Guide to Financial Security: Accounting Systems

Financial data security determines the well being of your entire organization. As businesses rely more on cloud-based technology, this presents many opportunities, but also challenges. Cloud accounting and other operations still face major security threats. As you investigate accounting solutions, security must take precedent. This guide will help you understand the threats to your financial data and help you pinpoint critical features needed for a truly secure accounting system.

We'll answer the following questions:

- How does cloud-based accounting data impact your company's well-being?
- What are the threats to your accounting system?
- What are the costs of an accounting system breach?
- What are the steps to secure your accounting system?
- How can accounting technology help or harm your financial security?
- Why is an accounting platform vs application safer and stronger?
- What are essential features for modern accounting data security?

accountingseed

CONTENTS

How does cloud-based accounting data impact your company's wellbeing?

Accounting data is one of your biggest assets in running and developing your business. However, this data can become your biggest liability if unsecure.

ACCOUNTING: YOUR GREATEST ASSET

Accounting, particularly in the cloud-based environment, is extremely insightful. Besides being able to more accurately and efficiently manage day-to-day finances in real time, accounting data is critical for understanding your customers and business performance.

Through automation and connectivity to other business tools, your accounting data can be accurately housed and used to assess the financial dimension of each aspect of your business. Return on investment for products, projects, staff, and other resources are clearly visible. Accounting data empowers you to make better decisions for both business operations and customer satisfaction. You have a lot to gain through clear, automated accounting. However, the benefits of this data can work completely against you if the system is breached.

UN-SECURE ACCOUNTING: YOUR GREATEST LIABILITY

When your accounting data is improperly secured, your company's livelihood, work efficiency, and reputation are at stake. If the financial data is corrupted, altered, or stolen this will affect all of your business processes. Your entire IT management system could be working with false or inaccurate data. Data theft could leave critical amounts and key information absent or exposed. This is the greatest danger.

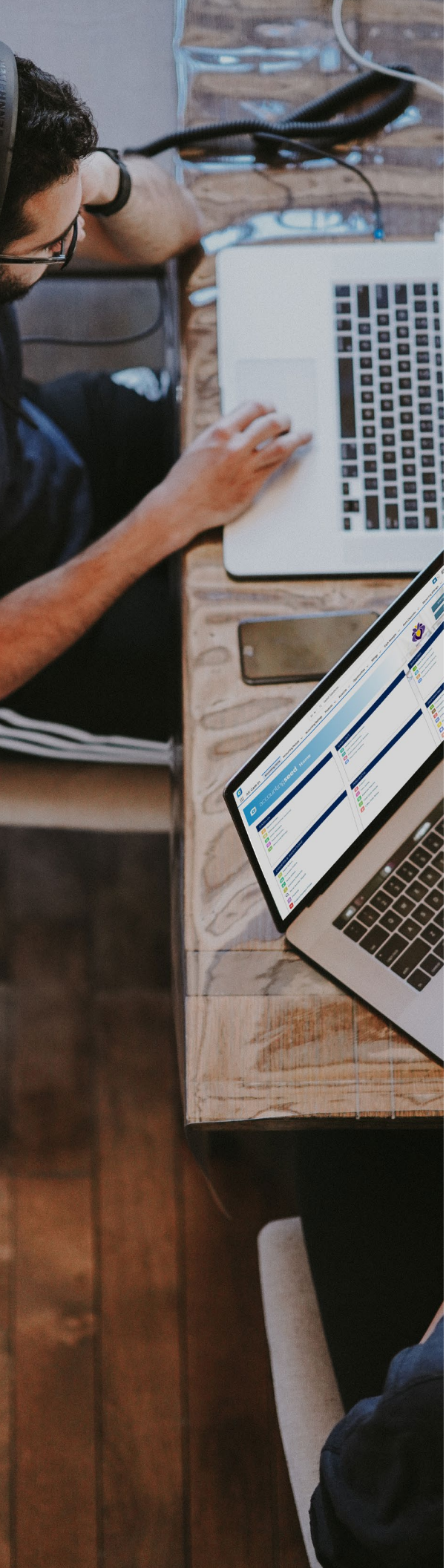
Stolen financial data can include:

- Account numbers
- Transaction details
- Credit card numbers
- Bank accounts
- User names
- Passwords
- Personal and private information

If this information is stolen, your company risks potentially millions of dollars in loss. Besides your own accounts being attacked, your customers may also experience financial theft. In addition to the monetary impact on your company, potentially staff, and customers, your company may be held responsible for compensations to customers. More money has to be funneled into reparations and legal fees as a result of the breech. But that's not all. Any accounting security breach can damage your reputation and threaten customer relations. Customers may leave and prospects may look elsewhere if they feel working with you is unsafe.

