GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

TITLE : A Case Study - Implementing Defense in Depth for a Community Network Service Provider operating in a Transition Economy

Dated : November 28, 2002

Version : 1.4b (amended August 29, 2002)

Option : 2 (TWO)

Name : Tee Meng (Raymond) WEE

Assignment : Practical for GIAC Security Essentials Certification (GSEC)

Submission : Original

Course : Onsite at SANS Marina Del Rey (July 13-18, 2002)
Track 1: SANS Security Essentials with Certification attempt

Note: As this assignment was based on a real-world example, identifying facts and information have been masked to safeguard the confidentiality of the company.

Abstract

Implementing security within a network involving internal and external users, public and private sector entities is a significant challenge. In a transition economy environment where the economic, social, legal and physical infrastructures are still in development, this task is made even more difficult.

This paper is the result of an experience with a client implementing a community-wide network service in a transition economy. It covers only a small subset of the security issues faced by the company in an environment where culture and personal priorities are sometimes in conflict with company or professional interests. The issues covered below are just a tip of the iceberg, but as an information security professional, one should not give up the opportunity to improve the situation, even if the process is more difficult and takes longer than usual. Instead of writing a book to detail the security and implementation issues faced, only two case studies are presented below for the purposes of this practical.

© SANS Institute 2003, Author retains full rights.

1.0 Introduction

The company, let's call it Firm_A, is a network service provider that provides messaging (or electronic document exchange) service to the business community in a transition economy. It is a local-foreign, public-private joint venture which also operates a document processing system outsourced to it by a Government Agency (GA) as part of its services. The project is highly visible both at the national level and in the region as similar regional administrations are awaiting the success of this project to follow suit. As such, a security breach will certainly receive a negative publicity and may cause the joint venture to suffer serious economic loss, or even collapse.

The network service involves external users (let's call them Applicants) sending structured text data through a MS Windows-based custom-built "front-end-software application" to a messaging hub. The messaging hub then relays this document to the back-end server of the Government Agency (GA). Its officials then checks the document and send back another structured text response to the Applicant providing instructions for the next steps. A hardcopy printout is then generated for Applicant to bring to the Government Agency's payment points for payment of fees and verification of supporting documents. In the process, depending on the results, additional messages are also sent to the Applicant and/or other stakeholders involved in the entire process.

2.0 The constraints

Owing to the relative lack of a legal framework governing privacy, electronic transactions and information security in general, Firm_A is unable rely on legislation or court actions for security breaches, making strict enforcement against such breaches difficult.

The general level of education, physical and telecommunications infrastructures are also low or unreliable by international standards. As a result of the relative small number of IT personnel available nation-wide, everyone knows almost everyone else in the IT field, making confidentiality and protection of intellectual property difficult. It is culturally acceptable to freely exchange information even if they may each be working for competing companies or in a government regulatory body or security agency.

The country concerned is listed by Transparency International as one that "have a serious corruption problem" because it has a 2002 CPI Score of less than 5.5. "CPI" stands for "Corruption Perception Index". [1]

It is observed that in this country, nationalistic, family, commonality in race, religion or tribal interests seems to take precedence over the interests of the company. For instance, comments such as "it is in the interest of the State" or "sovereign data" were often used. The fact that the management is mainly expatriate while the systems and security team is mainly local sometimes adds to the level of difficulty in implementing information security.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The author's official role with this project is mainly advisory with the exception of tasks (see Case Study 1) specifically assigned by the management of the company. It is therefore hoped that by sharing the following ideas and experiences here, some security professionals may benefit if they are to improve information security through an advisory or consultative role.

3.0 The risks faced

Against this background, the task of safeguarding confidentiality was difficult to enforce. So, the management of Firm_A had to rely solely on the trust of its employees in the systems administration, network and security departments because skilled IT professional were scarce and legal proceedings always take a long time. Some of them were also close to law enforcement agencies.

The task of safeguarding confidentiality was also made more difficult given the urgent need for the service to be rolled out as quickly as is possible with the limited human resources. For instance, the security and network teams were also overlooking physical infrastructure set up and configuration, which was to be completed in 3 weeks. The list of equipment included 3 main Unix Servers in 3 sites about 1 to 10 kilometers apart, accompanying UPS, stabilizers and network equipment. The teams were also responsible for the delivery, set up, configuration and training for about 150 users which includes Applicants, officials from the Government Agency and internal Firm_A users.

Availability was a prime concern prior to the launch and as such was given top priority, resources, time and attention by all. As such, this was less of a concern. All were sufficiently motivated to ensure that the systems and networks were properly functioning and available under their respective watch. Security measures ensuring that the network was available to all the duly authorized users, both internal and external were found to be sufficiently implemented.

This paper discussed, through the experience of Two cases, how attempts were made to improve the Integrity of the systems and output generated.

4.0 Situation prior to Intervention

The front-end-software applications, network and back-end systems were designed with a certain degree of security at the applications level. For instance, once the documents were sent and validated by the back-end, the front-end forbade the user to change its contents.

Secondly, the messaging software kept a copy of the message exchanged and audit trails were maintained to determine who sent what when.

Finally, the back-end was a relational database that logged all the transactions and the software tracked changes done at the application level.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Redundant data and audit logs were written into different "control tables" to make it difficult to change the data other than via the back-end application.

The concept of Separation of Duties was also also used to ensure that those who had access to the database did not have access to the source codes. Nevertheless, additional security was still needed and the following were two such cases :

4.1 Case Study 1 : (implementer role) ensuring that data printed on a hardcopy printout, relied upon for operational processing purposes, were not altered.

