an up-to-date incident response plan that is practised regularly
•Consider investing in cyber insurance to cover the exposure of data privacy and security.

Where to start and what to do now
Cyber security need not be complex or prohibitively expensive, in the UK Cyber Essentials (CE) is a government and industry backed scheme specifically designed to help organisations protect themselves against common cyber-attacks. In collaboration with Information Assurance for Small and Medium Enterprises (IAMSE) they have set out basic technical controls for organisations to use which is annually assessed. In the US the National Institute Standards and Technology (NIST) framework guides organizations through complex, emerging safety producers and protocols.

With an online information security management system (ISMS) that incorporates Cyber Essentials and NIST, accountancy firms can undertake a certification route guided by a virtual online security officer (VOSO) as part of their wider cyber security measures. This will help the organization to coordinate all security practices in one place, consistently and cost-effectively. Additionally, firms can take advantage of the expertise of online cyber security consultants at a fraction of the cost of a full-time in-house security specialist.

Demonstrating confidence to the client base
Cyber security certification ensures standardization and is a good differentiator as it shows a diligence to information security. By giving cyber security the same priority as other business goals, accountancy firms can proudly display their security credentials and demonstrate trust and confidence to their client base.

[i] https://ico.org.uk/action-weve-taken/data-security-incident-trends/
[ii] Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Mary Phillips
PR Artistry
+44 1491 845553
email us here