What are the threats to your accounting system?

Many people think that hackers are the biggest threat to your IT and cloud accounting system. It's absolutely true that hackers are a major threat, and certainly top of mind in the news. But they aren't the only, or greatest, threat. Your accounting system has three primary vulnerabilities: environmental/incident, external, and internal threats. But you also have potential threats with the technology you actually use too. To fully secure your financial data, you must account for all of these threats. A lapse in any of the following will still result in the loss, damage, or theft of financial data.



ENVIRONMENTAL AND INCIDENT THREATS

Natural disasters and structural damages can threaten your financial security, while outdated equipment or IT failure could jeopardize it as well.

A few of these threats include:

- Flooding
- Tornadoes
- Power outages
- Computer damage
- Data backup failure

Events like these can cause data to be lost or destroyed, which will leave you and your team scrambling to recover the information. However, cloud-based accounting solutions easily counter these types of problems. Through automated backups and by storing data on the cloud in remote servers, your financial data is always accessible and safe even when the office or equipment is compromised. This is one of the reasons why cloud-based accounting systems are essential for modern businesses. While being on the cloud effectively protects your data from natural disasters, your accounting still faces several financial security threats from people.

EXTERNAL THREATS

You already know that accounting systems face threats from cybercriminals. These represent the threats that are external to your company, individuals purposefully trying to penetrate your IT architecture to steal financial data or cause you harm.

A few examples of external accounting threats include:

- Hackers
- Phishing scammers
- Malware
- Spyware

Remember, the cloud is not a physical safe you can guard. While your data is safely accessible by staff any place and time, people can break past your IT security to access the data too. The ease of accessing your accounting data on the cloud, means that criminals anywhere can potentially do the same. Malware spread and data theft from hackers are definitely a cause for concern for all levels of companies, especially with accounting data.

2019 alone saw big companies like Toyota and even financial institutions like Capital One succumb to hacking. Millions of customers' information were exposed, which was devastating to both companies in reputation and recovering costs from the breaches. Unfortunately, the rate of hacking and data theft is precipitating. In 2020, during the COVID-19 crisis when many businesses increased their use of cloud tech, hacker activities dramatically increased too. As remote work and cloud-based accounting increase, so will cybercrime. However, the deadliest threats to your financial security can actually be within your company.

INTERNAL THREATS

Hackers are the most obvious threats to IT security, but the biggest, most costly financial security risks are within your own company. This happens when untrustworthy staff have access to view, steal, alter, and/or falsify accounting data for their own purposes. Recently, internal fraud and data theft have dramatically increased alongside hacking.

Malevolent threats include:

- Internal data theft
- Falsifying financial statements
- Stealing financial data
- Data or process tampering
- Hiding accounting errors or concealing actual finances

60% of all cyber attacks are rumored to be conducted by employees with mal-intent. This type of security failure is seen by many customers as a breach of trust or monumental incompetence on the part of leadership. Hacking is an attack on the company, but an internal data breach constitutes a lapse, on some level, of lack of oversight or negligence. Although both internal and external financial data breaches are serious, it may be harder to fully recover from an internal breach.

Recently, Forbes reported that 61% of internal database breaches were done by individuals who were not in leadership roles. According to a report by Verizon, "20% of cybersecurity incidents and 15% of data breaches are due to misuse of privileges."

Besides public and customer perception, an internal data breach is more financially damaging too. The level of knowledge and control individuals have within the accounting system means more high-level accounting data can be compromised - resulting in even higher costs than hacking. Though, unlike hacking, some internal accounting data breaches are not malevolent. Internal threats also include unintentional actions that jeopardize your accounting.

