South African Journal
of Information Management
[DoE accredited]

Peer Reviewed Article

Vol.6(4) December 2004

Hacker risk in e-commerce systems with specific reference to the disclosure of confidential information

C. Lamprecht
Department of Accountancy, University of Stellenbosch, South Africa
clam@sun.ac.za

Contents

Key words: Hacker risks; e-commerce; confidentiality; control framework; control model

1 Introduction

In a Web-centric environment, transactions between various parties, such as the e-commerce company, its client and a bank, are done electronically. Merging the business processes of this extended enterprise with the supporting technological processes adds to the complexity of the Web-centric environment. One of the intrinsic building blocks and security requirements in such an environment is the confidentiality between parties who exchange value electronically across open, and sometimes insecure, channels via the Internet.

Consumers need to feel secure and have assurance regarding the safety of private information that is captured and managed in the other party's database, which has become the heart of a company in this information age (Fogie and Peikari 2002). Moscove, Simkin and Bagranoff (2003:195) emphasize the fact that such private and sensitive information normally held in a database, must be protected from those not authorized to have access to it. Databases and the information stored in them sometimes represent the most important asset and are irreplaceable. A credit bureau's database files, for example, are its business. Databases are also critical components for corporate Web systems (Moscove, Simkin and

Bagranoff 2003:195).

Although companies seem to have security policies and procedures in place to control access to database information, unauthorized intrusion still occurs. The objective of this study was to identify the main hacker risks and to address them by identifying the components of control that should be in place to prevent such risks, as well as unauthorized access to confidential information.

Microsoft’s SQL Server was employed as an example of a database system that is used to manage confidential information. Hacker-specific risks pertaining to the MS SQL Server were therefore identified.

top

2 Delimitation of study

This study did not address the following areas, which fell outside its scope:

- E-payment systems
- Other general e-commerce risks, for example confidence, business practices and reliability
- Other means of gaining access to confidential information such as theft of a credit card with the PIN code written on it or posing as a representative of a reputable company and asking for or trying to confirm personal details
- The cost *vs* benefit aspects of suggested solutions to identified risks.

top

3 Hacker risks

As this study investigated the risks posed by 'hackers' to 'confidential' information, it is important to define these terms. Whatis.techtarget.com (2003) defines a 'hacker' as someone who attempts to break into computer systems. Typically, this kind of hacker would be a proficient programmer or person with sufficient technical knowledge to identify the weak points in a security system. The Microsoft Corporation (2000) defined 'confidential' as sensitive business information that is strictly intended for use within the organization.

According to Benson (2000), the unauthorized disclosure of confidential information could have a serious and adverse impact on the organization, its stockholders, its business partners and/or its customers. An example of such a situation occurred recently when private client information was compromized when a hacker allegedly gained access to eight million credit card account numbers by breaching the security of a company that processes transactions for merchants (Moneymax 2002).

Using the MS SQL Server as an example of a database system that can host confidential information, hackers can gain access by exploiting one or more of the following risks:

- Weak or nonexistent database administrator (DBA) passwords: In addition to a lack of passwords, many database administrators use weak passwords that can be found in a dictionary, that are short (less than six characters), or that are common names, places, or events. One of the most sought-after DBA accounts is the system administrator account used by MS SQL Server. This is mainly because MS SQL Server includes several very powerful extended stored procedures that give a DBA – or a hacker – full access to the server's file system. Using programs, a hacker can simply test passwords at the SQL server until it cracks. If the password is missing or is weak, it will only be a matter of minutes before the hacker has access to the data (Fogie and Peikari 2002).

- Poor programming or improper configuration on the SQL server: Another method of attack is via SQL injection techniques that exploit poor programming or improper configuration on the SQL server to allow a hacker to access, overwrite, or delete information in the data server. In addition, the infamous xp_cmdshell extended procedure can provide a hacker with a tool to take over the file system of the server (Fogie and Peikari 2002).

