City of Madison
Information Technology
Microsoft Access Policy
June 2009

Background

Today's increased dependency on networked software systems has been matched by an increase in the number of attacks aimed at these systems. These attacks have resulted in the loss and compromise of sensitive data, system damage, lost productivity, and financial loss. Software vulnerability reports continue to grow at an alarming rate. One weak application on the network puts the entire network at risk.

According to InfoTech Research, many IT Managers, Administrators, and Chief Financial Officers have concerns with Microsoft Access because of its poor security controls and its role as a substitute for bona fide enterprise applications. It presents a deficient internal control that could be identified by external auditors. In today's regulatory environment (GASB-34, HITECH, PCI,)* there is a need to rein in unsanctioned MS Access applications in the enterprise to improve security and mitigate the risk of material weaknesses.

Some potential Access problems include:

- **Few users are experts, and often make errors in calculations that end up skewing entire files.** Planning sessions consequently go awry when executives show up with their own data sets and cause confusion over whose information is right.
- **Financial and Resource Management statements are prepared using poorly designed Access tables.** The data's accuracy becomes compromised, and staff end up wasting many hours verifying the validity of the numbers rather than performing their jobs. Worse, this faulty information is used to make important business decisions that are not aligned with organizational goals and do not meet regulatory compliance or financial reporting requirements.
- **IT has little or no knowledge of an Access file's existence.** The valuable data contained within the file may not backed up, secured, or checked for quality.
- **Access files quickly become overly cumbersome and complex, ultimately breaking down since Access lacks sufficient scalability to grow as data requirements grow.** IT is brought in to sort it all out, only to discover that no documentation was written regarding the creation or purpose of the Access files, and the system was poorly constructed, often times with serious flaws.
- **Databases are often created to fill perceived shortcomings in corporate applications when a new query, report, or small modification would meet those needs.** This results in duplication of data across the organization and raises questions about which data should be used with decision making, and leads to silos of information that cannot be easily shared.
- **Often users eventually decide their Access data needs to integrate with other data sources or extend to the Internet**. Access's lack of controls and the poor design of most systems makes this a difficult and labor-intensive process, if not impossible.
- **The front-end application and database are combined in the same file.** This means application controls and database controls are one in the same, which is a security threat. Anyone that has permission to run the application has permission to do anything within the application.

- **Access lacks some controls altogether**, which include:
  - Database Controls
  - Input Controls
  - Processing Controls
  - Output Controls
  - Auditing Controls

Policy

1. **Access 2007 will not be deployed.** There are known issues with running earlier versions of Access applications under Access 2007. City IT will not be converting existing Access applications to later versions.
2. **City IT will limit Access support.** Beyond giving users network file permissions to existing Access 2000 applications, City IT will not provide further support. If support is needed, agencies will be responsible for contracting with a vendor approved by City IT and paying the associated costs. The vendor shall perform their work in accordance with City of Madison Database and Application Policies and Standards.
3. **Existing Access 2000 applications can remain.** City IT will not be removing existing Access 2000 applications. We will just not be able to provide further support beyond network file permissions as stated above.
4. **Migrate to current platforms.** Bring IT staff in to evaluate the data and the risks posed by it, then build a plan to migrate the data (or kill it entirely) to a more stable and controlled platform in accordance with City of Madison Database and Application Policies and Standards. This may involve some costs, and may be time-consuming, but should be worth the effort to eliminate suspect data and the subsequent costs of misinformed decisions made from it.

Conclusion

As a tool for individuals or small teams, Microsoft Access does have productivity benefits. However, Access was never designed to function as a production database, yet many small workgroups use Access to build mini-applications that are ultimately pushed out to more and more users in a production environment.

Access has business benefits when used appropriately. However, it is equally important to recognize Access's limitations and the dangers it poses when not utilized properly.

Exceptions

Any exceptions to this policy will require the approval of the Information Technology Director. Requests for exceptions shall be in writing and will state the specific policy item that is being challenged and the business reason for the exception. The decision of the Information Technology Director shall be final.

References

Sources: InfoTech Research; ISACA (Information Systems Audit and Controls Association); Carnegie Mellon University Software Engineering Institute - CERT.

**GASB-34 – Governmental Accounting Standards Board*

HITECH – Health Information Technology for Economic and Clinical Health, recently enacted as part of the American Recovery and Reinvestment Act of 2009, this is an expansion of HIPAA (Health Insurance Portability and Accountability Act).

PCI – Payment Card Industry