4.2 Case Study 2 : (advisory role) ensuring that the data contained in the systems were not altered in any unauthorized way and ensuring that the programs were not altered from its originally designed and accepted state.

A brief discussion was then made (post implementation) on the "Big Picture" where "security is a process, not a product.", as advocated by authors in the book "Inside Network Perimeter Security". [2]

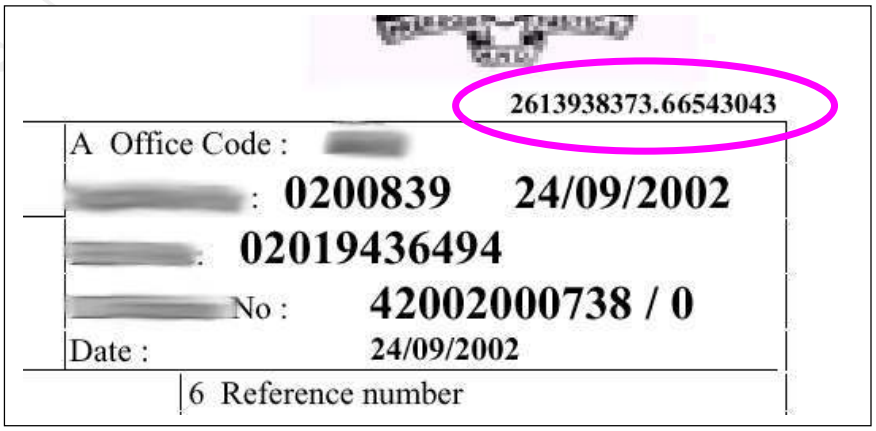
5.0 Case Study 1 : Hardcopy data integrity

5.1 The issue

The management of Firm_A wanted to provide additional safeguards so that the hardcopy data printed by the front-end-software application were Not being used for purposes other than those it was intended.

5.2 The methods used

Apart from printing labels such as "For use by Government Agency only", "Not a validated document", and obtaining a back-end-system generated numbers, a series of check-digits was generated at a specific place on the Hard copy printout. See Figure 1 below .



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Digits to the Left of the dot were made known to a "restricted" group of External users who needed to quickly verify the authencity of the printout, without referring to the electronic message received or data stored in the database. If they did not match, then "a reason for doubt" was raised and further checks on the authenticity of the application were needed. That speeded up the document process at the payment points and allowed limited computer resources to be shared by more than one User ID, thus reducing equipment and communication needs. Those authorized users with direct back-end access would not need this feature since they would be able to verify all the data online in real time.

Another set of numbers was generated to the right of the dot, if there were financial values or payments involved. These numbers followed a certain algorithm. The algorithm and method of digit generation was only made known to one or two key personnel within Firm_A. It was also only generated if there was an amount to be paid. If not, there was no digit generated to the right of the dot, except for a random number generated acting as a "decoy".

See Exhibit A at end of this paper for a copy of the pseudo-code provided courtesy of the programmer [3] who wished to remain anonymous for the purposes of this paper.

5.3 The Shortcomings or Difficulties faced

Applying simple cryptanalysis techniques like gathering many samples of the cipher digits, it quickly became clear that :

a. Guessing the digits to the left was relatively easy since only the random "seed" number changed with each printout of the same document. For example, printing 10 sets of the same document would yield :

   64946474
   63936373
   68986878
   62926272
   67976777
   61916171
   64946474
   65956575
   69996979
   66966676

   The originating data on this document was 3 - 0 - 3 - 2 in the selected fields.

b. Secondly, the digits to the right of the dot were fixed except for the random digit. Multiple prints of the same document would also yield a fixed pattern. E.g. if the selected amount was zero, only the random digit was printed. So, printing the same form over 15 times will quickly reveal that it's a

© SANS Institute 2003, Author retains full rights.

random number from 0-9. In addition, not making any payments for the selected amount would also be one of the aims of potential forgers.

c. Thirdly, as soon as the algorithm for the second part was compromised, the printed hardcopy could be easily forged with an appropriate report generation or even word processing tool.

d. As mentioned earlier on confidentiality, the risk for the compromise of second part was relatively high especially with the encrypting "key" in clear text in the source codes.

Also as a result of this ease, forgers may be encouraged to duplicate the documents so as to trick the Government Agency, its payment / collection departments or any unsuspecting users of the Hardcopy printout.

Finally, with only 2 weeks left to the service rollout, it was a race against time to implement something "quick and dirty" to provide the added safeguards.

5.4 Additional security measures

After understanding the concerns of the management and the issues faced by the programmer, the following decisions and recommendations were made and implemented :

a. As the first part of the digit was to facilitate the relative ease of checking at the payment points and selected external users in the field, the risk was deemed acceptable by the management of the company.

b. Using the concepts of "Defense in Depth" and simple cryptography, a third layer of security was added to the check digits.

- Firstly, the last 2 digits (least significant digits) from second part (numbers to the right of dot) were moved to the left while the first digit (most significant) of the second part was moved to the right. If the value of the selected amount was less than 3 digits, no shifting was done.

- Next the random number generator was attached to the right as before.

- Finally, all the digits were added and a mathematical function (e.g. modulus 23) was done on the results.

