Wolters Kluwer
When you have to be right

Protect Your Firm:
Knowledge, Process, Policy and Action

By Sandra Wiley, COO, Senior Consultant, Shareholder, Boomer Consulting Inc.

Introduction

It is an exciting time to be in our profession. The abundance of cloud-based solutions is providing more opportunity than ever before to work faster, communicate better and collaborate more efficiently. However, with new opportunity comes new danger.

Your firm needs to be committed to protecting information assets, including personal data and client documents. As a trusted advisor to our clients, the expectation is that we are aware of threats and are guarding their data. Data privacy and information security are fundamental components of doing business today, no matter how large your firm is.

In this paper we will look at three specific ways of protecting our clients:

1. Protection through our ability to research and improve intellectual capital
2. Protection through policies, procedures and processes
3. Protection by securing client data

Protecting through Improved Intellectual Capital

Protecting clients begins with increased intellectual capital. Our clients come to us because of our technical expertise. They expect that we will be able to give them advice and counsel based on the knowledge we have of their business. The reality is we must be able to quickly and efficiently get the answers that we need to serve our clients well. The brilliant part of this task today is that we are moving to the cloud to do our research.

In a recent study by BCI and Wolters Kluwer, our responding audience showed that the research firms are relying on is deeply anchored in online resources. The preference for online research resources was especially pronounced when participants were asked which type of resource they used most often.

The act of staying up to date on regulations is increasing in complexity each day. The expectations of our clients also increase in a world where anything can be researched online. When asked in the survey about how difficult research and building intellectual capital was, a whopping 82 percent of the audience responded they were not highly confident that they have the tools they need, nor the knowledge to properly use them, to deliver the right information to their clients.

In addition to research tools, there is another opportunity to share intellectual capital and improve client service. This involves internal knowledge collection from working with clients in specific verticals or niches. Using tools designed to collect this type of knowledge will improve the speed and accuracy of answers to client questions. Alternately, many of these internal knowledge tools allow for someone to ask a question of firm experts, who can provide answers in a searchable, stored location.

The more we understand how to use cloud-based tools for research and growing our intellectual capital, the more likely we will be to decrease the overall number of hours we are spending in the research area of the firm. In the survey we show that number of hours spent in research is considerable, and we know that the more effective we can make that process the more time we can spend with the client. Tools like CCH® IntelliConnect Direct give access to all kinds of tax data instantly. CCH® KnowledgeConnect™ can be another resource for internal knowledge collection through a collaborative knowledge base and question/answer platform as well.

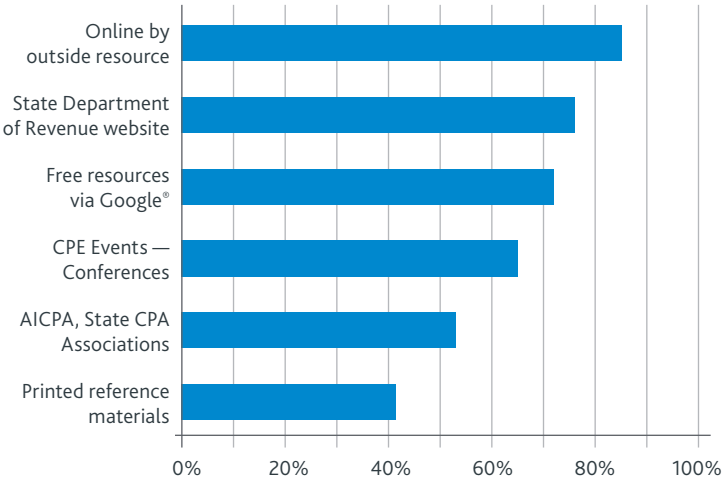

FIGURE 1: Sources of Tax Research

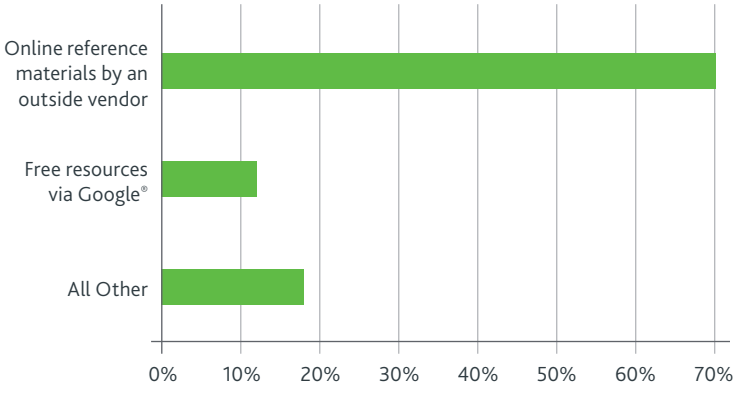

FIGURE 2: Source of Tax Research Used Most Frequently

Protecting through Policies, Procedures and Processes

As we turn our attention to processes, let us first think about the process of actual data entry and the ability to move quickly, efficiently and accurately as we build a firm that is protecting client data. The process of entering data is still largely completed manually which leaves the door open for "operator error." It is also slower and therefore does not help reduce hours to leave more time for deeper client conversations. The move to scan and auto-fill is beginning to catch on, but slowly as the survey shows.

