accountingTODAY WebCPA http://www.accountingtoday.com

10 Tech Moves Every Accountant Should Make This Summer

JUNE 30, 2014
BY RAMESH RAJAGOPAL

The use of cloud or web-based applications is becoming prevalent across the spectrum of accounting activities. The simple reason: Cloud applications shift the pain of managing technology to a vendor who deals with updates, feature enhancements and uptime in return for a predictable per-user fee. But more importantly, delivering apps over the web offers the flexibility that accountants and their clients increasingly need to support decentralized and mobile teams who must access information from anywhere and any device. It's clear that web applications are here to stay.

But the shift to the web has also introduced new challenges when it comes to data security and control. One clear challenge is the potential for data compromise when users trust the local browser to safeguard client information (including login credentials). Sensitive data is usually well protected as it sits in the cloud. But as it's accessed and dumped into the local browser, the likelihood of misappropriation increases sharply.

Browsers are designed to indiscriminately connect to websites and fetch code. All that code sits in the same browser memory, which means that business data gets mixed with whatever else the user is browsing. This creates a fundamentally untrustworthy environment from which to access business data. It's therefore unsurprising that the browser remains the No. 1 target for hackers who capitalize on users' casual surfing habits and carefree propensity to click on links to create an open channel to inject malicious code alongside valuable data.

accountingTODAY
60 seconds smarter
$300k – $400k
Estate Planning with 529 Plans
BROUGHT TO YOU BY HD VEST FINANCIAL SERVICES
VIEW HERE

Once compromised, an exploit might capture keystrokes as users login, or redirect the user to a fraudulent web page to gather account information there. The finance and accounting world is particularly susceptible given the prevalence of "work-from-anywhere-any-device" users and the resulting inability to ensure that business data is always being accessed from a pristine environment. Zeus, Spyeye and Zberp are just a few examples of banking trojans that have compromised browsing sessions over recent years. Zeus alone is estimated to have caused damages of $100 million since inception.

But the risk to sensitive online data isn't limited to outside hackers and exploits. Given the ubiquity of web applications, users themselves are a point of vulnerability, either unwittingly or not. Consider how most of us create and store usernames and passwords, or reflexively download documents to personal devices or upload them to cloud storage folders like Dropbox to access from home. In most cases, we're just trying to get our jobs done, but we pay short shrift to the impact of real-life events in the process: a lost or stolen laptop, a USB flash drive left at a client site, or a notebook containing usernames and passwords dropped in a coffee shop.

For accounting firms, these risks can be compounded in team situations. A good example is a shared service bureau in which client coverage responsibilities rotate across a pool of users, each of whom needs access to a common set of login details and client documents. As a general principle, the more people who share access to data, the greater the potential for something to go wrong. Consider the tedious and error-prone process of revoking account access when someone leaves a team.

So what should accounting leaders do to realize the benefits of web apps in light of the data access risks outlined above? Here are some things to consider:

1. Dedicated computers for certain jobs: Reserve one computer for nothing else but accessing key financial portals. It's a bit crude, but if your team is small and you don't need to grant third-party access, it can reduce the likelihood of an online exploit. At a minimum, encourage your users understand the value of using two browsers, reserving one for business data.

2. Basic endpoint security: Install and regularly update anti-virus tools and hard disk encryption software on all company-issued computers. It's the bare minimum for any finance organization, although it does not address the prevalence of employees and contractors logging into corporate systems from unmanaged and often unsecure personal devices.

3. Virtual containers for secure browsing: A more robust solution for larger, distributed teams is to access key accounts from within virtual containers. Think of this as a segregated environment on a computer from which to access important data. With some offerings, the container sits on the user's computer, which is a little cumbersome, especially as users roam across different devices. But a new class of technology is emerging that virtualizes and secures the browser in the cloud so it can be accessed from any device. If your firm has moved to remote desktops, think about how Web accounts are accessed. If from a general purpose browser within the hosted environment, you've done nothing to safeguard data from the risks described above.

4. Backup your data: Take your critical data and back it up. Then back up your back up. The risk here goes beyond a stolen computer or a hard drive failure. A class of malicious code known as ransomware is used to encrypt data and extort the victim into paying a ransom to retrieve it.

5. Revisit internal processes around credential management: Take a hard look at your IT security and business processes in the area of shift management, credential-sharing and access revocation. You might find that clients welcome a conversation on this area, since they too face risk within their internal user population. There are also technical solutions to consider that can enable both parties to share account access without exposing usernames and passwords.

6. Move away from simple logins: Think about two-factor authentication solutions that are practical. Having a separate method for every account quickly becomes a nightmare. But there are ways to implement a common strong authentication and single sign-on framework that can apply across all accounts.

7. Insist on user training, and even testing: Put your team through actionable security training, particularly with regard to the latest social engineering exploits. Some organizations have even created test phishing sites to measure employee behavior.

8. Enforce device and data access controls: Determine what level of data access you are comfortable allowing when users log in from different machines. Consider solutions that can allow you to contain or restrict company data from reaching unauthorized devices and that can enforce remote data wipe when devices are stolen or go missing.

9. Audit your web logs: Business data is commingled with personal browsing. Look at logs of web activity to see where users go and get a picture of suspicious or objectionable content on your network.

10. Partner with your clients: Sit with business owners, the IT team with trusted clients and work collaboratively to define responsibilities. Both parties share a role in protecting sensitive data. The best solution will likely be a byproduct of the two perspectives.

Many of the steps outlined above are free or very affordable and can be done quickly. Others might require more planning. But the cost of inaction can be tremendous. Data breaches and regulatory violations can cost millions in penalties and fines, not to mention the loss of customer trust. Start taking simple steps today.

Ramesh Rajagopal is co-founder and president of ***Authentic8****.*