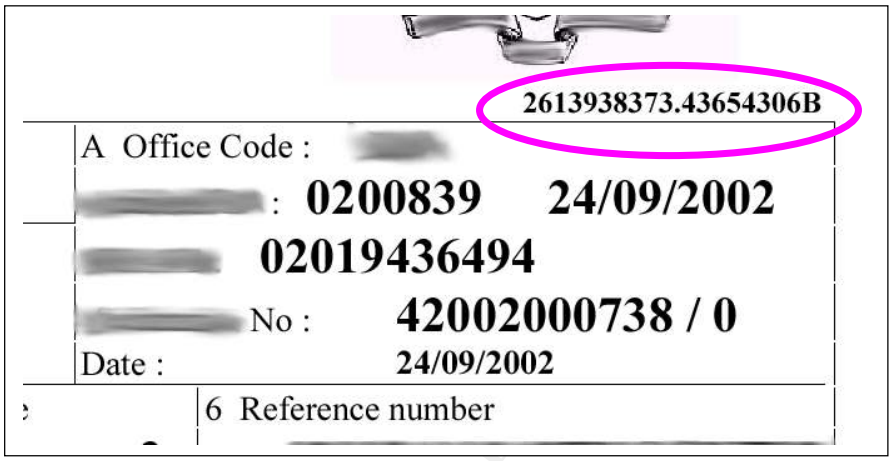
- This was then used to read off the position of a second key or password known only to the author and the programmer. The final result was a alphanumeric character that varied with every printing because of the random digits to the left and right of dot.

- The second key or password was made alphanumeric to allow more possibilities than just 10 possibilities.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- While the method used above was considered much weaker than a message digest like MD5 or "hash" algorithms like SHA-1, there was not enough time to implement these.

  A copy of the pseudo-code is provided as Exhibit B, courtesy of the Anonymous programmer. See also Figure 2 below.



c. Limiting the amount of information in the "public domain". After a detailed discussion with the management, the implementation objective was then modified to discourage forgers rather than verification or authentication, since all the data and information could be verified online, in real time by authorized users. As such, the details on the generation of these check digits need not be made known to all personnel within Firm_A.

d. A report by the author was made to the management to inform Firm_A of all the details and how the check digits were generated. Only one hardcopy of the report was generated and provided to Firm_A. Some intentional mistakes were made to provide authenticity. See Exhibit C for a copy of the report that was submitted by the author to Firm_A's management.

e. The final algorithm and second encryption key was kept secret between the author and the programmer. And apart from the author and programmer, no other persons were involved. Programmes were compiled on the Programmer's laptop and only executables was given to Firm_A.

f. Finally the management was advised of the physical safeguards (online access, legal statements and continuous monitoring) as part of the due diligence process.

Time used for completion of task : 5 days including implementation.

The main benefits of the added security features were :

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1. By adding the shifting operations, the "guessing" of the relationships between any selected amount figure and the cipher text was made a little more difficult, even though they were fixed with every printing. (Protection against external forgers)

2. Apart from the author and the programmer, no other person knew the second encrypted key and mathematical function. This was kept as a separate calling program and not kept within the source codes of the front-end-software which would be ultimately delivered to Firm_A. (Protection against internal users with access)

3. This calling program might be "by-passed" or improved upon with a replacement if Firm_A decides to do so in the future. (Protection against external programmers / consultants). However, so long as the management of Firm_A decided to maintain the check digits, the features above would make potential attempts or attacks, by even the software programmers within Firm_A, more difficult or time-consuming.

4. Potential frausters might also be discouraged to forge the printout by making simple cryptanalysis through pattern guessing or matching a little more difficult.

5. The design-implement process (only 2 pesons were involved from start to end) and limited circulation of information and documentation also helped to limit the possibilities of information leakage. (Need to know principle)

6. Separation of duties was achieved as the author contributed to the method and do not have access to the program source codes. In addition, both the programmer and the author do not remain on site after the project was completed. The changes were also easily understood and implemented by the programmer which was important due to the lack of time.

