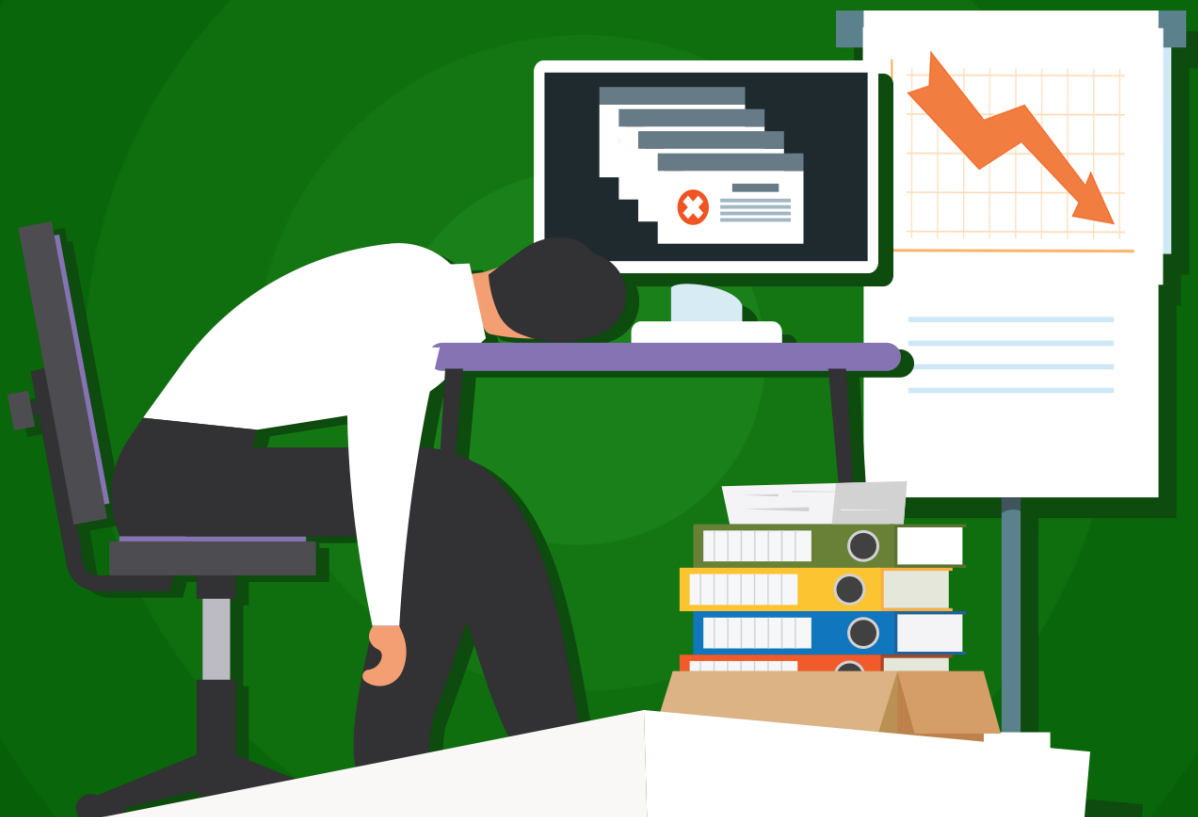


ADDRESSING THE BIGGEST

TECHNOLOGY ISSUES

FOR ACCOUNTANTS





Digital transformation impacts every industry, and accountancy is no different. This backbone to business functioning must evolve and adapt to new technologies, which could mean fresh challenges and cybersecurity risks. Yet the advances also bring improved accuracy and efficiency. This ebook discusses available tech and how to safely incorporate it into your practices.



Accountancy in the Digital Age

Accounting started out with the abacus. Today, it's evolved to include automation and artificial intelligence (AI). Digital transformation can be daunting for the small business accountant, but technology offers many advantages. This ebook will examine:

- what digital transformation looks like for accountants;
- challenges addressed incorporating IT into business processes;
- cybersecurity risks;
- best practices for keeping systems up and running.

Client expectations have changed, and how accountants fulfill their responsibilities continues to evolve. You can adapt more effectively using current IT.



Digital Transformation and Accounting Firms

The first mechanical calculator was developed in 1642. Astronauts on the Apollo 13 mission travelled to the moon with a slide rule. In 1961, the first desktop electronic calculator was released. Just eight years later, portable calculators were available. The speed of change has only picked up from there.

Accountants need to be keeping abreast of a constantly changing landscape. Some of your business owner clients may never have filled out a tax form on paper or set up an Excel formula. They may loathe anything that needs to be posted or signed. Thanks to cloud accounting packages and DocuSign software, they expect to be digital.

