SafeComs

Security and Performance...

CUSTOMER Information Security Audit Report

Version 1.0

Date Wednesday, 18 January 2006

SafeComs
Internet: www.safecoms.com
Email: mailto:info@safecoms.com

2001 Chartered Square Building.
20th Fl, 152 North Sathorn rd.
Bangrak, Bangkok 10500, Thailand
Telephone: +66(02) 634 5465
Fax: +66(02) 634 5467

Acknowledgments

Authors:	Yannick Thevenot CTO, SafeComs Jared Dandridge COO, SafeComs
Reviewers:	Bernard Collin CEO, SafeComs
Publisher:	SafeComs, 2001 Chartered Square Building Bangkok

Table of Contents

Executive Summary

CUSTOMER’s Core Assets and Risks

- CUSTOMER’s business depends heavily on reputation and credibility in the industry. products from clients are valuable, and must be handled appropriately. Risks include:
    - <Risk 1>
    - <Risk 2>

- The core production application system is the nervous system of the entire CUSTOMER operations. Core activities include <omitted>. Risks include:
    - <Risk 1>
    - <Risk 2>
    - <Risk 3>

- People, the processes they perform, and the expertise they acquire is critical to CUSTOMER (communication, project controls, delivery, etc…). Risks include:
    - <Risk 1>
    - <Risk 2>

Management Attitude, Knowledge and Awareness

- COMPANY Directors have expressed firm commitment to implementing security in the organization. There are solid intentions to secure the business and its operations, and this commitment has served the company well.

…
<omitted>
…

- During the business and operations analysis, there was a complacent feeling from some management and staff that we interviewed about the security risks and liabilities at CUSTOMER. There is a mixed understanding of security and of security policies and procedures amongst the staff and management at CUSTOMER. The organization would certainly benefit from a session or workshop on security awareness. Managers need to review security risks in relation to their division and responsibilities.

Summary of primary security threats

A summary of the primary security threats, along with their risk scores (1 low to 45 high*), is outlined in the chart on the following page.

(*) The calculations used to rate these threats is explained in Risk Score Calculations.

Score	Risk Level – Issue
18	**Medium – Prior to Employment**
	Employees are not formally notified of their role in information security, nor are they made aware of the potential penalties for not conforming to company standards. This becomes a liability to the company, if any security incidents occur
18	**Medium – Operational Procedures and Responsibilities**
	Without a list of standard software for PC's and servers, both staff and IT personnel do not have a clear understanding of what is considered acceptable applications, and confusion and misunderstanding will follow. For the weak control on patching and change management, security vulnerabilities and unexpected results from applications could occur without the control or knowledge of IT
18	**Medium – Backup**
	Inconsistent procedures for backups could lead to corrupted data, lost tapes, or the inability to restore lost data. It is not known whether email can be restored, as it has never been tested. For other files, only test files are restored, and no trial of production data is attempted
18	**Medium – Business Requirements for Access Control**
	The lack of an access control policy leaves room for error of both users and IT staff. As there are no guidelines, changes to staffing or systems could result in a security breach. This is already apparent in how too many file servers are being established. This issue also compounds other factors such as server licenses (cost), patching issues (server management), and configuration and access issues (user management).

…
<omitted>
…

Score	Risk Level – Issue
36	**High – Information Security Policy & Awareness Program**
	As many staff are unaware of the wide range of potential security issues, various breaches in security could occur, and go un-noticed or un-reported. The potential level of damage to the company could be severe (e.g. loss of revenue, customers, or reputation).
36	**High – Internal Organization of Information Security**
	A false sense of security with no direction or substance will continue, until a major security event occurs, or active steps are taken to implement security awareness in the organization. The security coordinator has not had any formal security training, and currently she only has limited knowledge as to all the areas that her position is responsible for.
45	**High – Reporting Information Security Events and Weaknesses**
	If employees are not properly trained, security incidents could go unreported and/or unnoticed, causing increased risk for the company. For example, passwords written on paper next to a monitor, confidential documents left in a copier, or other blatant security breaches are items that should be alerted to the security coordinator.

Compiled Recommendations

A Protect Core Systems and Critical Data from Potential Hackers

Objective

Prevent unauthorized access and defend against possible data manipulation or loss. Due to mis-configuration of the firewall, gateway antivirus, and missing patches, there is a logical path for intruders to access core systems and critical data.

We believe this requires utmost attention.

Action:

- **Review all policies and appropriately reconfigure the firewall**
- **Reconfigure the Virus gateway scanner**
- **Reconfigure the spam filter**
- **Ensure all servers have all appropriate patches applied**
- **Remove any unnecessary / unused shares**

Requirement - Immediate

…
<omitted>
…

D Gain Control of Data & Defend Against Possible Disasters

Objective

Guarantee that any incident could be recovered from, including virus, fire, and accidents on manipulation of server, disks or data, programs, or HD crash.

