Cybersecurity Risks to CPA Firms

Mitigating the Perils of Data Collection and Retention

By Yigal Rechtman and Kenneth N. Rashbaum

In Brief

CPAs rely upon various forms of technology to accumulate data related to the work at hand, be it an independent audit or a tax return. While this data is needed to execute professional services, its very retention represents a potential security threat. This article discusses the nature of these threats, both internal and external, and ways to reduce risks presented by a result of data retention.

"You can have data without information, but you cannot have information without data."

—Daniel Keys Moran, programmer and science fiction writer

CPAs accumulate and analyze data in the form of financial information. The "data sets" exchanged by accounting professionals range from ubiquitous check registers and electronic trial balance spreadsheets to complex databases and valuation analyses. Now, and increasingly in the future, these will be viewed on electronic screens of all sizes, signed using various technologies, and stored somewhere in the vast silos of audit and tax workpapers. In the age of mobile electronic devices, more audit information is accumulated than ever was on paper, and it is easier to lose. Rule 301 of the AICPA's Code of Professional Conduct requires that CPAs "shall not disclose any confidential client information without the specific consent of the client." *Disclosure* includes the loss of information to unauthorized individuals by malware, inadvertent disclosure, or other means. All CPA practice areas, including tax, audit, advisory, and other services, are affected by this ethics requirement, as well as by state and federal legal confidentiality requirements, because of practical considerations that entail the collection of massive amounts of confidential or private data. As malware proliferates and cyber attacks increase, how can auditors meet the professional standards that require audit information to be secured?

Compliance Risks

CPA firms are both data collectors and data custodians. This is derived from U.S. GAAS, which requires CPAs to collect large sets of data. AU-C 230 summarizes the requirements of audit evidence as providing 1) evidence of the auditor's basis for a conclusion about the achievement of the overall objectives of the auditor, and 2) evidence that the audit was planned and performed in accordance with GAAS and the legal and regulatory requirements that apply to it (http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-C-00230.pdf).

Thus, the collection of evidence by auditors is presumed to be a basic part of quality control, and the foundation of any well-designed audit or attest service. From a tax practice perspective, the Statement on Standards for Tax Services (SSTS) 3, *Certain Procedural Aspects of Preparing Returns*, instructs: "Even though there is no requirement to examine underlying documentation, a member should encourage the taxpayer to provide supporting data where appropriate" (http://www.aicpa.org/InterestAreas/Tax/Resources/StandardsEthics/StatementsonStandardsforTaxServices/DownloadableDocuments/SSTS,%20Effective%20January%201,%202010.pdf). Much of the information that is collected during the preparation of a tax return is retained by the tax preparer, and most often it is in an electronic format. Thus, data sets of tax-related information are accumulating in CPA firms' data centers in growing volumes.

Functionality versus Security

CPA firms recognize that a "paperless environment" will increase the efficiency of tax and audit services, expand the scope of such services, reduce the size of audit teams, and improve gross margins that are sustainable in a competitive environment. The term paperless office was coined four decades ago to describe the predicted expansion of all computers, and in particular personal computers, in business; CPA firms were early to adopt and quick to adapt to these resources (*BusinessWeek*, June 30, 1975, pp. 48). On one hand, this adaptation produces better results, albeit with added complexities. On the other hand, professional firms, and CPA firms in particular, are finding themselves guarding silos of information that could be misused by others.

The threat of misused information is not limited to accountants, and the expanded use of technological functionality to provide increasingly efficient services constantly introduces new risks. The amount of data stored continues to rise dramatically: In 2015, the global storage market is forecasted to grow from $23.5 billion to $30.3 billion, a 29% jump (http://www.statista.com/statistics/203386/global-market-forecast-of-it-storage-from-2007-to-2015/).

For many professional service firms, such as law firms, medical practices, and particularly CPA companies, data sets that are never purged will likely stagnate in servers, either at the firm-level network, or shared through "infrastructure as a service" (IaaS) or "software as a service" (SaaS) cloud based provisioning. (For additional discussion of cloud computing, IaaS and SaaS, see "A CPA Primer on Cloud Computing" by Michael Pinch, http://www.nysscpa.org/ezine/ETPArticles/PM62509.htm.) The threats against data sets for professional offices of any size stem not just from computer hackers; the threats are more nuanced, and the solutions to address these threats have to be creative, adaptive, and thoughtful.