Accounting firms today are doing e-business. Internal and external communications use email, and files are imported and exported electronically.





All this offers several advantages:

- improved accuracy;
- greater productivity;
- reduced operational costs;
- increased speed of write-ups and reconciliations;
- enhanced organization;
- wider, searchable access to client history to analyze trends and make recommendations.

Technology helps accountants interact with clients to provide advice and settle tax issues. They have greater



agility, too, as software streamlines time-consuming paper-based practices.

Automation and AI

Accountants may worry that automation and artificial intelligence (AI) will take over. Automatic bank feeds, for example, sync client financial transactions in one place.

Yet the job of an accountant isn't at risk of replacement by robots. Automation hands tedious, time-consuming, repetitive tasks over to the machine's processing power. This saves time and improves accuracy, but it also frees up the human accountant to focus instead on higher-order thinking.

Even with AI algorithms, the accountant still needs to take an advisory role. The AI isn't a big-picture, critical thinker. The accountant's role remains holistic oversight, verifying automation results, and making sense of the numbers. Making technology work for you can set your strategic thinking and efficiency apart.



Technology Challenges for Accountants

Accounting businesses are taking advantage of many IT tools:

- Desktop or laptop computers are connected to a network for data exchange, storage, and backup.
- Cloud services are easy to install and provide small businesses with enterprise-level tools.
- Social media helps spread the word for the accounting business.
- Mobile devices and a bring-your-own-device (BYOD) policy can promote employee flexibility.
- Application integrations make accurate data available from different departments and customer systems.
- Cloud or off-site backup provides a plan B in case of on-site IT disruptions.



All this available technology offers many benefits. However, there are challenges to consider, too, and cybersecurity comes foremost.

Cyber bad guys target businesses of any size across industries. The daily news covers the big breaches, yet no company is too small to be harmed. A breach at an accountant puts sensitive client information at risk, as well as the firm's own data. Address, date of birth, and account numbers are the details needed for identity theft.

Smaller businesses are also targeted with the expectation that they will have weaker security. They can be the first stepping stone in an attack against a larger target. Your business may have access to a customer's supply chain management (SCM) software. Hacking your business may be focused on gaining your credentials to that SCM site.

In malware attacks the bad actor disrupts business services and charges a ransom. Ransomware attacks can lock away



years of records you keep for clients. If you don't pay the price, you're stuck with encrypted data you can't access (unless you have data backups). Next we'll discuss preventative measures accounting firms can use to reduce risk.



Best Practices to Keep Systems Up and Running

Accounting firms are more reliant than ever on technology. Ensuring all IT works together can make a real difference to business productivity. Even an hour without email can be a big deal. Server failures are not only a barrier to success but also discredit your business brand. Plus, accounting businesses operate under regulatory rules, and your business could face serious consequences if you don't meet the requirements.



First, inventory all connected devices, including scanners, servers, office printers, desktops, and more. Identify all financial preparation software, billing systems, and other applications (such as Office 365). To maintain your system, you need a clear picture of what's online. Keep up to date with all software updates and patches for all devices. Upgrading the operating system but using a default password on a router is counterproductive.

Use solid IT controls. Set up firewalls. Encrypt all data. Develop backup and recovery plans. When it comes to your backups, make sure there is at least one version that has an air gap. That means the backup is not accessible remotely or connected to the internet.

Institute network monitoring. Review data files for unusual activity patterns. Configure alerts for unusual traffic. Examine external traffic. All this can help you detect a threat or identify a breach quickly. It's also important to ensure



employees understand their role in information security, especially when working remotely. Educate them to protect against phishing attacks or information disclosure, and emphasize the importance of strong passwords.

Finally, have an incident response plan in place. Without data access, you and your employees can't do your jobs. Missing a deadline is costly. Plan ahead so that if the worst does happen, you're able to react effectively.

Conclusion

Evolving accounting technology offers tremendous growth potential for the future, but digital transformation leaves accounting firms with more technology to maintain. Some small business take a break-fix approach: after the damage is done, when systems are down, they reach out for help.

Working with a managed service provider (MSP) provides proactive support. You'll pay a small, consistent fee to have an IT expert on call to address your technology needs.



The MSP will begin by getting an overview of all your technology. After asking about business goals, the MSP recommends best solutions for your needs. They can set up virus and malware protection and domain name server (DNS) controls, or install mobile device management or secure remote network access as needed.

Maintain business continuity, minimize your risk exposure, and keep your business effectiveness high. For best results, partner with an MSP that knows accounting management and tax preparation software. We can help your accounting firm streamline processes and secure information. Give us a call at (508) 617-1310 today.





Phone: **(508) 617-1310**

Email: info@powerupboston.com

Web: www.powerupboston.com

Facebook: facebook.com/powerupboston