Ensure that information is appropriately controlled, handled, and secured, by classifying and organizing information in a structured manner.

Action:

- **Implement a business continuity plan**
    - **Step A**
    - **Step B**
    - **Step C**
- **Develop of a policy for information classification**
    - **Step A**
    - **Step B**
    - **Step C**
- **Control of effective backup and restore operations**
    - **Step A**
    - **Step B**
    - **Step C**
- **Encryption should be applied to the backup of sensitive data**
- **Use of vault for temporary storage before transfer off site**
- **Install an appropriate computer room fire suppression system**

Requirement – Immediate

Scope

CUSTOMER required that SafeComs perform an audit of their IT infrastructure. The audit must cover all aspects of the IT function at CUSTOMER, including:

- IT policy and procedure
- Business continuity of the IT function
- Physical security around IT assets
- Host-based security on IT assets

Results of the audit should provide CUSTOMER with an understanding of their information security positioning, as well as providing recommendations on how to improve areas that have been identified as being high security risks to CUSTOMER.

Methodology

SafeComs conducted its audit in conformity with IS0-17799 – Information Technology – Code of practice for information security management. The basis for this is that ISO-17799 standard provides a common basis for developing organizational security standards and effective security management practice as well as providing confidence in inter-organizational dealings.

The audit consisted of an interview of the Management Team and some key staff. We also observed the IT practice and reviewed appropriate documentation when available.

Selected Workstations and Servers were analyzed, and system software and anti-virus signatures controlled. A full vulnerability scan was conducted, on all servers (both public and private) in use at CUSTOMER. Reports are attached.

Various recommendations in policies and procedures, including hardening recommendations, will be issued to improve the overall security at CUSTOMER.

Risk Score Calculations:

In this document, you will see ratings indicating the risk level of our findings. There are two variables used to determine risk, which are Business Impact and Level of Control.

Business Impact – How bad could it be?

The first box of rankings is an indication of benchmarks, industry standards, and the level of importance placed on this item, as identified during interviews with your staff. To calculate the Business Impact of a given risk, the two scores for the Potential Impact and the Probability of Occurrence are multiplied together:

Potential Impact (The level of impact to the business, of a security breach)

3	High
2	Medium
1	Low

Probability of Occurrence (The likelihood that a security breach might occur)

3	High
2	Medium
1	Low

Business Impact (The overall assessment of how impacting this item could be)
By multiplying the above items, we will get the result of the Business Impact.
(Potential Impact x Probability of Occurrence = Business Impact)

7 ~ 9	High
3 ~ 6	Medium
1 ~ 2	Low

Level of Control – How much are you doing to prevent it?

Based on the findings from the audit, a score is assigned to identify what the business is doing to address and prevent security breaches from this item. The amount of controls or measures in place to mitigate the security breach are ranked as:

5	Nothing Being Done
4	No Controls
3	Weak Controls
2	Not Consistent
1	High Control

Risk Score (*) – What is the your over-all rating for this item?

By combining the potential business impact with the company's level of control for that item, we can identify the risk for that item. Therefore: Business Impact x Level of Control = Risk Score; Risk Score is divided into three possible categories, as follows:

31 ~ 45	High Risk
16 ~ 30	Medium Risk
1 ~ 15	Low Risk

For each finding above, the following table is used to represent the Risk Score of that item:

Indicator	Score	Low Risk High Risk
Business Impact	PI x PO = BI (Level)	1 2 3 4 5 6 7 8 9
Level of Control	LC (Level)	1 2 3 4 5
Risk Score	RS (Level)	1~15 16~30 31~45

(*) To be issued a certificate of compliance, the company must only Rate in the Low Risks.

Note on SafeComs' approach:

IT Security is not an absolute; that is to say that no organisation can be completely secure. Further measures can always be taken to improve the security of an organisation, and to minimise the risk to that organization of an IT security breach. However not all security measures represent a good investment of IT resources. IT security is therefore a risk management process, which aims to reach a delicate balance between required functionality, security and cost. The SafeComs approach to conducting IT security audits is based on this philosophy.

Current State

CUSTOMER has many services such as <omitted> that are handled by a computerized control system. In addition, service time is offered 24 hours a day and 365 days a year to support the customer needs. CUSTOMER goal is to be one of the best service providers in Asia with advanced technology and well-maintained facilities such as <omitted> on the World Wide Web in order to ensure that customers will be able to access directly to receive real time information.