Christman and Hayes (2003) of the National Security Agency of the United States of America recommended several general guidelines for the secure configuration and administration of the MS SQL Server. A study of these guidelines indicated the following exploitable risks:

- Failing to physically restrict access to the SQL Server machine
- Not documenting access via trust links from other domains to resources on the SQL Server for its intended purpose
- Failing to configure a demilitarized zone architecture (i.e. with a Web server and database server) where the SQL server will be accessed from the Internet
- Installing SQL Server on a server machine that is also required to support other services, such as a Web server
- Installing application software and development tools on the production server
- Installing SQL Server without blocking incoming traffic prior to implementing the security configurations, and while the SQL Server services are active
- Leaving unnecessary services such as 'Internet Connection Sharing' and 'Remote Access Connection Manager' enabled on the SQL Server database server
- Leaving unnecessary protocol stacks on the server machine.

Organizations face many potential hacker risks as indicated above. In general, management does not ignore this and is implementing controls to prevent these risks and events from being realized in its organization. However, despite this, hackers still find gaps and illegal intrusion does occur.

The solution is to implement control at different levels, incorporating risk assessment to reduce hacker risks to an acceptable level.

top

4 Components of control

The Committee of Sponsoring Organisations of the Treadway Commission (CoSo 1992) defines internal control as a process effected by an entity's board of directors, management and other personnel and designed to provide reasonable assurance regarding the achievement of objectives in the categories of effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations.

After identifying business objectives and risks, the existing controls for managing the risks should be identified and their adequacy evaluated. Evaluating the adequacy will go hand in hand with balancing the investment in control systems and the risks addressed. Information systems security and control systems will help to manage the risks, but it will not eliminate them entirely. Management must then decide on the acceptability of the residual (net) risk. The residual risk decision is difficult and a proper control framework of generally accepted control practices is needed as a benchmark for the existing and planned IT environment.

4.1 Control framework

A control framework serves as a guideline for management to give it insight into managing its systems, business risks and internal controls effectively. Several control frameworks have been put in place, for example CoSo (*Internal Control – Integrated Framework* 1992) in the USA, Cadbury in the UK, CoCo (Criteria of Control) in Canada and the *King Report on Corporate Governance* in South Africa.

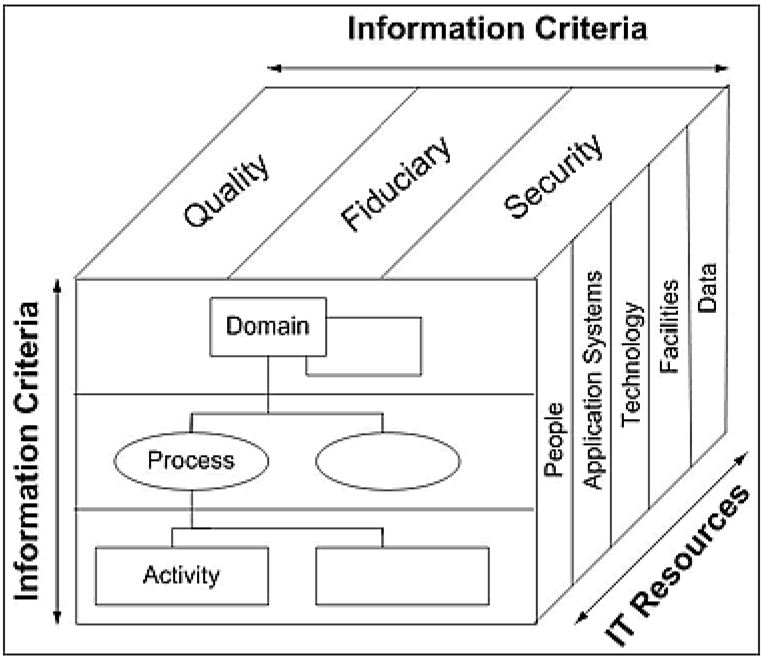
A more focused control framework on the IT level is the Governance, Control and Audit for Information and Related Technology (CobiT) Framework of the Information Systems Audit and Control Association and the IT Governance Institute, both in the USA. This conceptual framework was used because of its focus on IT and was evaluated as a solution against the stated research problem concerning hackers risks of illegal intrusion.

