CPA
Practice Advisor

ADVISORY

Ransomware: Is Your Accounting Firm At Risk?

Ransomware is a type of malicious software that encrypts files, blocks access to computer systems then requires an anonymous payment, and has the ability to make a dramatic and devastating impact on your business. A recent report released by the FBI ...

Christopher Stark • Aug. 22, 2016

In this day and age, accounting firms need to be just as aware of cybersecurity threats as they are of filing deadlines and tax guidelines. One of the most vicious cyber threats in history is affecting small businesses, individuals and accounting firms right now- ransomware.

Ransomware is a type of malicious software that encrypts files, blocks access to computer systems then requires an anonymous payment, and has the ability to make a dramatic and devastating impact on your business. A recent report released by the FBI claims ransomware infections caused more than $1.6 million in losses last year for individuals and businesses- an absolute pandemic, as stated by *TechTarget*.

It only takes one click of a mouse for your firm to quickly become infected with ransomware. Often times, it occurs when staff opens attachments within emails. These emails may appear to contain important client data or a shipping confirmation, but they are just disguised malware. Microsoft Malware Protection Center notes your firm's infrastructure can also become exposed to ransomware when employees access fake or suspicious websites.

Keeping your data and applications safe and secure from ransomware attacks, while increasing your clients' awareness of malicious software, requires collaboration with

your internal IT department and/or managed IT provider. There are three things you can do to better protect your firm and clients: examine your current IT infrastructure, update security measures, and educate your staff and clients.

1. **Examine Current IT Infrastructure:** Your firm stores and accesses client information on a daily basis, so you must make sure this critical information is kept safe. To ensure client files are protected, your firm should perform a security audit to identify vulnerabilities in your organization's IT infrastructure. The New Jersey Society of Certified Accountants (NJCPA) recommends partnering with a third-party security firm to conduct a Vulnerability Assessment or Penetration Test at least once each year. The results from the security audit can help your firm establish a plan to close any security gaps that make your organization vulnerable to ransomware.

In addition, you should review and test your disaster recovery and business continuity plans each time your IT environment changes. In the event of a ransomware attack, these plans are invaluable. *IT Business Edge* notes disaster recovery plans can help your firm get systems back up and running after a cybersecurity attack. The same article also advises that business continuity plans enable staff to remain productive while cybersecurity issues are being resolved.

2. **Update Security Measures:** When ransomware infects an organization's IT infrastructure, it can restrict access to critical information stored within the computer system. Because of this, it is important for your CPA firm to be proactive in updating security measures. Your firm's data backup procedure is a key security measure that should be top of mind. *TechAdvisory.org* advises that small to mid-size businesses that work with critical client information should perform daily backups. Frequent backups will minimize your organization's loss of data in the event of a ransomware attack.

Along with updating your firm's data backup procedures, you should also consider where your data backups are being stored when revamping security measures. Many organizations store their backups to on-site servers within their IT infrastructure, making their data vulnerable to ransomware attacks. To ensure your data backups will not be infected by malicious malware, you should consider storing data backups on servers at a secure off-site storage facility. This will allow your organization to restore its IT infrastructure from the most recent backup in the event of a ransomware attack.

3. **Educate Staff and Clients:** As mentioned earlier, emails containing suspicious attachments and fake websites can lead to your firm becoming infected with ransomware. To minimize the likelihood of your staff opening these types of emails or websites, collaborate with your internal IT department to develop and implement cybersecurity training courses. Cybersecurity training courses will help educate your staff on the different types of ransomware threats. Once your employees become well-versed on the types of email attachments they should not open and websites they should not access, then they can pass along their knowledge to your clients as advisory services. The American Institute of Certified Public Accountants (AICPA) recommends that firms provide advisory services in which their staff educates clients on their organization's security measures, potential cybersecurity threats, and steps they can take to ensure their critical information is safe and secure.

Examining your IT infrastructure, updating security measures, and educating staff and clients will help you protect your organization and client base. If your organization's IT department or IT managed provider is struggling to keep up with the latest cybersecurity threats, a cloud service provider with extensive cybersecurity experience can step in and fill the gap in areas where you feel your firm's security practices are lacking. Whether you are working with your IT department or consulting a cloud vendor, your firm's top priority must be keeping your IT infrastructure and your clients' data safe from any cybersecurity threats, including ransomware.

———

Christopher Stark is the founder, president and CEO of Cetrom (www.cetrom.net), an industry-leading provider of custom cloud solutions that transform the way businesses succeed. With nearly 30 years of experience in all facets of the IT industry, and some of the industry's most prestigious technical certifications, Stark employs unmatched insight on the future of IT to serve clients across many markets, including the CPA and accounting industry.

Advisory • Firm Management • Article • Data Security • Extortion • Financial Crimes • Firm Management • IT Security • ransom • ransomeware • ransomware