rewind

What Accountants Need to Know About Safeguarding Client Data

By: Mike Potter, CEO

Table of Contents

Introduction 3

Cybercriminals: How Do They Do It? 4

Designing Your Firm's Information Security Plan 6

Getting Started 8

About Rewind 10

Introduction

Contrary to popular belief, data leaks don't just happen to people who are unfamiliar with computers or the internet. Data is stolen every single day. If you think it's never happened to you or your firm–it likely has, and you probably haven't even noticed it. Data loss is more common than we'd all like to believe.

According to a multi-year study by IBM, the odds of experiencing a data breach within two years was 29.6% in 2019. The same study revealed that 24% of cybercrime occurs because of human error and 51% due to malicious attacks (the remaining 25% is due to system error).

The fact that three-quarters of data leakage is due to human error and lack of security means that the power to flip that statistic upside down is in our hands. It's up to individuals to take responsibility for safeguarding data.

"Many people think that backups are a thing of the past, now that everything is stored in the cloud. However, it is important to note that not all cloud solutions are created equal and not all of them are securely storing your data."

– Jacob Schroeder, CPA,
CEO + Founder, Ascend Consulting LLC

Cybercriminals: How Do They Do It?

Here are some of the most common ways that data is stolen from individuals and entities alike. It's important to be familiar with these areas in order to create multiple points of protection for client data.

> *"Cybercriminals work hard through various tactics to penetrate your network... They may steal the data, hold the data for ransom, or use your own computers to complete and file fraudulent tax returns."*
>
> *- IRS Publication 4557, 2018*

Malware

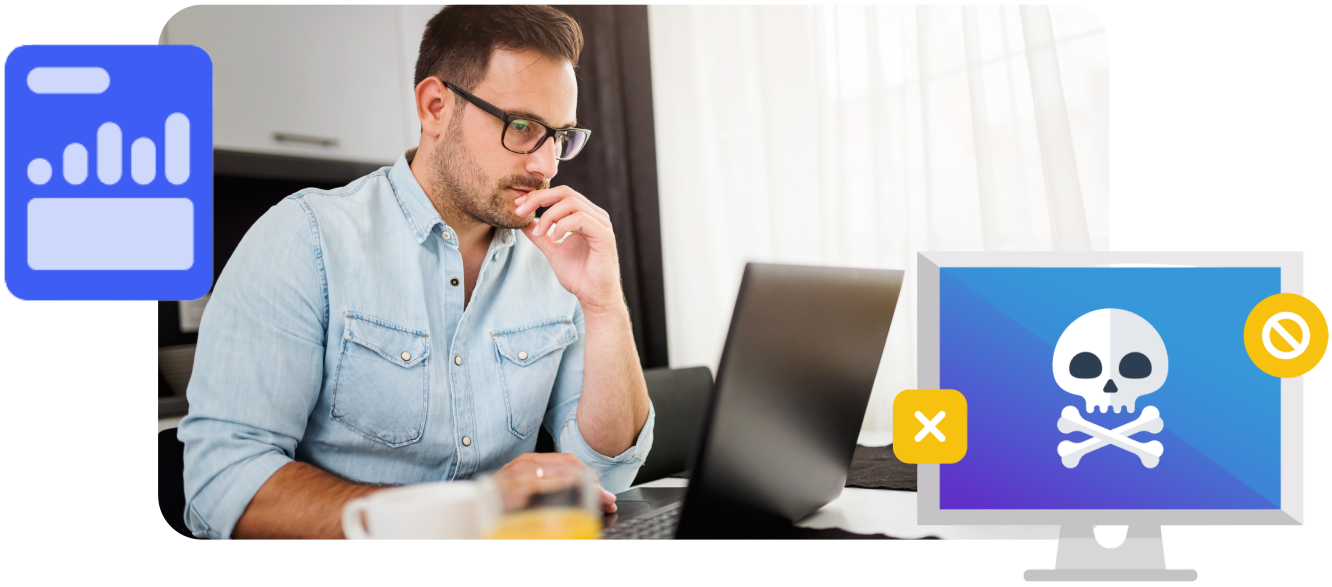
The word malware refers to "malicious software" (PnC). There are many types of malware, and variations of every type are continuously being reinvented by cybercriminals.