Currently, there are a number of significant applications on the computer systems such as <omitted> that are running on UNIX and Windows Server 2003, respectively. Recognizing the criticality of role of the computer systems in the operation of the company, CUSTOMER management is concerned with adequacy of controls to ensure accuracy, integrity and reliability of the computer systems.

Findings, Risks, and Recommendations

In compliance with ISO-17799, the audit results at CUSTOMER are organized into the eleven security control clauses of the ISO standard. Within each of the ISO-17799 clauses, the identified items are represented with their associated findings, risks, and recommendations. The 11 security control clauses are as follows:

1. Security Policy
2. Organization of Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

Note: The order of the clauses does not imply their importance. Depending on the circumstances, all clauses could be important, therefore SafeComs will identify applicable clauses, how important these are and their application to individual business processes.

1. *Security Policy*

Information Security Policy

Business Impact

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Indicator	Score	Low Risk High Risk
Potential Impact	High	1 2 **3**
Probability of Occurrence	High	1 2 **3**
Business Impact	High	1 2 3 4 5 6 7 8 **9**

Control

Information security policy document
An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

…
<omitted>
…

Finding

There is no formal, documented security policy in existence at CUSTOMER. During interviews, some staff assumed a policy was in place, due to their understanding that security was only about passwords. In the procedure manuals, we found that

…
<omitted>
…

Indicator	Score	Low Risk High Risk
CUSTOMER's Level of Control	No Controls	1 2 3 **4** 5

Risk

As many staff are unaware of the wide range of potential security issues, various breaches in security could occur, and go un-noticed or un-reported. The potential level of damage to the company could be severe (e.g. loss of revenue, customers, or reputation).

Indicator	Score	Low Risk High Risk
Risk Score	36 - High	1~15 16~30 **31~45**

Recommendation

Immediate action should be taken to develop and implement a comprehensive information security policy that will define and communicate the management's commitment to information security to the entire organization.

5. Physical and Environmental Security

Secure Areas

Business Impact

Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.

The protection provided should be commensurate with the identified risks.

Indicator	Score	Low Risk		High Risk
Potential Impact	High	1	2	**3**
Probability of Occurrence	Medium	1	**2**	3
Business Impact	Medium	1 2 3 4 5 **6** 7 8 9		

Control

Physical security perimeter
Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

...
<omitted>
...

Protecting against external and environmental threats
Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

Finding

...
<omitted>
...

A primary concern is the fact that there is no fire suppression system in the computer room.

Indicator	Score	Low Risk				High Risk
CUSTOMER's Level of Control	Weak	1	2	**3**	4	5

Risk

A fire in the computer room could destroy all current support activities, as well as destroy the servers of the other company hosted in the CUSTOMER computer room. CUSTOMER could be liable for damages incurred to both companies, including lost assets and time to recover from the loss.

Indicator	Score	Low Risk		High Risk
Risk Score	18 - Medium	1~15	**16~30**	31~45

Recommendation

Continue regular maintenance on the perimeter, entry controls, and facilities.

An appropriate computer room fire suppression system should be installed as soon as possible to prevent a fire disaster.

...
<omitted>
...

7. Access Control

Network Access Control

Business Impact

Objective: To prevent unauthorized access to networked services.

Access to both internal and external networked services should be controlled.

User access to networks and network services should not compromise the security of the network services by ensuring:

a) appropriate interfaces are in place between the organization's network and networks owned by other organizations, and public networks;
b) appropriate authentication mechanisms are applied for users and equipment;
c) control of user access to information services is enforced.

Indicator	Score	Low Risk High Risk
Potential Impact	High	1 2 **3**
Probability of Occurrence	High	1 2 **3**
Business Impact	High	1 2 3 4 5 6 7 8 **9**

Control

Policy on use of network services
Users should only be provided with access to the services that they have been specifically authorized to use.

...
<omitted>
...

Network routing control
Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Finding

Customers and suppliers are able to access CUSTOMER data/application. There is no control or logs monitoring on what they do remotely. PC Anywhere was still opened on a server during the audit when the supplier had requested to access during a previous timeframe.

...
<omitted>
...

Security breach possible – During an external scan, we found that the Virus scanning interface is open and available without the need of a username or password. We have access to control this service. In addition, we believe that with a small amount of effort, we could penetrate this machine and thereby gain access to the CORE system via a hole identified in the firewall.

Indicator	Score	Low Risk High Risk
CUSTOMER's Level of Control	No Controls	1 2 3 **4** 5

Risk

Production systems are vulnerable to attack and security breaches from multiple channels (Internet and Wireless) and there is no true control or knowledge of what is passing through the network on a daily basis.

Indicator	Score	Low Risk High Risk
Risk Score	36 - High	1~15 16~30 **31~45**

Recommendation

<omitted>