6.0 Case Study 2 : System and Data integrity

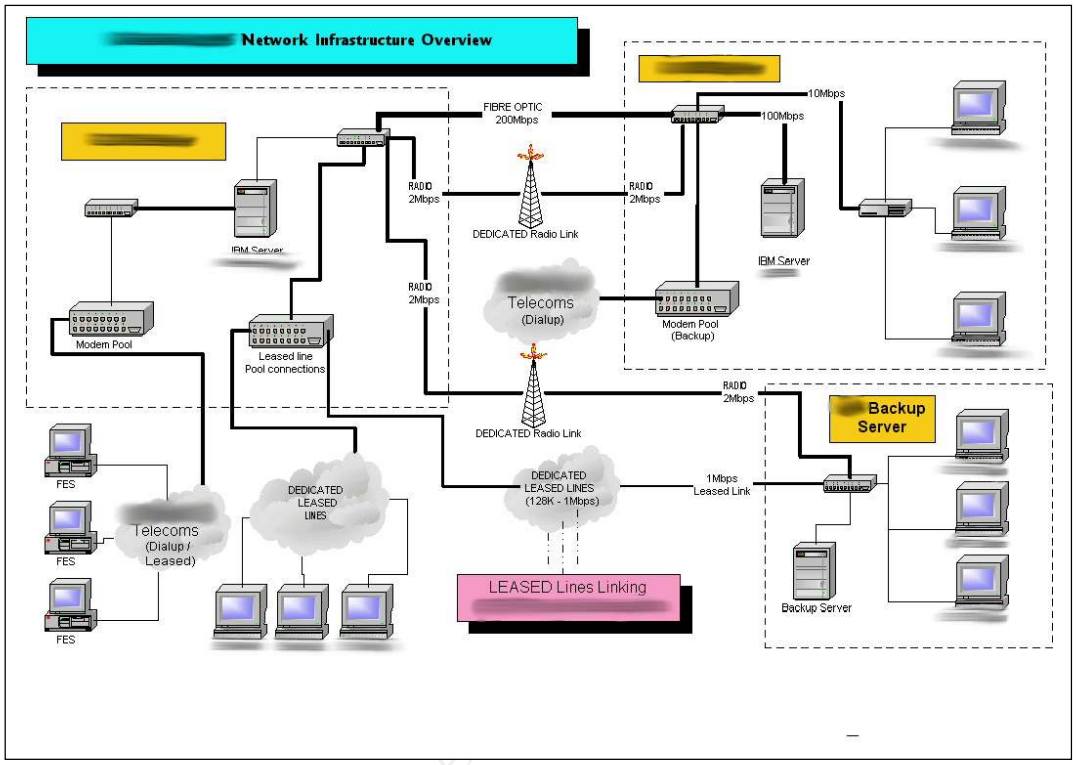
6.1 The Issue

While various security measures had been taken, there was no definitive way for Firm_A's management to know for sure. At the same time, the high visibility of the project meant that the company could ill-afford the bad publicity nor the deterioration in customer confidence caused by a major network or system security incident.

Confidentiality safeguards were found to be far more difficult and sensitive to enforce at the time of writing. It was decided that implementing integrity measures might be a more pragmatic, neutral and attainable security objective. This is especially so given that the network infrastructure had to be connected to external and third party networks, although the application and network environment was primarily non-web-based. See Figure 3 below for an

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

overview of the essential network components. Office intranet and other supporting systems and network were omitted.



All External Users accessed the network and systems via dedicated leased lines or dialup telephone lines (through TCP/IP over asynchronous or leased tele- communications). All the lines were administered by the local public telecommunication company or third party network provider. The company also owned some of the dedicated lines (Fibre-optic and radio) although the equipment installation, administration and monitoring were outsourced to the third party provider.

6.2 The methods implemented

By design, the network and systems were relatively secure against web based attacks as it was a closed network using custom-built, legacy communications software developed from the early days of telnet, sendmail and ftp. However, as this network was connected to the office intranet which was in turn connected to the Internet, the exposure to attacks from the Internet remained.

In all cases, "security by obscurity" was also not a good principle to live by, as observed by Chad M. Steel in his GSEC practical [4]:

> Despite this advantage (of a Proprietary Security Infrastructure), the system relied upon security through obsurity. There was no independent verification or validation of the proprietary security infrastructure, and no way of knowing the true protection it afforded.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The following areas / methods were already in the plans or implemented by the System and Security teams at the time of writing :

a. Formulation of security policies for use in-house, by third party service providers and for the Government Agency.
b. The Security team as part of the training programme for external users conducted awareness seminars on Security.
c. Border Router - the "Internet- or External-network-facing" router
d. Firewall - Checkpoint Firewall-1
e. Use of NAT (Network Address Translation)
f. VPN (Virtual Private Network - for internal cross border communications)
g. Physical security and access control, including the use of access cards and closed-circuit television cameras.

6.3 The additional security measures recommended

While the above measures were deemed adequate at the time the network was launched, additional measures were recommended to further protect the network from intrusions and unauthorized systems tampering, accidental or otherwise.

The approach adopted (still implementing) was as follows :

a. Educate the management of the importance of information security and protection of systems through the use of intrusion detection systems and data integrity tools. See Exhibit D showing an email sent to the management of the Firm_A.

b. Share security-related information with the Systems and Security teams by introducing the concepts of data integrity and intrusion detection. [5]

c. Help ascertain the costs, resources and processes for its effective implementation. For example, apart from regular backups, images of the hard disks and databases were also backed-up regularly and stored away.

d. Allow Firm_A to decide whether these products would be needed but continue the sharing of information and experiences that security implementation is a "process" and thus, can be done in phases.

e. If and when authorized, assist Firm_A to chart the course towards a more secure network and systems environment and obtain assurance by adopting international standards such as BS 7799-2:1999.[6]

f. If directed, and provided there was no conflict of interest, understand the company's security requirements and promptly recommend suitably qualified security professionals to provide the necessary expertise or audit services depending on the needs of the company.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

By allowing management to understand the issues revolving Information security, it was hoped that more "enforceable" security measures could be implemented gradually and enforced over time.

On the technical front, various security documentation and products were introduced to the technical teams for their information and perusal [7]. The next stage would be to implement these measures in phases.

Leading website such as those below were also introduced to the teams :

- http://www.sans.org/top20
- http://cve.mitre.org
- http://www.cert.org

Time for completion: Ongoing

Main Benefits of this approach :

1. A balance between management concerns and sensitivities of the technical teams was attained. Ownership of the decisions and the responsibilities of further actions were placed on the respective teams.

2. Management would gradually have the information and tools to decide for themselves and not be led or "perceived" to be led by one party or another. The role of the author was advisory because the charter was not to implement security measures in the company. The author can thus maintain independence, neutrality and not be involved in "turf wars".

3. The technical teams were given their time and opportunities to consider and decide which necessary security measures should be implemented, especially after the network and systems had been in production for a period of time.

7.0 Post Implementation and the "Big Picture"

7.1 From a Management Perspective

Management deserved to be educated, formally or informally, on Information security matters so that key decisions were not abdicated to IT or Security teams. To illustrate, an article in the November 2002 issue of Harvard Business Review, entilted " Six IT Decisions Your IT People Shouldn't Make", Jeanne W. Ross and Peter Weill stated [8]:

> (One decision Under "Execution" was)
> What security and privacy risks will we accept ?
>
> (And Under "Senior Management's Role", managers need to)
> Lead the decision making on the trade-offs between security and privacy on one hand and convenience on the other.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

(And the "Consequences of Abdicating the Decision" were that :)
An overemphasis on security and privacy may inconvenience customers, employees, and suppliers; an underemphasis may make data vulnerable.