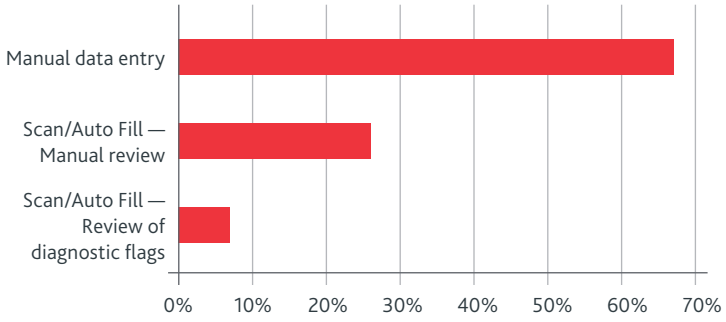

FIGURE 3: **How do you get client tax data into your tax system?**

Standardization is the key to any process that a firm uses in protecting data integrity and security. The move to standardization of processes is high on the list of the individuals in the Boomer Technology Circles™. These firms see that standardization will guard against human error, and will help to improve productivity for the entire firm. One interesting result from our survey is that 76 percent of the audience felt that they were somewhat or very standardized in their processes. Our experience shows that firms do have processes, but they are not standardized across the firm. Most firms have a difficult time deciding on the one process that is really best for everyone in the firm. This is an even greater issue for those that have multiple offices.

Process improvement will benefit your firm in three distinct ways:

1. Reducing data entry
2. Identifying errors earlier in the process
3. Streamlining preparation and review

In all cases, these improvements will also protect the client by allowing for greater accuracy, quicker turnaround time and more time to spend with their trusted advisor to find new opportunities for their business.

Protecting through Secure Client Data

Just mention the words "Target" or "Home Depot" and you know that you will start the conversation about protecting client data. The world of data security starts and ends with solid policies that are developed and shared often throughout the firm. Data thieves are out to get our personal data in order to ultimately steal from us. Personal data is a hot commodity and we have an obligation to have a plan to protect our firm against these thieves.

The first logical step is to develop a written policy for firm client data security. Our survey participants showed that many have engaged in the act of developing these policies, however with the speed of change in technology today, the act of reviewing those policies, updating them and then sharing them with the overall team may not be happening often enough. The graph below shows how our audience responded. One point is that there is really no excuse with the knowledge we have today to be in the 13 percent with no official security policy. Firm leaders are making a conscious decision to not protect their clients.

The next step after developing the policy is to ensure the policy is well known and followed in the firm. This can happen by training staff on the policy at least one time per year. Have them acknowledge that they have been informed and ensure the policies are being followed by allowing your IT Professional to monitor the policies. Steps that are often taken by firms include the following:

- Requiring strong passwords
- Training staff annually
- Requiring password changes after a specific length of time
- Requiring encryption on mobile devices, laptops and USB drives
- Implementing a device management platform that includes the ability to wipe a lost/stolen mobile device
- Enforcing email retention policies
- Developing security breach policies and procedures to provide a timely response to potential data breach

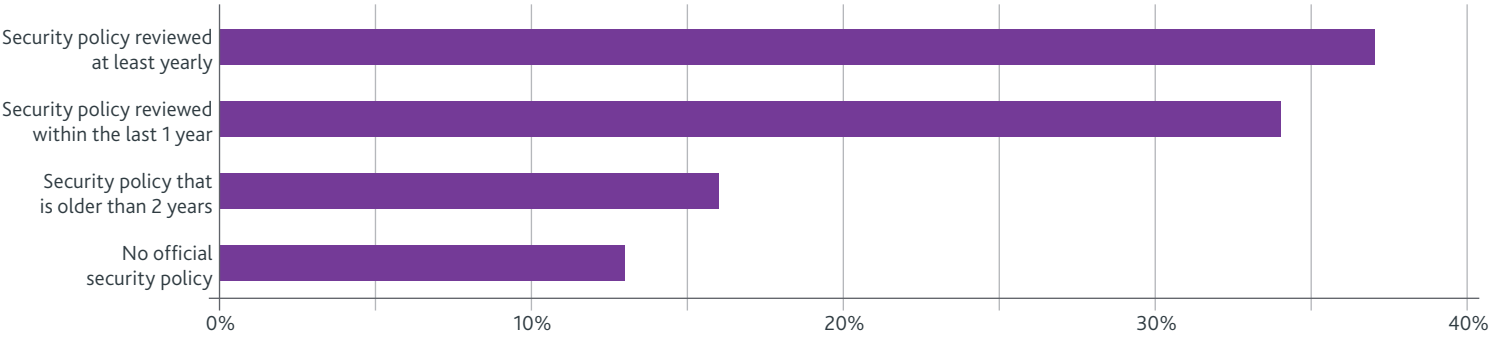

FIGURE 4: **Which of the following best describes your firm's policies regarding client data security?**