Here are non-malevolent internal security risks:

- Human errors
- Improper data handling
- Financial mistakes
- Accidental data sharing

Some of the biggest internal security breaches are the results of mistakes. Whether by a combination of technology or staff errors, these security breaches can be just as damaging as internal fraud or corporate espionage. If staff are using ineffective technology, this can easily precipitate inappropriate information sharing and data alteration.

Primarily, internal breaches occur when employees perform actions they shouldn't be doing, and/or have access to accounts that they shouldn't be allowed to view or alter. About 40% of senior executives have cited that internal accidental data sharing is a big security issue. Additionally, 80% of breaches are attributed to human error.

TECHNICAL THREATS

You'll see throughout this guide that the design and features of your accounting tool, or lack thereof, are imperative in financial security. Some accounting systems are simply ineffective or outdated.

Here are some general technical threats:

- Old or unupdated cloud accounting system features
- Poor encryption capabilities
- Lack of user role designations
- No password and username protection
- No notification system
- Audit trail function is lacking
- Poor or limited data redundancy measures
- Vague process definitions

If your accounting system isn't up-to-date with features that protect access or have tools to notify you of security issues, this is a major risk. First American Financial's 2019 data breach exposed over 800 million records as the direct result of poor database design. Their system allowed data to be visible to anyone using a web browser for more than two years. Because of this, tax records, bank accounts, and even Social Security numbers were exposed. Why? Because the data required no username or password to access it. Something as simple as requiring a password is the first line of defense in preventing both internal and external data theft, yet this was absent. The IT system failed First American Financial, but they should have thought to check for and establish proper controls.

Without cloud features that define work rules, processes, and access, anyone with or without access can damage or expose financial data in the accounting system.

What are the consequences of accounting system breach?

There are many damaging and long-lasting consequences of accounting system breach. We've addressed several, but to help you pinpoint a secure accounting solution, it's important to understand what's at stake.

YOUR BUSINESS CAN FAIL

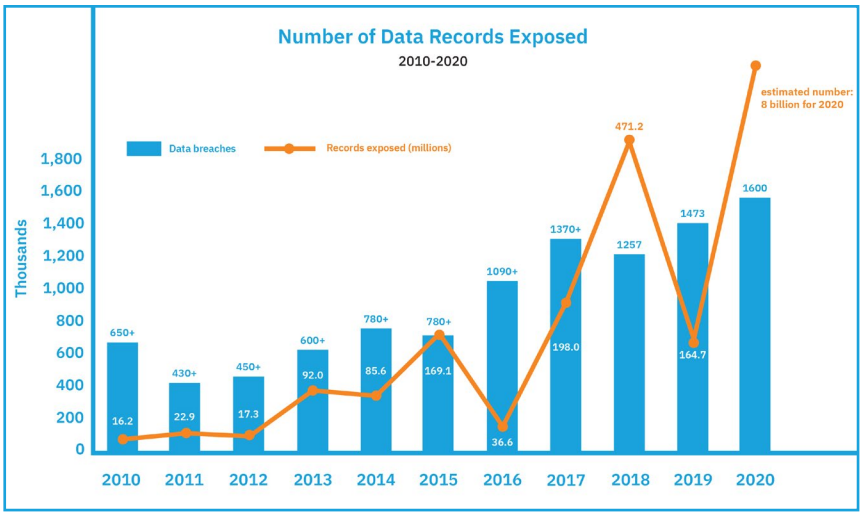
Companies worth millions have completely failed because of security breaches. This includes external data theft and internal data breaches, or sabotage. When accounting data is involved, the situation becomes more dire. Besides the fact that money is directly at stake, personal information and strategic business data are tied to the accounting life cycle so all this information is at risk.

This loss represents a major blow to your business objectives, cash flow, and IT integrity. Again, loss of customer trust can occur if their information and accounting data are affected, causing them to leave, and prospects to drop interest. If you're a larger company or a nonprofit, investors and sponsors alike may also be affected. These groups might withdraw support and/or pursue legal action that could further entrench your financial burdens. The financial costs of trying to recover, coupled with the chaos of reorganizing, might be too much to handle depending on the scope of the breach. Even if your business survives, an accounting system breach is a costly proposition that will affect you for months, maybe years, ahead.