Data Threats

Data that has been collected and retained by a professional can pose a threat by its very presence. Who has not been surprised to find a file, such as an audit or tax worksheet, from 20 or 30 years ago tucked away on a shared folder on a server? These data sets can become a threat when legal or regulatory challenges face the company with a subpoena or discovery request. On the other hand, there is a risk that a piece of data will not be timely found, causing an adverse legal inference to be raised [*KCH Services, Inc. v. Vanaire, Inc., et al.*, F. Supp. 2d (W.D. Ky July 22, 2009) (Civil Action 05-777-C)].CPA firms learned this when asked to produce "all relevant" documents, including any electronic documents, that were retained in connection with massive frauds such as the Madoff Ponzi scheme, the BP Deepwater Horizon oil spill, and others. Besides the risk that the data will be inadvertently not turned over, and the consequences thereof, there is the risk that data will contain evidence damaging to the firm itself.

Internal Threats

Internal threats are often presented by individuals who are authorized to access data sets and decide—for a variety of reasons—to misuse the data either during or after the access period. Employees are the most common individuals on this list, but professional firms should be mindful that the obvious threat is not always the most common. Controls over employees' access are often built into various software and access points; for example, tax software developers have responded to e-filing requirements by restricting access to client's bank accounts. Other parties, how-

ever, may be less likely to be questioned about data breaches, positioning them to misuse and abuse the intangible value in data sets. Although the overall tax returns are sometimes open for every employee to view, the mass collection of personal identifying information can and should be restricted on a need-to-know basis.

Increasingly, vendors have access to data sets and data centers without much control over their activity. This includes, but is not limited to, janitorial providers, heat and cooling service providers, and IT consultants. Even if the service provider (e.g., a HVAC-related company), is not a hacker per se, it represents a weak link in the electronic perimeter of the firm. This is how, in November 2013, the internal network of the retailer Target was hacked: the credentials of a third-party provider were stolen and misused by hackers who stole records from Target (Paul Ziobro, "Target Breach Began With Contractor's Electronic Billing Link," *Wall Street Journal*, Feb. 6, 2014).

Less obvious, but also ubiquitous, are the risks from "bring your own device" (BYOD) programs. This business practice allows individuals' electronic devices to connect to their employer's network. BYOD opens network access for information theft, the extent of which has not yet been fully explored. These devices are often configured in inconsistent ways, making it difficult to standardize the controls to limit the possibility of a breach. For example, individuals may not timely apply software patches to their devices, or different configurations by cellular carriers may require some devices to contain suboptimal controls on access. Of course, the largest risk is loss of a device and discovery by a person who might sell the contents found on the device's memory.

External Threats

Hacking activity keeps rising in our interconnected world. Kaspersky, a cybersecurity firm, reports that 54% of hacking attempts in 2013 occurred in the United States. Significant among the findings is that hacker activity rises at a rate of 25% rate every three months (http://securelist.com/analysis/kaspersky-security-bulletin/58265/kaspersky-security-bulletin-2013-overall-statistics-for-2013/). Accordingly, regardless of the absolute number of hacker attacking systems in the United States, professional firms of all sizes are targets. Even major cloud computing servers such as Google or Amazon are continuously tested and retested for vulnerabilities. Moreover, mobile devices are also continuously monitored by hackers, who see these devices as a way in to corporate servers.

Familiarity with hacking risks gives most professional firms a false sense of security. Hackers, unlike virus attacks, work hard not to leave any virtual "bread crumbs" that indicate that an unauthorized visit has occurred. Stolen client data can surface months or even years after it was taken. At that point, little can be done to trace when or how the breach occurred, much less correct the problem. The damage is often steep in both direct financial costs and indirect reputational damages.

Risk reduction should primarily address obvious, common sense controls over data sets that a CPA firm retains.