CobiT's mission (CobiT 2000) is to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors. The developers state that they meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. Their main objective is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organizations, and to develop these control objectives primarily from the business objectives and needs perspective.

The classification of domains where high-level control objectives apply (domains and processes), an indication of the business requirements for information in such domains, as well as the IT resources primarily impacted by the control objectives, together form the CobiT Framework (CobiT 2000).

The conceptual framework depicted in Figure 1, can therefore be approached from three vantage points, namely IT processes, information criteria and IT resources.

Figure 1 CobiT conceptual framework (adapted from CobiT 2000)



IT processes

CobiT provides good/best practices across a domain and process framework and presents IT activities in a manageable and logical structure. The four domains are (a) planning and organization, (b) acquisition and implementation, (c) delivery and support and (d) monitoring. This study focused on security, which is covered by the 'ensure systems security' IT process and grouped into the domain 'delivery and support' (CobiT 2000).

Information criteria

Information criteria are divided into three groups, namely quality requirements, fiduciary requirements and security requirements. Confidentiality (which concerns the protection of sensitive information from unauthorized disclosure) is grouped into the security criteria (CobiT 2000).

IT resources

Control is approached by looking at information that is needed to support the business objectives or requirements. Information is then the result of the combined application of IT-related resources that need to be managed by IT processes. The different IT resources are people, application systems, technology, facilities and data (CobiT 2000).

Application to the research problem and critical evaluation of CobiT

The CobiT Framework has been limited to high-level control objectives in the form of a business need within a particular IT process, the achievement of which is enabled by a control statement, for which consideration should be given to potentially applicable controls. Ensuring system security is the control objective and confidentiality the business requirement (CobiT 2000).

Thus, control over the IT process for ensuring systems security that satisfies the business requirement of safeguarding information against unauthorized use, disclosure or modification and damage or loss is enabled through logical access controls which ensure that access to systems, data and programs is restricted to authorized users (control statements) and takes the following into consideration as control practices:

- Confidentiality and privacy requirements
- Authorization, authentication and access control
- User identification and authorization profiles
- Need-to-have and need-to-know
- Cryptographic key management
- Incident handling, reporting and follow-up
- Virus prevention and detection
- Firewalls
- Centralized security administration
- User training
- Tools for monitoring compliance, intrusion testing and reporting (CobiT 2000).

CobiT is successful at a high level in addressing the security risk posed by unauthorized entry and disclosure of confidential information. It shows clearly what must be managed through its control objectives, but does not show one how to design, implement and maintain a hacker risk management system.

A need therefore exists for some kind of model that will *focus* on the design, implementation and maintenance of a risk management system.

4.2 Control model

Generally, a control model focuses on the design, implementation and maintenance of risk management by identifying application-centred control objectives and a set of minimum control standards to achieve those stated objectives, as well as an evaluation of residual risk. This is done through the application of control techniques.

A well-known model is the American Institute of Certified Public Accountants, Inc. (AICPA) and Canadian Institute of Chartered Accountants (CICA) *Trust Services Criteria and Illustrations.* AICPA/CICA explains that these trust services criteria and illustrations present a common framework with a set of core principles, criteria and illustrative controls to address the risks and opportunities of IT. It is used by practitioners while they provide attestation services on systems in the fields of security, availability, processing integrity, online privacy and confidentiality, which also compromise the broad statements of objectives. The trust services criteria are benchmarks used to measure and evaluate the subject matter, and are objective, measurable, complete and relevant. It is specifically stated that the illustrative controls are presented as examples only. (AICPA/CICA 2003)

The trust services principles and criteria are organized into four broad areas that cover the design, implementation and maintenance of risk management and make it an ideal example of a control model.