Certainly from a management perspective, costs was not always the issue but economic value was. The management had to constantly seek the best value for all its assets and investments, and this included products, people (training) and processes (time and effort spent).

As such, management usually required from the technical / operational team :

a. assurance that the systems and networks set up were secure and met the requirements of the business and its processes;

b. formal documentation to show evidence of :

- constant monitoring of facilities, systems and networks
- reporting of incidents and the responses to those incidents
- presentation of evidence in times of need
- allowing independent audit and later certification

c. regular updates, constant education and communication of the changing trends in the IT and information security fields

7.2 From a Systems and Security Teams Perspective

Given the perpetually short time frame (e.g. "we need it yesterday") for the implementation of the system and network and the relative lack of resources, availability was usually the first main concern (e.g. "spare me the details, when will it work / work again ?"). As such, security implementation and enforcement had to sometimes take a lower priority, especially when there was a competition for scarce resources.

Usually, a lot of the behind-the-scenes work had already been done to ensure that the systems and network met the requirements of the business processes and users (both internal and external). Unfortunately, reporting or formal documentation, seen by many technical personnel as a chore, usually lagged behind the actual work done. The situation was also made a little more complicated as technical teams were also learning on the job as they were implementing such projects for the first time.

8.0 Lessons learnt

Many security lessons were learnt. The most important ones were :

a. Patience and pragmatism was the key in this environment. Balancing between the idealism of best practices and the realism of the real-world

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

environment was a continuing management process. International best practices while applicable to many cultures and environments, they needed to be modified to suit the local context.

b. "Positive approach" - was a principle that was constantly used so as to avoid cultural sensitivities and focus on the job or task on hand. Frequent and effective communications, sharing of information and knowledge were also perceived to be positive traits accepted by all as the company was still learning the ropes of the new network business.

c. "Unenforceable policy" was a frequent discouragement to both the management and technical teams of a company. While the intentions of the management were clear to the author, the policy decisions and statements sometimes made enforcement a tedious chore. In some cases, it caused some degree of irritation to the technical teams who were by nature or training tended to be more task-oriented.

d. International Courses and Certifications from institutions such as The SANS Institute[9] and (ISC)[2] which administered CISSP (Certified Information Systems Security Professional) [10] were important in such an environment because it reflected the attainment of a certain level of technical knowledge and competence in the field of information security.

9.0 Conclusion

Implementing security measures in a difficult environment is possible. It takes a little more patience and time when compared to other similar projects but different environments. While international best practices may not always apply to a particular environment, they serve as useful guides and directions for advisors, implementers and management alike.

Security risks, tasks and incidents will always be a part of daily operations in a network environment, so long as systems and networks are connected to the outside world, via the Internet or POTS (Plain Old Telephone System).

While access and authorizations may not always be given to the Information Security Professional, this does not and should not stop one from continuously trying to share and educate those involved, albeit from a neutral and independent role. Afterall, education is but one of the values of a good Information Security professional.

10.0 Reference Materials

The following materials provided the necessary inspiration and guidance, without which this practical would not have been possible and would have taken a longer time to complete.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

BOOKS

Harris, Shon. The CISSP All-in-one Exam Guide. McGraw-Hill Osborne Media : Book&Cd-Rom edition. December 26, 2001.

PAST PRACTICALS

Brassinne, Pierre de la. "Web Application Security for Managers". GSEC Practical Assignment. August 24, 2002. http://rr.sans.org/appsec/managers.php (23 Nov 02)

Keim, Scott. "Implementing a Comprehensive Security Program in an Existing Environment". GSEC Practical Assignment Version 1.4. September 9, 2002. http://www.giac.org/practical/Scott_Keim_GSEC.doc (23 Nov 02)

Osgood, Dustin. "ASP Security; Defense in Depth". GSEC Practical Assignment Version 1.4. November 16, 2002. http://www.giac.org/practical/Dustin_Osgood_GSEC.doc (24 Nov 02)

OTHERS

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). "Information Technology - Code of practice for information security management", **ISO/IEC 17799:2000(E)**, First edition 2000-12-01

11.0 List of Exhibits

Exhibit A : Pseudocode of check digit generation before intervention

Exhibit B : Pseudocode of check digit generation after intevention

Exhibit C : Actual Report given to management by the author

Exhibit D : Actual Email written to management to increase security awareness

Note :

For reasons of confidentiality, information relating to entities or identities is masked and changed in the Exhibits to protect the identity of Firm_A from the public domain. All information is provided "as is", unabridged but sanitized. Potential users please check before use.

