The hidden cyber risks of siloed financial data

sage.com/en-us/blog/the-hidden-cyber-risks-of-siloed-financial-data

July 14, 2022

Accountants

Teresa Meek

Teresa Meek is a content contributor with over ten years experience in technology writing. Her areas of expertise are: cloud computing, cyber security, AI, data analytics and SaaS.

CFOs and their finance teams are in many ways at the center of an increasingly complicated threat landscape. The information they use is too often stored in unconnected databases, hard drives, and software applications, which teams export into spreadsheets and send across the organization as email attachments. Each data transfer and hand-off introduce a new set of risks – at a time when cyberattacks are rapidly increasing. Data compromises rose more than 68% in 2021, according to the Identity Theft Resource Center.

Breaches are also getting more expensive. The average cost of a breach rose 10% to $3.6 million last year, the IBM/Ponemon Institute's 2021 Cost of a Data Breach survey found.

Leadership teams know they need to do a better job of securing sensitive financial data. In Foundry's 2021 Digital Business study, over a third of business and IT leaders cited improving security as a top strategic objective, and 58% said security had taken on greater importance as a result of the pandemic, when many companies switched to remote operations.

Bogged down by manual procedures

When it comes to financial data, many security and compliance issues stem from the use of outdated, highly manual business processes, including sharing financial data through spreadsheets and emails. People with access to financial data and processes are especially attractive targets for cyberthieves. With manual processes and locally stored spreadsheets, people may send sensitive data to those who shouldn't see it or post it on internal messaging platforms that don't meet compliance rules. They also may share it with vendors and contractors, taking it out of company control. Every new instance of data sharing opens the door to a potential breach. "When information changes hands, you don't know who's accessing it or who's changing it," explains Scott Freedman, Director of Marketing for Sage Intacct.

Safety in the cloud

Consolidating financial information on a cloud-native platform creates a single source of truth, substantially reducing these types of risks. Cloud-native applications are built with granular controls for compliance and access. This allows finance managers to provide different levels of information to different stakeholders, via personalized dashboards that display all the information they need to do their jobs, but nothing more.

Not all cloud-based applications provide the same level of safety precautions. Because security is critical, it's important to determine whether a solution meets your specific needs. Here are some of the questions financial professionals should ask:

- **Audit and compliance controls:** Does the solution support audits to validate compliance with all the rules we must follow? Examples include SSAE 18, SOC 1 Type II, SOC 2 Type II, ISAE 3402 and 3000, PCI-DCC Level 1, HIPAA, and GDPR.
- **Security incident response:** Does the solution support the ability to react quickly to actual or suspected unauthorized access? Does it review data logs for signs of trouble?
- **Data loss prevention:** Does the solution have technology to identify and prevent data loss in email, collaboration tools, and other internal systems?
- **Monitoring and penetration testing:** Does the provider monitor and review its servers and user activity? Does it conduct regular tests on data, applications, systems, and infrastructure?

- **Network security:** Does the solution have up-to-date firewalls and antivirus software? Does it also remove unnecessary features that could serve as portals to future hacks?
- **Business continuity and disaster recovery:** What are the vendor's procedures for securely backing up and restoring our data in the event of an emergency? What does their solution do to prevent data loss and maintain data integrity during the transfers?

A cloud-native application offers stronger protections for financial data than an on-premises system, but not all cloud providers are alike. Before making the transition, take the time to document your needs and make sure your critical data will be in good hands.

To learn more about Sage Intacct, check out our daily Coffee Break Demo.