The four areas are:

- Policies. The entity has defined and documented its policies relevant to the particular principle.
- Communications. The entity has communicated its defined policies to authorized users.
- Procedures. The entity uses procedures to achieve its objectives in accordance with its defined policies.
- Monitoring. The entity monitors the system and takes action to maintain compliance with its defined policies (AICPA/CICA 2003).

To apply the AICPA/CICA trust services principles and criteria control model to manage the identified hacker risks, one clearly needs to look at the principles and criteria regarding security, online privacy and confidentiality. AICPA/CICA defines each of these selected principles, which are sufficient for purposes of this study, as follows:

- Security: The system is protected against unauthorized access (both physical and logical).
- Online privacy: Personal information obtained as a result of e-commerce is collected, used, disclosed and retained as committed or agreed.
- Confidentiality: Information designated as confidential is protected as committed or agreed (AICPA/CICA, 2003).

Evaluation of AICPA/CICA control model

AICPA/CICA deals with each of the above principles by providing a list of criteria under each of the four broad areas, as well as some illustrative controls. The criteria serve as questions against which an organization's adherence can be evaluated. The document further mentions that the illustrative controls are not complete, and may not be applicable to the organization that is considering the application.

Although the AICPA/CICA model provides an adequate framework for *how* security, online privacy and confidentiality can be achieved, it still only offers questions and no solutions. One therefore needs to find something that will guide one towards the implementation and operation of techniques for a hacker risk management system.

4.3 Control techniques

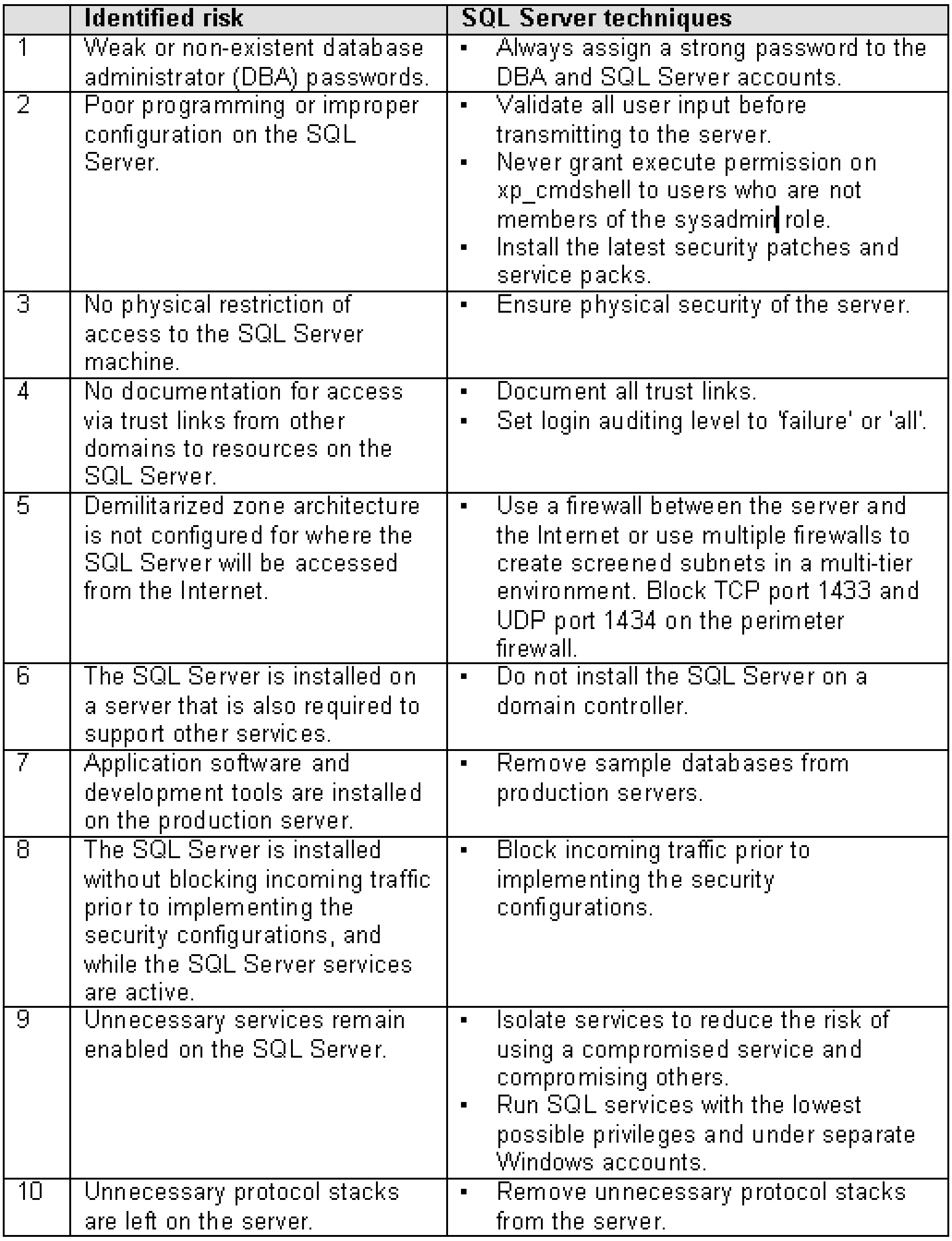
Fogie and Peikari (2002) suggest that in many computer-based technologies it is not the product that is at fault, but that the fault lies in the implementation.