12.0 End Notes

The list of footnotes used in the practical.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Exhibit A : Pseudocode of check digit generation before intervention
(Source : Anonymous programmer from a different country)

```
String Constant : ENCRYP_ID = '07890123456'
String Constant : DECRYP_ID = '03456789012'
Set EncryptionMode = 'E'
Set PartCodeTwo = ''
If (Message_Status= 'A' OR Message_Status= 'B' OR Message_Status= 'C'
    Message_Status= 'D')
    Set RandomNumber = GetRandomNumber(0 -9)
    Set InitialNumber = GetName()||RandomNumber||GetDesc()||
                        RandomNumber||GetDetail()||RandomNumber||
                        GetSelXxx()||RandomNumber
    Set ANumber = Repeat('9', Length(InitialNumber))
    Set PartCodeOne = GetString((GetNo(ANumber) – GetNo(InitialNumber)))
    If (Length(PartCodeOne) < Length(InitalNumber) )
       PartCodeOne = Repeat('0', Length(InitalNumber) - Length(PartCodeOne) )||
                     PartCodeOne
   End If
   If EncryptionMode = 'D'    --  To Test For Encrypted Amount Only
      Set  AnySelectedAmount  = '?'
   Else
       Set AnySelectedAmount = GetAnySelectedAmount()  – From DOCM
   End If
   If AnySelectedAmount > 0
      For EachCharacterOf(AnySelectedAmount) :
         Set  ANumberOne = GetAsciiCode(OfCharacter)  – 47
         If EnCryptionMode = 'E'
            Set PartCodeTwo = PartCodeTwo||SubString(ENCRYP_ID, Anumber + 1, 1)
         Else
            Set PartCodeTwo = PartCodeTwo||SubString(DECRYP_ID , Anumber + 1, 1)
         End If
      End For
   End If
   If EnCryptionMode = 'E'
      Set RandomNumber = GetRandomNumber(0 -9)
      Set PartCodeTwo = PartCodeOne||'.'||PartCodeTwo||RandomNumber
   End If
End If
```

Additional Note : The programmer used "Decryption" routine to help check that the program was correctly encrypted. In all cases, a simple one-way hash or encryption method followed by matching, was considered to be sufficient for off-line verification purposes.

© SANS Institute 2003, Author retains full rights.

Exhibit B : Pseudocode of check digit generation after intevention
(Source : as before)

```
String Constant : ENCRYP_ID = '07890123456'
String Constant : DECRYP_ID = '03456789012'
String Constant : CHAR_ID = 'XXXXXXXXXXXXXXXXXXXXXXX'
Set EncryptionMode = 'E'
Set PartCodeTwo = ''
If (Message_Status= 'A' OR Message_Status= 'B' OR Message_Status= 'C'
    Message_Status= 'E')
    Set RandomNumber = GetRandomNumber(0 -9)
    Set InitialNumber = GetName()||RandomNumber||GetDesc()||
                        RandomNumber| |GetDetail()||RandomNumber||
                        GetSelXxx()||RandomNumber
    Set ANumber = Repeat('9', Length(InitialNumber))
    Set PartCodeOne = GetString((GetNo(ANumber) – GetNo(InitialNumber)))
    If (Length(PartCodeOne) < Length(InitalNumber) )
       PartCodeOne = Repeat('0', Length(InitalNumber) - Length(PartCodeOne) )||
                     PartCodeOne
   End If
   If EncryptionMode = 'D'   --  To Test For Encrypted Amount Only
      Set AnySelAmt = '?'
      If Length(AnySelAmt) > 3
         If Length(AnySelAmt) = 4
            Set AnySelectedAmount = SubString(AnySelAmt, 2,1)||
                                    SubString(AnySelAmt, 0,2)
         Else
            Set AnySelectedAmount = SubString(AnySelAmt, Length(AnySelAmt) – 2,1)||
                                    SubString(AnySelAmt, 2,  Length(BoeTotQty) – 3)||
                                    Sub  String(AnySelAmt,0,2)
         End If
      Else
         Set AnySelectedAmount = SubString(AnySelAmt, 0, (Length(AnySelAmt) – 1))
      End If
   Else
      Set AnySelectedAmount = GetAnySelectedAmount() – From DOCM
   End If
   If AnySelectedAmount > 0
      For EachCharacterOf(AnySelectedAmount) :
         Set ANumberOne = GetAsciiCode(OfCharacter) – 47
         If EnCryptionMode = 'E'
            Set PartCodeTwo = PartCodeTwo||SubString(ENCRYP_ID, Anumber + 1, 1)
         Else
            Set PartCodeTwo = PartCodeTwo||SubString(DECRYP_ID, Anumber + 1, 1)
         End If
      End For
   End If
   If  EnCryptionMode = 'E'
      If Length(PartCodeTwo) > 2
         If Length(PartCodeTwo) = 3
            Set PartCodeTwo = SubString(PartCodeTwo, 1,
                              2)||SubString(PartCodeTwo,0,1)
         Else
            Set PartCodeTwo = SubString(PartCodeTwo, Length(PartCodeTwo) – 3, 2)||
                              SubString(PartCodeTwo, 1, Length(PartCodeTwo) – 3)||
                              SubString(PartCodeTwo, 0, 1)
         End If
      End If
      If EnCryptionMode = 'E'
         Set RandomNumber = GetRandomNumber(0 -9)
```

© SANS Institute 2003, Author retains full rights.

```
        Set PartCodeTwo = PartCodeOne||'.'||Part CodeTwo||RandomNumber
          Set CumulateNumber = CumulateEachNo(PartCodeTwo)
          Set CumulateNumber = GetModulus(CumulateNumber, XX)
         Set PartCo deTwo = PartCodeTwo||SubString(CHAR_ID, CumulateNumber, 1)
      End If
   End If
End If
```

SEPARATE CALLING PROGRAM

For added security, the following pseudocodes in bold may be placed in another separate program:

```
String Constant : CHAR_ID = 'XXXXX XXXXXXXXXXXXXXXXX'
Set CumulateNumber = CumulateEachNo(PartCodeTwo)
Set CumulateNumber = GetModulus(CumulateNumber, XX)
```

Additional Note : The programmer used "Decryption" routine to help check that the program was correctly encrypted. In all cases, a simple one-way hash or encryption done on the source text and matching the two ciphers was considered sufficient for off-line verification purposes.

© SANS Institute 2003, Author retains full rights.