THE COSTS OF DATA BREACH ARE ONLY RISING

What does an accounting system security breach look like once it happens? Expensive. On average, U.S. businesses typically face a loss of $8.19M per breach. All over the world the costs do range but are still very high. According to a recent article post by CSO Digital Magazine, "Each record lost costs around $150 on average globally; in the U.S. that figure rises to $242 while in the U.K. the cost is $155 per record."

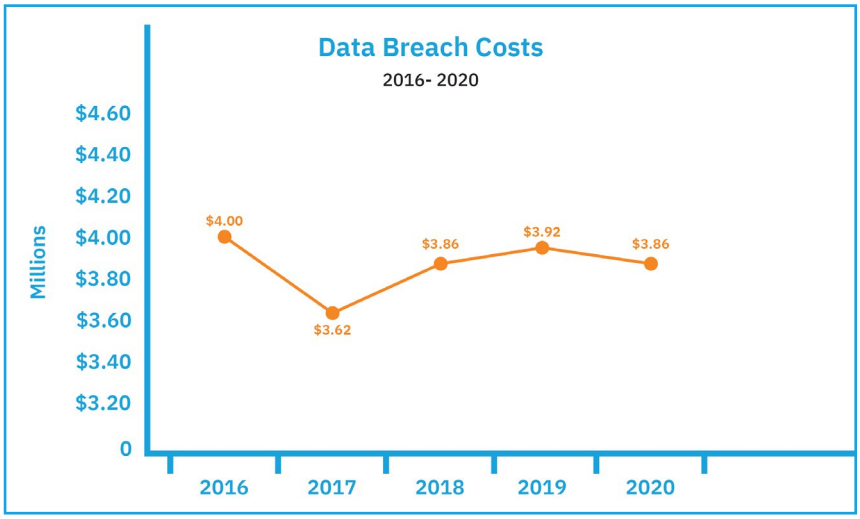
While cases of millions of data records being lost or compromised are still uncommon, data breaches involving thousands of records are increasing. With the scope of data breaches intensifying, so are the costs of dealing with them. Accounting-related data is consistently the most common data attacked and stolen.



This data was compiled from expert sources including Market Watch, The Insurance Information Institute, IBM, and Security Intelligence.

> **Each record lost costs around $150 on average globally; in the U.S. that figure rises to $242 while in the U.K. the cost is $155 per record."**

As you can see, the rates of data threat continue to climb. Some experts even estimate that the average cost of a data security breach for enterprise-level organizations could surpass $150M. This is directly attributed to increased use and connectivity of the cloud. Of course, the recent data breach spikes following COVID-19 seem to be confirming the rate.



This data was compiled from expert sources including IBM and Security Intelligence. As evidenced by the data breach of major data services provider Blackbaud, significant data breaches may not even be discovered until much later than when they occur. The results have already launched Blackbaud into a formal lawsuit:

"The suit stems from a data breach which happened on Feb. 7 and was not discovered by the company until May 14. Users were not notified until July, as reported exclusively by The NonProfit Times." - Richard H. Levey, The Nonprofit Times

This may indicate a lack of security features or sophistication within their IT systems, which could be indicative of other organizations.

The cost of data breaches can come in multiple forms:

- Lost revenue through data loss
- Costs of reparations to customers
- Potential downsizing
- Legal representation fees
- Fines
- IT/technology costs to mitigate or fix breach
- Time/money spent dealing with the data breach
- Potential backfees for payment delays
- Customer loss
- Missed business opportunities
- And more...

Besides compromising your plans for business growth and revenue streams, your whole company's peace of mind will also be damaged. As an organization, one cannot discount the effect such a loss will have on your own staff. People might not feel secure working for you after a data breach, or you might be forced to make staff reductions as a result. Remember, your accounting system security impacts your entire company. It also affects how you stand as an organization in your industry.

PENALTIES AND INDUSTRY DISCREDITATION

Part of the costs and consequences of accounting data insecurity relate to legal compliance. All organizations are beholden to tax requirements. If your accounting data is stolen or altered, this will likely affect your reporting efficiency. In addition to losing opportunities because of data errors, failure to meet the tax amounts and requirements will incur repercussions from the IRS. This can range from fines and other penalties on your organization. You may also experience delays as you're audited.