Here are some common types:

- **Viruses**, which hide in downloaded programs. The virus is dormant until the program is opened by the computer's user– it then springs to life, infecting and disabling the system.
- **Ransomware** works by gaining access to sensitive data in a computer system and holding that data "ransom" for a payout. If the victim doesn't comply, the data is deleted or rendered irretrievable through encryption.
- **Worms** are similar to viruses in that they are downloaded from external sources, but they don't need a program to 'live' in. They can hide in documents, files, or even network connections. Worms quickly multiply across whole networks, causing disruption and data loss.

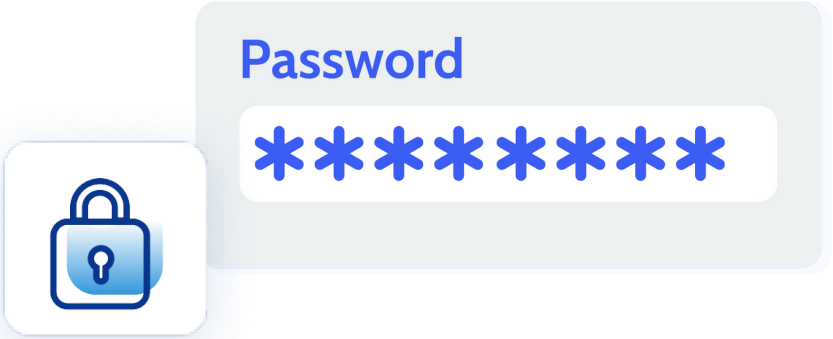
Phishing

Phishing attacks occur primarily through email, but can also happen through cleverly designed websites, text messages, or even voicemail messages. Unlike malware, there's usually an individual on the other side of the communication. It's a dangerously effective scam in which the perpetrator poses as a trusted individual or company—sometimes even using familiar names of family members or friends. When the victim clicks a link in the email or communication, they might accidentally download malware, or share sensitive personal information.



Password Theft

Most cybercrime seeks the same information: The user's online credentials. A username and password is often the only barrier preventing a hacker from accessing bank account numbers, addresses, phone numbers, and practically the user's entire identity. Usernames are commonly publicly displayed, so the password is the only information left to find. Tools used by hackers to find out passwords are so simple that they involve guesswork. This is highly effective because people are so afraid of forgetting their passwords that they set predictable, memorable, guessable passwords. And according to PnC, "...many consumers continue to use the same password across different online platforms, so once one account is breached, they all are at risk" (2018).



Designing Your Firm's Information Security Plan

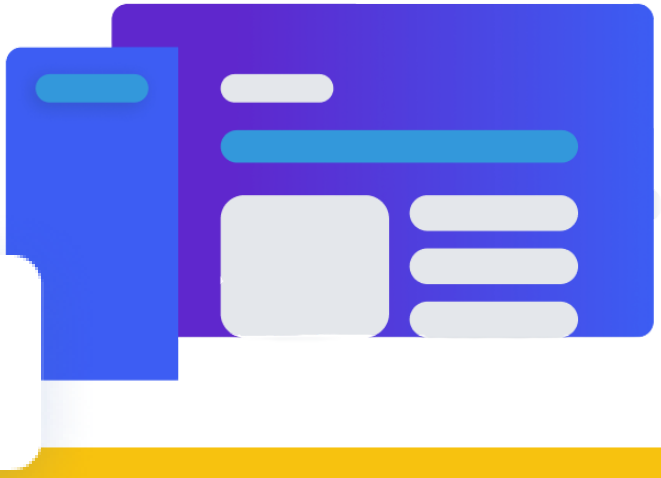
Security doesn't just happen by chance—it requires planning. Your firm and your clients will benefit from a comprehensive security plan that includes accountability checks, clear roles, and responsibilities.

What the Rules Say

Since the Gramm-Leach-Bliley Act was passed by the Federal Trade Commission in 1999, all financial institutions are required to comply with the Safeguards Rule in order to protect their client's data. The FTC defines financial institutions as any business that is "significantly engaged in providing financial products or services."

For example:

- Professional tax preparers
- Bookkeepers
- Financial advisors
- Accountants
- Mortgage brokers
- Hedge-fund managers
- Real estate appraisers



"Our Information Security Plan started with a generic template, then expanded it to cover our internal processes and operations. But the most important piece of safeguarding your client data is not the plan itself, but making sure your staff abide by the policies in it."