Exhibit C : Actual Report given to management by the author

To : Mr. <Manager>, <FIRM_A> Only Dated : DD MMM YYYY

From : Raymond Wee

Subject: Printing of some security numbers on Hardcopy <Application>s to provide some levels of authenticity and validity on request of <Firm_A>

1.0 Background / Issue

As hardcopy <Application Document>'s will be printed and used for <Application> <Approval> under the <Country_X> <Doc Processing> System, there is potentially a risk that these hardcopies may be duplicated, used for fraudulent and/or for purposes other than <Gov Agency> <Approval>.

As such, a Security Feature has been added into the printing function of the Front End Software (FES) so as to generate 2 sets of numbers at the TOP RIGHT HAND corner of the printed <Application Document>. See Figure 1 below. As can be seen, it contains Two sets of digits separated by a Dot.

(ACTUAL FIGURE MASKED)

Figure 1 : Two sets of security numbers separated by a DOT.
Found Only in validated and accepted Printed <Application Doc>

2.0 Security Application

2.1 The Security Feature applies only to those Hardcopies printed as Validated <Application Document>s. For Unvalidated <Application Document>s, a message stating "This is not a <Gov Agency> Validated Document" is printed instead of the Signature Block in the Left Bottom Box. See Figure 2 below.

(ACTUAL FIGURE MASKED)

Figure 2 : Signature Block in Un-Validated Printed <Application Doc>

A <Gov Agency> validated printed <Application Document> is show in Figure 3 below.

(ACTUAL FIGURE MASKED)

Figure 3 : Signature Block Found Only in Validated Printed <Application Doc>

2.2 The Security Numbers Feature only applies to FES used by Registered <Applicant>s installed into their computers AFTER DD MMM YYYY. No earlier versions of FES contain this security function.

2.3 The hardcopies of other FES (<other stakeholder users>, etc) are not affected as these are NOT full fledge <Application Document>s and do not contain all the info and/or look like valid <Application Document>s.

3.0 The solution (Part 1 - public - for Restricted circulation)

3.1 How to identify a VALID <Application Document> (Face Vet of Hardcopy <Application Document>)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

a. A single-digit random number placed immediately to the lef t of the DOT is used as a "seed". E.g. "8"

b. Deduct the "seed" from 9 (Nine) to get a NEW "Separator" number. I.e. "1"

c. Obtain a series of numbers on the Printed <Application Document> IN THE ORDER BELOW :
   - Numeric <Application> No. (6th to 11th position) - e.g. 12002000038 = 38
   - Code No. - e.g. 0
   - <Details> (in xxxxxxx) - e.g. 1
   - <SelectXXX> (in xxxxxx) - e.g. 120

d. Group the series of numbers above using the "Separator" number as a separator in between them.

e. Use 9 (NINE) to DEDUCT EACH DIGIT in sequence with the "Separator" Number in between.

f. Compare the Resulta nt numbers in item e. to the Security Number at the top.

g. The 2 numbers above Must ADD up to 9 (NINE) for EACH DIGIT.

The following is an example to illustrate the encoding process :

1. <Application> No. in full is "000038", which means = "38"
2. Code of <Application> is "0"
3. <Details> (xxxxx) should be "1"
4. <SelectXXX> (xxxxxx) is "120"; and
5. The Single Digit immedia tely to the LEFT of the DOT is 8 ("seed")

Performing the operations in steps a to e above, the steps are :

a. "Seed" No. as shown as the FIRST digit to the LEFT of DOT is "8".

b. New "Separator" No. is therefore : 9 - 8 = 1

c. Using the example above, we have : 38 - 0 - 1 - 120 -

d. Inserting the "Separator" No., i t then becomes : 38 1 0 1 1 1 120 1 or "38101111201"

e. Deducting every digit from 9 (Nine), it produces : 61 8 9 8 8 8 879 8 or "61898888798"

f. If the number in step e. above is NOT equal to the Security Number at the top (all digits appearing to the LEFT of the DOT), the Validity and Authenticity of Pri nted <Application Document> is IN DOUBT . Please proceed to check and verify using the other methods described in section 3.2 below.

A valid Securi ty No to the LEFT of the dot should thus be "61898888798".

It is adviseable that some of the "valid" printed <Application Document>s are further verified (according to section 3.2 below) on a Random basis to monitor the situation.

3.2 Other measures to ensure validity

a. The legal <Application> - Printed <Appli cation Document>s are to be used by <Gov Agency> ONLY !

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The following text are printed to remind ALL potential users of the Hardcopy <Application Document>s other than <Gov Agency>, Collecting <payment points> and <Applicant>s that :

- It is a "<APPLICATION> FOR <GOV AGENCY> USE ONLY" - this is printed at the top of Printed <Application Document>s, just below the Logo.
- "The information and particulars on this document are for use by the <Country_X> <Gov Agency> only." - found in the signature block of the printed <Application Document> validated by <Gov Agency>.

As such, ALL OTHER USERS of printed <Application Document>s use them at their OWN RISK !

b. <BACK-END SYSTEM> or Message verification

ALL Authorised users of the Hardcopy <Application Document>s like <Gov Agency>, <Payment Points> and <Other users> have access to either :

- The <BACK-END SYSTEM> (<Country_X> <Gov Agency> System) via a valid login and password, coupled with the relevant online access control (data, menu & program screens and report access); all access within <BACK-END SYSTEM> is also logged with user interventions stamped with a date and time to produce an Audit Trail; OR
- The Front End Software which contains ALL the valid <Application Document>s and <Response Messages> as the case may be. Different parties at different points of the <Approval> Process will receive various <Response> messages, generated by the Systems with a date and time stamp to produce an Audit Trail.