Control techniques are implemented to address business and control objectives. The type of technique that is implemented will depend on the context of the environment. In a Web-centric environment, control techniques would mainly be automated and would consist of preventative, detective or remedial controls.

Microsoft control techniques for SQL Server (Microsoft Corporation 2003) were chosen as it is well known and considered to be authoritative.

An evaluation of the Security Best Practises document revealed a host of mainly preventative control techniques for use by the administrator. The techniques are also mainly automated after an initial manual setup. In Table 1 the relevant techniques are summarized and linked to the identified risks:

Table 1 Identified risks and control techniques



	Identified risk	SQL Server techniques
1	Weak or non-existent database administrator (DBA) passwords.	▪ Always assign a strong password to the DBA and SQL Server accounts.
2	Poor programming or improper configuration on the SQL Server.	▪ Validate all user input before transmitting to the server. ▪ Never grant execute permission on xp_cmdshell to users who are not members of the sysadmin role. ▪ Install the latest security patches and service packs.
3	No physical restriction of access to the SQL Server machine.	▪ Ensure physical security of the server.
4	No documentation for access via trust links from other domains to resources on the SQL Server.	▪ Document all trust links. ▪ Set login auditing level to 'failure' or 'all'.
5	Demilitarized zone architecture is not configured for where the SQL Server will be accessed from the Internet.	▪ Use a firewall between the server and the Internet or use multiple firewalls to create screened subnets in a multi-tier environment. Block TCP port 1433 and UDP port 1434 on the perimeter firewall.
6	The SQL Server is installed on a server that is also required to support other services.	▪ Do not install the SQL Server on a domain controller.
7	Application software and development tools are installed on the production server.	▪ Remove sample databases from production servers.
8	The SQL Server is installed without blocking incoming traffic prior to implementing the security configurations, and while the SQL Server services are active.	▪ Block incoming traffic prior to implementing the security configurations.
9	Unnecessary services remain enabled on the SQL Server.	▪ Isolate services to reduce the risk of using a compromised service and compromising others. ▪ Run SQL services with the lowest possible privileges and under separate Windows accounts.
10	Unnecessary protocol stacks are left on the server.	▪ Remove unnecessary protocol stacks from the server.