– Jacob Schroeder, CPA,
CEO + Founder, Ascend Consulting LLC

Be Compliant, Not Complacent

To be in compliance with the FTC's Safeguards Rule, accounting firms must maintain a "written information security plan that describes their program to protect customer information."

The firm's plan should include the following:

- At least one employee named as the coordinator of the plan
- Identification and assessment of the risks to customer information in each relevant area of the company's operation
- Regular monitoring, testing, and adjustment of the plan whenever relevant
- Requirements that ensure all the necessary safeguards can be maintained by any 3rd party service providers

For a complete description of the Safeguards Rule, visit the Federal Trade Commission website.

Getting Started

Protect Stored Client Data

As part of their obligation to protect stored data, all accounting professionals should ensure they back up their client's data regularly. Accounting industry professionals are required to safeguard taxpayer data to protect it from data theft or accidental loss and damage.

"It is mandatory that our client's data is backed up. There are numerous reasons for this. For example, natural disasters, physical theft, digital theft, hardware or software failure, and employee unintentional mistake or intentional fraud. All of these reasons present a solid use case for backing up data and I'm a 100% advocate of backing up all data offsite and on a different platform."

–Caleb Jenkins, EA, CQP, RLJ Financial Services, Inc.

Cloud accounting software like QuickBooks Online has an all-or-nothing approach to backing up user data. Many SaaS providers, including QuickBooks Online, follow the Shared Responsibility Model. This means that they back up their operating structure in case anything disastrous happens, like an earthquake or flood. However, as part of the Shared Responsibility Model, account-level data is the responsibility of the user. That means that if account data on their system is damaged or lost due to human error, upset ex-employees, cybercrime, or a dozen other threats–it's irretrievable.

In order to recreate and restore compromised databases, the data must be backed up in a separate system, outside the original platform.

In the end, liability always falls onto the professional to ensure that their client's data is secure. Firms must perform due diligence to ensure that their clients' data is backed up, encrypted, and safe.

"Prior to using Rewind for backups, it felt like going out on a limb when we needed to make massive changes to the structure of clients' data and we couldn't go back. Now, we can restore data as needed and know that we won't create a bigger mess."

–Geni Whitehouse, CPA, International Keynote Speaker, Even a Nerd Can Be Heard

Password Strength

Even complex passwords are guessable by hackers, especially when AI is employed. Use a password generator to create extremely unique passwords that are essentially un-guessable. Passwords should be so complex that most people would seriously struggle to memorize them– that's why password "wallets" exist. There are many options available, like 1password, Lastpass, Dashlane, or Bitwarden to name a few.

Spot Data Theft

Data theft does happen, even with the best protections in place. It's crucial to stay on guard and keep a critical eye trained on all systems that interact with sensitive data.

From IRS Publication 4557, here is a list of some common signs that data theft has occurred.

- → Client's e-filed tax return is rejected because a return with their Social Security number was already filed
- → Clients who haven't filed tax returns receive refunds
- → Clients receive tax transcripts they did not request
- → The number of returns filed with the tax practitioner's Electronic Filing Identification Number (EFIN) exceeds the number of clients
- → Tax professionals or clients respond to emails that the practitioner did not send
- → Network computers begin running slower than normal
- → Computer cursors move or change numbers without touching the keyboard
- → Network computers lock out tax practitioners

Reporting Data Loss

When data loss occurs, it's imperative that ego and embarrassment are put aside so the breach can be addressed swiftly and transparently. Sharing clear communication around exactly what happened can go a long way in preventing further information loss and theft. Review the FTC's Data Breach Response: A Guide for Business for more detailed guidance on responding to data loss.

Educating Clients and Your Team

Most data loss can be prevented with consistent education and a robust information security plan. For more reading on data security best-practices within the accounting industry, explore Online Data Security for Accounting Professionals next.

Ready to build your firm's backup strategy?

Learn more about implementing Rewind for your QuickBooks Online clients.

rewind

About Rewind

Since 2015, Rewind has been on a mission to help businesses protect their SaaS and cloud data. Today, over 80,000 customers in more than 100 countries use Rewind's top-reviewed apps and support to ensure their software-as-as-service applications run uninterrupted. The Rewind platform enables companies to back up, restore and copy the critical data that drives their business.