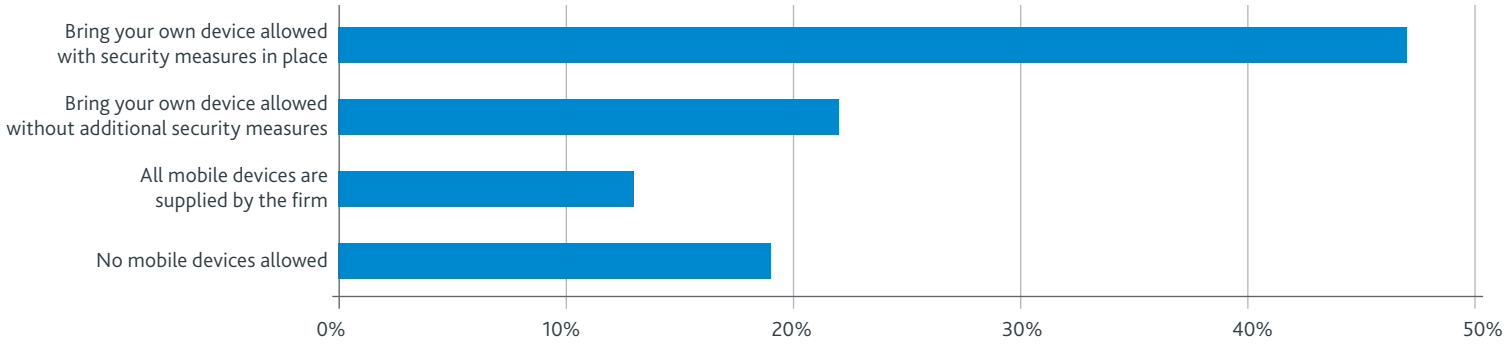

FIGURE 5: **Does your company supply mobile devices for business purposes?**

An additional data breach concern comes with the mobile devices that are in most team members hands today. Firms are recognizing the need to encourage use and also guard the client data that is accessible through these productivity boosters. The trend appears to be for firms to allow team members to use their own devices and then give them parameters for the security on that device.

Firms have another challenge as they look at data security — backing up client data in the event there is a loss. The ability to backup data takes many roads from backing up to a tape and literally taking it home at night to backing up at multiple offsite locations. Our survey shows there is not a clear winner today among this group.

One of the biggest challenges with technology is ensuring that the data that runs the business is both accessible and recoverable in the event of an emergency. Using cloud backup services takes your internal data and moves it to a secure offsite location. This is crucial if you are in a single location.

Cloud applications can provide another way of tackling backup issues. Cloud vendors have an iron clad reason for effective backups — their entire business model revolves around making your data accessible and recoverable. Consider this aspect when upgrading or updating core business applications. Data backups are just one feature of cloud applications, but a very important one.

On the flip side of this coin, cloud applications provide a simple way to add additional features or capabilities to the firm. This is a strong consideration when looking at overall data security. What cloud applications are in use, where and how is that affecting client security? This can be an adversarial point between IT professionals where data security is a top focus, and employees who need to get work done. By working together, the firm's security can be improved and productivity can be gained as both IT and other staff learn about the best applications to use in the firm.

A final threat to the firm is that of insider threats. What are insider threats? They are the staff members that you have sitting right in your firm today. They are not educated on how they might inadvertently allow viruses into the firm by simply clicking an email. It can also involve giving staff members access to more data than they need. These insider threats could wreak more havoc than we can imagine, but are entirely preventable by taking some precautionary steps. In our survey, we asked firms how they protect their firm against these security threats.