Different industries have more robust regulations regarding data security. For example, government contractors' accounting systems are required to be Defense Contract Audit Agency (DCAA) compliant to ensure government and taxpayer money is used safely and effectively. A data breach can indicate that the contractor is not working with DCAA compliant software, and or that controls are not in place effectively.

Even if a breach is accidental, this puts the entire contractor in question. This will make it harder to get more federal contracts because federal governments will not want to risk data breaches or potential fraud. This damages the contractor's industry status and will likely require an overhaul to regain face. For nonprofits, a financial data breach could jeopardize cost tax exemption status. This can also make patrons hesitant to support the cause, which can drastically reduce funding and other nonprofit benefits.

No matter the industry, there will likely be some type of compliance issue following a data breach. But, accounting data theft and loss discredits the organization. You immediately seem either incompotent, unsafe, or unprepared for the rigors of business. Patrons and customers will turn towards competition who are more secure. Why would they take the risk? The burden then falls on the organization to rebuild credibility and trust after the breach. Not to mention money and resources.

What are the steps to securing your accounting system?

While there are serious threats to your company's, even customers' financial security and data, these threats are controllable. Through a combination of process and technology, your accounting can be safe on the cloud. But remember, an effective plan is only effective if it can be implemented fully. Here are the first security steps you should take to secure your accounting system.

1. Know your threats

The threats outlined above are the overarching threats all modern companies face. Your individual company faces these threats, but also unique threats depending on your operation and industry. Try to be granular with your threat assessments. This lets you pinpoint functionalities you need in place to keep your accounting secure.

2. Know your regulations
Some of your security threats may be covered within business regulations you must follow. These regulations protect you, your customers, and ensure proper accounting standards. Again, government contractors and nonprofits are examples of heavily regulated industries, but be sure to check for your individual industry too. Review these regulations to incorporate them with your other financial security needs. This is critical for compliance.

3. Establish security requirements
Work with your team to identify risk factors and regulation demands to create a comprehensive financial security requirements list. Internal controls should be considered too, this plays a big role in defining the features and functionality you need from an accounting system. Accounting system approvers and decision makers must be identified. You'll also want to outline staff roles, responsibilities, and limitations to solidify safe protocols. Define how accounting data should be handled to ensure no mistakes. This also helps you identify data tampering. You may find that you want to engage in financial experts to establish proper controls.

4. Choose the right accounting system
After establishing financial security requirements, you need a secure accounting system. The reality is that basic accounting security features like usernames and passwords aren't enough protection anymore. Most accounting apps lack in-depth internal security features or are restrictive in their deployment. You'll need to be able to tailor the security requirements and processes to your specific needs. This is the biggest step in achieving a fully secure accounting system.

How can accounting tech help or harm your financial security?

A reliable, well secured cloud-based accounting system is your greatest defense, but only if it's fortified to deal with the threats you face. The truth is that many accounting solutions only offer basic security features. With the growing complexity of cloud technology, matched with your unique business processes and the rise of data theft, these aren't enough. Inefficient accounting solutions will harm your data security even with the best practices in place.

Remember, using only superficial IT protections leaves your accounting open to the more invasive threats. And again, if access restrictions and definitions aren't flexible and articulate to your needs, internal mistakes and data theft can easily occur. Bear in mind, internal data security measures also serve as a secondary layer of protection even if your accounting is penetrated by hackers. You need a full range of protections today that many accounting solutions don't offer.

Before looking at essential accounting data security features, it's important to distinguish areas where many accounting programs lack refined protections.

CORE AREAS LACKING ACCOUNTING SYSTEM SECURITY

Insecure IT infrastructure | Be sure to investigate any history of hacking for whichever accounting solution you consider. Several accounting applications have reports of stolen banking info and being easily hacked. This is usually caused by minimal encryption and transmission features. This can also be caused by poor Application Programming Interface (API) - how a solution connects to your accounts and other business tools. A secure cloud accounting tool will have a robust API and have a reliable cybersecurity design.