Reducing the Risks

Professional firms should be versed in the risks of electronically stored data and address them head-on. In 2014, the New York State Department of Financial Services (DFS) issued a cybersecurity protocol for banks; this represents a good benchmark for professional firms of all sizes and a place to begin the process of protecting one's data ("DFS-Regulated Banks to be Examined Based on Cyber Security Protocols, Governance, Third-party Vendor IT Security, Other Issues," DFS, http://www.dfs.ny.gov/about/press2014/pr1412101.htm). The list of controls is extensive.

Risk reduction should primarily address obvious, common sense controls over data sets that a CPA firm retains, such as the following.

Review access controls. Access to data should be handled on an "as-needed, when-needed" basis.

Regularly purge proprietary and generic data sets. This includes tax return data beyond a given expiration period, and should also apply to "unassociated" data (various spreadsheets or documents strewn around a server). One way to purge unclaimed files is to have a manual or semiautomatic sweep of folders and files that have not been accessed for some time, and collect them in a keep-or-purge file. If the files are really not needed after a given period of time, they are then removed. Of course, a thorough review of an organization's quality control and retention policy should be made, and an attorney should be consulted for any special circumstances when retention is imperative.

Review cloud-based service providers. Both IaaS and SaaS providers should be able to give some assurances on the ways that they mitigate internal and external threats. These assurances, often in an attestation report under SSAE 16, are a good starting point to confirm that data in the cloud is protected and reasonably secured. CPA firms should be extra careful when implementing contractually obligated activities. The SSAE 16 report specifies controls required to design and implement the virtual seam between the service provider and the company.

Obtain insurance that properly addresses the potential exposure of the firm to internal and external risks. Insurance clauses should cover both the direct costs associated with a breach and the indirect costs, such as regulatory inquiries, fees to review a legal discovery request, and defense costs in the case of a deleted file that should have been retained. Most standard insurance policies exclude hacking attacks or contain high deductibles and limited maximums for such incidents.

Train, vet, and monitor employees, vendors, and even customers. Any party that could have access to a firm's data set is a

potential entry point for internal or external threats. Monitoring vendors and creating contracts with "right-to-audit" clauses provide useful tools to ensure that vendors are compliant with the firm's tolerance for risk. Entities that qualify as a "business associate" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or are covered under various other federal or state regulations (such as anti–money laundering rules), are advised to establish and enhance their vendor qualification processes.

Create a written information security plan (WISP). A WISP should include identification and response protocols enforced by the firm in response to a breach incident. An effective WISP program includes responsibilities for day-to-day operations, assignment of tasks (e.g., network monitoring, vendor qualification, breach notification, training), as well as contacts and protocols to follow when a breach has occurred (e.g., legal notice, legal holds, public relations response, workforce notification).

Data Retention: a Double-Edged Sword

As auditors and tax advisors accumulate data and turn it into useful information, the underlying data is often retained—with good reason. In the past, data retention introduced the complexities of data access and organization, and presented challenges in terms of retrieving it in an efficient way and providing it to users who need it. As data grows exponentially, it causes professional firms to become a target for unauthorized use.

Recognizing this new trend, and addressing it with a set of coordinated and creative moves, can put a firm ahead of the rising tide of exploits, hacks, and other damaging activity. Furthermore, CPAs, as trusted advisers, can grow their professional offerings by preaching what they practice: knowledge gained from understanding the value and vulnerabilities of data sets can be valuable to many clients as well. Other professional clients would be first on that list, but services could be expanded to other clients who utilize intellectual property data sets (such as manufacturers) and customer and vendor data sets (such as retailers).

By recognizing the threats, addressing the risks, and creating an effective plan of counterattack, CPAs should be well positioned to continue do what they do, do it well, and assist their clients in an ever-growing aspect of professional services. ❑

Yigal Rechtman, CPA, CFE, CITP, CISM, *is a senior manager for litigation support and forensic accounting at Grassi & Co., as well as an adjunct professor at the Lubin School of Business, Pace University, New York, N.Y. He is a member of* The CPA Journal *Editorial Board.* ***Kenneth N. Rashbaum, JD,*** *is a partner at Barton LLP, New York, N.Y., and an adjunct professor of law at the Maurice A. Deane School of Law at Hofstra University, Hempstead, N.Y.*