Implementation and operation of these techniques would be sufficient to reduce the identified hacker risks to an acceptable level. However, these techniques on their own are merely ad hoc if they are not linked into a proper control framework and model.

A proper control environment for managing hacker risks must therefore consist of a control framework that indicates what should be done/not be done; a control model to focus on the design, implementation and maintenance controls to manage the risks; and control techniques appropriately implemented to address the control objectives.

The problem is that control techniques are mainly implemented by the IT personnel, whereas a control framework and model are implemented by management. Furthermore, management often does not understand the problems and technical complexities experienced by the IT personnel in making the technology work, and IT personnel, on the other hand, often do not understand the theory, concepts and frameworks put into place by management. It is at this point that a gap is opened up for hackers to enter the system.

Hackers do not get into systems because there are no management policies and procedures or because there are no control techniques in place, but rather are able to enter because management and technical policies and procedures do not merge into one risk management unit.

top

5 Conclusion

The best way to manage hacker intrusion risks, and other IT risks as well, is to implement a three-level control model. This model should include risk assessment to determine residual risk, and must merge management's business objectives and identified risks with the technological standards, implementations and control techniques performed by the IT personnel. Introducing the three-level control model suggested will not keep hackers out of the system 100% of the time, but will reduce the risk of illegal intrusion and compromising of confidential information to an acceptable level.

top

6 References

AICPA/CICA. 2003. Suitable trust services criteria and illustrations. [Online]. Available WWW: http://www.aicpa.org (Accessed 14 April 2003).

Benson, C. 2000. Microsoft solutions framework. Best practices for enterprise security. Microsoft Corporation. [Online]. Available WWW: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp (Accessed 18 August 2003).

Christman, S. and Hayes, J. 2003. Guide to the secure configuration and administration of Microsoft SQL Server 2000. National Security Agency. [Online]. Available WWW: http://www.nsa.gov/isso/index.html (Accessed 18 August 2003).

CobiT Steering Committee, IT Governance Institute. 2000. *CobiT*3 rd edition. [Online]. Available WWW: http://www.isaca.org (Accessed 11 August 2003).

CoSo (Committee of Sponsoring Organisations of the Treadway Commission). 1992. *Internal control – integrated framework* . [Online]. Available WWW: http://www.coso.org (Accessed 11 August 2003).

Fogie, S. and Peikari, C. 2002. SQL Server attacks: hacking, cracking, and protection techniques. [Online]. Available WWW: http://www.informit.com/content/printerFriendly.asp?product_id={9AF62809-408D-401A-9144-B0A695B72424}&st={340C91CD-6221-4982-8F32-4A0A9A8CF080}&session_id={B960CE95-2199-49F9-B783-4DA7B64A0FF0} (Accessed 18 August 2003).

Microsoft Corporation. 2000. Security planning. [Online]. Available WWW: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp (Accessed 18 August 2003).

Microsoft Corporation. 2003. Microsoft SQL Server 2003: Checklist: security best practices. [Online]. Available WWW: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/sql/Default.asp (Accessed 18 August 2003).

Moneymax. 2002. A credit card secure site. [Online]. Available WWW: http://www.moneymax.co.za/help/secure.asp (Accessed 11 April 2003).

Moscove , S.A. , Simkin, M.G. and Bagranoff, N.A. 2003. *Core concepts of accounting information systems.* New York: John Wiley & Sons, Inc.

Whatis.techtarget.com. 2003. [Online]. Available WWW: http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci212220,00.html (Accessed 6 October 2003).

Disclaimer

Articles published in SAJIM are the opinions of the authors and do not necessarily reflect the opinion of the Editor, Board, Publisher, Webmaster or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special, incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user's use of the Website.

top

ISSN 1560-683X

Published by InterWord Communications for the Centre for Research in Web-based Applications, Rand Afrikaans University