Spreadsheet emphasis | Spreadsheets are notorious for being prone to data errors and being insecure. Any accounting tool that makes you rely heavily on spreadsheets instead of consolidating

the data securely is a major risk. Spreading financial data out in spreadsheets makes accounting harder to manage, which also generates more costly mistakes. Access is difficult to control on spreadsheets. Anyone in or outside your company can see and damage the data. Once changes are made, they're almost impossible to detect until it's too late.

Activity monitoring | Leaders and decision makers should know when accounting data has been viewed or altered. This is critical for detecting any external or internal tampering. Not all accounting solutions will provide notifications of these instances, or may only have vague activity reports. To take corrective or preventive measures, you need to know what accounts were affected, how, and by whom in real-time.

Preventative measures | Preventing data errors, sabotage, and theft must be a core design of the accounting system. Many accounting systems have little functionalities that let you control the levels of accessibility. You'll want to be able to fully articulate the roles and levels of access each teammate has. This is essential for preventing errors and theft internally, as well as block hackers from penetrating the system should it be attacked.

Data management | Control your accounting data and you control the quality and accuracy of your finances. You also prevent people from falsifying or tampering with accounts. By defining rules and processes around how accounting data is logged, monitored, and used, you ensure mistakes are avoided. And as a bonus, you can identify suspicious or erroneous activity if people are trying to override or enter info contrary to the rules you define. More complicated measures like these are vital, but often absent in many solutions.

Data tracking | Many accounting systems offer data tracking or activity tracking tool(s). You'll want to have a notification and approval process that can be monitored alongside features like an audit trail. Otherwise, you might have to hunt for accounting information which could cost you time. Such delays can lead to further security breaches that cannot be contained or prevented.

Communication | While not explicitly tied to security, it's important for your team to be able to collaborate. Discussing the accounting data easily within the system is important for identifying erroneous or potentially malevolent activity. If individuals recognize a security issue, they can alert leadership before damages escalate. Many accounting systems have communication features, but you should look for multiple options. You should have alerts and chats that let you pinpoint and tag precise data to ensure clear focus on important information.

Why is an accounting platform safer and stronger?

Modern accounting systems need security features that address all areas of your data's security. It's that simple. The best way to do this is to use an accounting platform, not just an application.

What separates an IT platform from an IT application is the level of control and operational dexterity it allows. Applications typically offer the basic security features like usernames, passwords, posting status of transactions/records and closing accounting periods. But they seldom offer many of the higher-level controls for internal security and the ability to customize them to more refined requirements. Or when they do, they're limited or restricted in how you can apply them.

Think of an accounting application as a framework. The basic functionalities and protections are there, but that's it. In today's digital world with all of its data threats, you need more security measures and the ability to build on them. An accounting platform isn't just a framework, it's also a toolset letting you dictate how you use the technology. IT platforms are designed to be tailored according to user needs and be built on top of. You'll have basic accounting system functions, but also features with more advanced ways to control the overall system. This is especially true for accounting data security features.

Besides greater flexibility, accounting platforms like Accounting Seed are designed to give you high-level security right out of the box. All the security features and IT architecture you need to keep your accounting safe is the accounting platform. Let's look at several of these features.

What are essential features for modern accounting data security?

All accounting threats and areas of concern can be managed and controlled. Using a modern, reliable accounting platform that is frequently updated and well-supported is a major first step. You'll want to assure that the accounting tool is flexible and capable of meeting up-to-date accounting requirements. This includes having features that fully cover both external and internal threats.

Let's break down a few of these essential accounting platform security features.

Accounting Seed is the perfect customizable accounting solution to a custom-built Salesforce solution."

- Dru Dalton
CEO & Founder, Real Thread

EXTERNAL ACCOUNTING SECURITY FEATURES

Robust encryption and IT architecture | A truly reliable cloud accounting system must have IT architecture designed to be secure. Systems built on platforms like Salesforce® are more robust, equipped with high-level security features out-of-the-box. Encryption and event monitoring are just two examples of features that prevent external breach. You'll want to validate how strong these anti-hacking measures are by researching the history of hacking, and also examining which organizations are using it. Be sure to look for certifications connected to the product too.