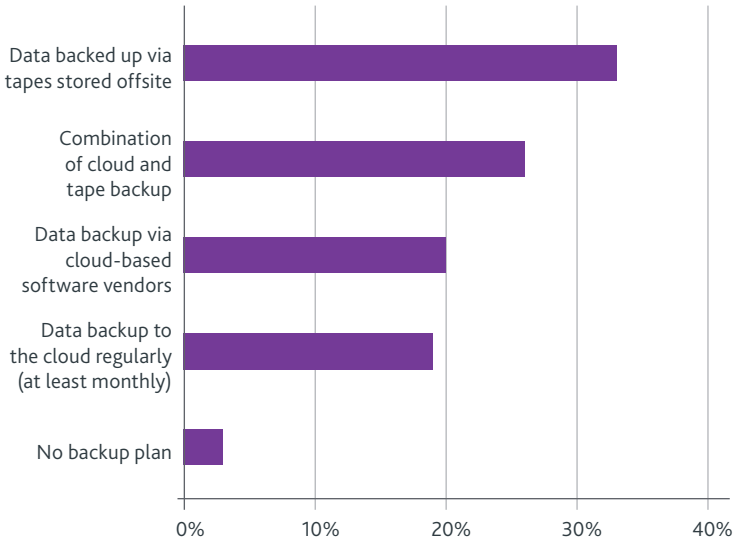

FIGURE 6: **Which of the following best describes your firm's data backup plan?**

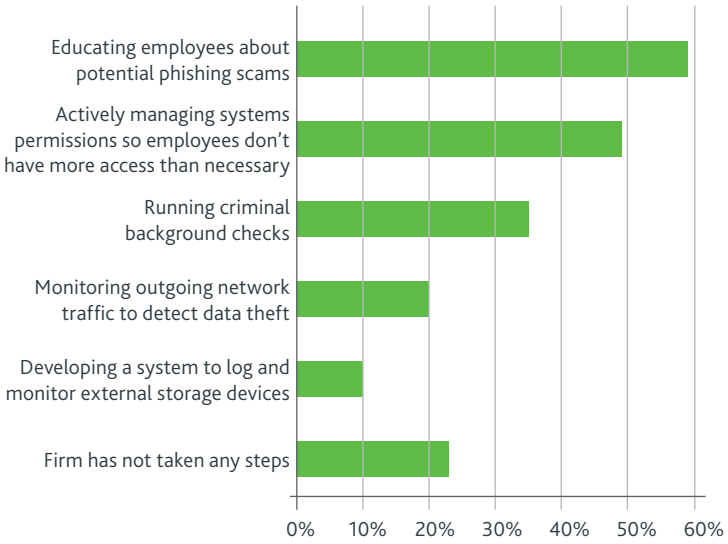

FIGURE 7: **What steps have you taken to protect your firm from insider threats?**

How to Protect through Action

- **Conduct a security audit.** If you don't know what parts of your business are vulnerable or what data you have that needs to be protected, you can't properly secure it. It is critical that you work with a professional to audit your entire IT infrastructure — computers, network, mobile devices and cloud applications used (known or unknown) — to determine what you need to do to prevent hackers from accessing client information.
- **Conduct a social engineering experiment.** Many firms in the Boomer Technology Circles™ have hired outside companies to create "phishing" emails to be sent to their staff. The technology department then uses the results from the experiment to educate staff on best practices when it comes to email. The firms that have done this regularly have seen a significant drop in viruses and other issues due to email.
- **Educate staff on their important role in security.** Your staff is your front line of defense when it comes to security. Sure, hackers can access your network remotely and siphon off data without setting foot in your office. However, vigilant employees (consultants, partners and vendors, too) can ensure that human error — which is a big cause of data security breaches — is minimized.
- **Use multiple strong passwords.** Too many of us use simple passwords that are easy for hackers to guess. When we have complicated passwords, a simple "dictionary attack" — an attack by a hacker using an automated tool that uses a combination of dictionary words and numbers to crack passwords — can't happen. Don't write passwords down; use password management services, also called identity management solutions.
- **Encrypt your data.** Encryption is a great security tool to use in case your data is stolen. For example, if your hard disk is stolen or you lose your USB thumb drive, whoever accesses the data won't be able to read it if it's encrypted. Keep in mind that email is not encrypted, but there are ways to make client communication secure and protected.
- **Back up to the cloud.** Security is important, but if your data is not backed up, you WILL LOSE IT. Ensure that your data is properly backed up, and test the backup to ensure that your data can be recovered when you need it.
- **Be aware of where your data is stored.** Perform a regular application and use audit. Understand what employees are using to perform work, where this information is stored and who has access.

This attention to data security can actually bring your firm full circle. We started this discussion with a look at protecting your client through knowledge advice. Businesses come to your firm for strong advice on financial matters. If you have strong internal security policies that are understood and enforced, you can also protect your clients by sharing what you know regarding data security.

Strong policies and technology solutions are often the end of the discussion on the best ways to protect clients. By bringing the focus of the protection back to client service, we shift from a focus of security and compliance to effective answers, advice and support. We can then offer our clients the security that their business is safe as well.