*Example: Salesforce achieved FedRamp certification, ensuring the platform has the data security control needed for government work. These security features are shared by Accounting Seed which is a native accounting platform built on Salesforce. Accounting Seed has not been hacked since it's creation, over 10 years ago. This is greatly due to the native Salesforce security features our product has inherited.

Secure API | A strong Application Programming Interface (API) is important for secure amid reliable connections into and out of your accounting system. The most resilient and adaptable API in the industry is Open API. This API is extremely flexible to user requirements but equally difficult to disrupt. This is part of what allows companies to create unique internal controls within the accounting system too.

INTERNAL ACCOUNTING SECURITY FEATURES

Again, standard internal security measures like passwords, and usernames, are still important, but you need more measures in place to secure these, and your overall system, properly. To combat the growing security trends, you'll want features that create internal controls.

Internal control features establish accounting and auditing processes and procedures that ensure accounting is conducted efficiently and with compliance with laws, regulations, and internal policies. These security features dictate the scope and range of who can do what within the platform.

These defenses layer your accounting data with rules in place designed to keep it organized and properly maintained to both discourage data theft and prevent errors. These also serve to help alert management of erroneous or malevolent activity. The accounting system becomes more accessible and visible to those with authorization, but still guarded in access and user capabilities. These features let you set the safety measures instead of just having a few basic options.

Here are a few examples of important internal control features you'll want in your accounting system:

Two-factor authentication
Enable a second level of authentication for every login. You should also be able to implement this when a user is performing a specific function.

User permissions
Define what tasks users can perform, approve, and access. Create unique permission sets for more complex processes.

User role hierarchy
Establishing a user hierarchy lets you dictate which specific user(s) can view or change specific components of accounts or records within the system, like reports.

Validation rules
Establish standards for recording and handling data. Based on business logic, these rules prevent processes from being completed out of sequence or inappropriately.

Approvals
Automate sequences of events to require an official signoff on record to ensure accuracy and legitimacy. No one can alter or use the accounting data unless they are designated approvers or are given approval.

Real-time event monitoring
Monitor and detect standard events in near real-time. You can store the event data for auditing or reporting purposes.

Session security settings
Fully monitor, control, and even delete active user sessions. You're also able to view the specific IP address from where users are logged in, as well as approximate city and postal code locations.

Audit trail functionality
Track changes throughout the financial reconciliation process to maintain accurate, up-to-date information. See exactly who is doing what in the general ledger, with project accounting, and every other aspect of the accounting process.

Object/field trail functionality
View and document changes done to an object or a specific record within the object. This serves a dual role in helping identify errors and see which users are responsible, or to see if a user is trying to defraud the system.

Workflow rules
Workflow rules let you create and automate internal processes and procedural steps in orchestrating key accounting functions. This dictates how data is logged, accessed, processed and used.

Field history tracking
Select and track accounts, campaigns, orders, projects, and an unlimited range of standard and custom objects to monitor progress and maintain accurate data.

Chatter
Create secure chat groups and leave messages to help your team understand what's going on and identify security issues and threats.

Secure emails
Encrypt and safely send sensitive emails with accounting data involved. In Accounting Seed, you can utilize page layouts and Salesforce permissions to restrict users from viewing attachments too.

For more in-depth details on critical accounting features for a secure, efficient, reliable accounting, visit our blog or check out our Accounting Technology Buyers Guide.

Secure Your Accounting, Secure Your Future

Cloud data threats are only continuing to grow. While you can't prevent this trend, you can prevent data theft from damaging your business. Investing in a reliable, flexible accounting platform with the latest accounting security features isn't just a preventative measure, it's an asset that helps you continue thriving on the cloud. As new threats arise, the features and qualities described will help you adapt and remain secure.

ABOUT ACCOUNTING SEED

Accounting Seed is a modern, robust accounting platform powered by the Salesforce platform. We're committed to breaking down silos and building connections in order to take your business to the next level. Part of the way we do this is by ensuring your company's and customers' financial data remains fully secured. The features listed above are all available on Accounting Seed right out of the box.

Schedule a free demo here or contact us today to begin our conversation.

accountingseed

410.995.8406
accountingseed.com