As such, the authenticity of the printed <Application Document> may be verified at the Message- or <BACK-END SYSTEM> level by contacting and checking with the appropriate parties involved.

c. <Firm_A> Messaging System verification

All messages submitted to and routed by <Firm_A> are archived and logged within the <Firm_A> Messaging system.

If necessary and duly authorised, these messages may be retrieved for further verification purposes. The messages are also archived into tapes for storage.

4.0 The solution (part 2 - For Restricted internal use witin <FIRM_A> only)

4.1 How to further check validity of Printed <Application Document>s

As an additional security measure, another set of numbers are added to the RIGHT of the DOT. Here are the steps to obtain the security number for similar matching purposes.

1. Encrypt_ID string is set to be as "07890123456".
2. Take all digits of the <Selected Amount>, say "180,000"
3. Take the ASCII code of the digit and deduct 47. Say for "1", it'll be 49 - 47 = 2.
4. Next add 1 to it and the resultant No. will be the position of the digit to read from the Encrypt_ID string above; i.e. 2 + 1 = 3 or 3 rd position.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. The corresponding digit from the Encrypt_ID is : "8"

6. Do the same for all the digits and the resultant number is : "857777" for "180,000" - the <Selected Amount> value at the <a particular location>.

7. Next, shift the last 2 digits to the first and first digit to the last. Ie. "857777" now becomes "775778".

8. Finally, compare the resultant value of "775778" with all the digits to the Right side of the DOT, ignoring the LAST Character (this is a System-Generated Character for other checks).

9. In the rare event that there is only 3 or less numbers, these are only converted and a System-Generated Character added.

4.2 *It is adviseable that knowledge of part 2 of the solution be strictly limited to only 1 or a few authorised personnel within <Firm_A>.*

Additional notes :

1. It is to be noted that none of the numbers generated above are kept in any database of the Front End Software (FES) for security reasons.

2. Only object codes are loaded into the Front End Software (FES) source codes. The source code for this security number-printing program to generate the above codes is also not revealed to anyone within <Country_X>.

3. By design, Each printout of a printed <Application Document> is likely to have a Different set of Part 1 & Part 2 codes even if all the information contained therein is the same. I.e. every time a <Application Document> is printed, Part 1 & Part 2 codes will likely vary. Simply perform the steps above to verify the security numbers or codes.

4. It is noted that Both the solutions above are only meant to be used as a simple first-line defence against potential misuse of the printed <Application Document> - by making the forging of printed <Application Document> a little more difficult. At all times, the checks under section 3.2 are the only legal and authoritative verification methods.

5. The above program was developed to meet a specific need of <Firm_A> and was developed with limited resources. In the event that <Firm_A> need not require this security feature and/or needs to improve on it, <Firm_A> programmers only need to remove it from the FES source codes and insert it with a better security program, if needed.

6. Finally, No soft copies of this document and the security program is found on ANY computer linked to the <Firm_A> network or in <Country_X>. Only ONE hard copy of this document is given to <Firm_A> management on DD MMM YYYY.

It is hoped that the security features above is sufficient to serve its purpose.

Thank you for your attention.

This document is prepared by the undersigned on the specific request of <Firm_A>.

Author's note : An update was made to this report manually just prior to the report submission (e.g. point 4.1 item 8) and the original document was generated with a print-date-time-stamp.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Exhibit D : Actual email written to management to enhance security awareness

Email dated 20 Xxxxxx 02…

Hi guys,

I thought I should share some info and suggestions on Informatio n Security, so as to help you guys better understand some of the issues / decisions that may be involved in this area.

It is also hoped that by understa nding the technologies or issues better, you may make better decisions when needed.

I'll try my best to present the technical material in a manner that you can hopefully understand.

It is meant to be only an overview based on my training and past experi ences and is NOT meant to be an exhaustive nor expert advice on the subject matter.

Please feel free to comment and/or verify as yo u deem fit. And me know if it is unclear or too technical, etc.

So Here goes ...

========== ==========

A. What is Information Security ?
==========
Info Securi ty usually means 3 things (as defined in ISO17799 or BS7799):

a. Confidentiality - ensuring that informa tion is accessible only to those authorized to have a ccess;

b. Integrity - safeguarding the accuracy and completeness of inf ormation and processing methods;

c. Availability - ensuring that authori zed users have access to informat ion and associated assets when required.

A copy of the BS7799-1:1999 Part 1 and 2 will be circulated to you for your reading pleasure ...

There are many standards* in implement ing InfoSecurity (e.g. XXXXX IT Security standards, etc) but I suggested BS7799 bec ause it is simil ar to ISO 17799 ... meaning <Firm_A> may then get ISO certification at a later date if necessary.

* Other standards for your info :

IETF (Internet Engineeri ng Task Force)
Site Securi ty Handbook
http://www.ietf.org/rfc/rf c2196.txt?number=2196

NIST (National Instit ute of Standards and Technology)
Principles and Practices for Securi ng IT Systems
http://csrc.nist. gov/publications/nistpubs/800-14/800-14.pdf

For more : visit - Center for Internet Secuity
http://ww w.cisecurity.org/ click on Standards

B. How to implement ?
==========

© SANS Institute 2003, Author retains full rights.

Most of us are clear - need a policy, need to implement and enforce it, etc., get the necessary software, firewalls, intrusion detection systems, etc.

On policy, there are also those that are "Un-enforceable" as well. These may be due to legal or cultural reasons because as managers, one cannot sit behind each employee to see what they do. And being computers and networks meant IT or people with access can easily view / change the data in the computer or networks.

As such, a pragmatic approach is suggested :

a. Determine what <Firm_A> wants (e.g. get certification on ISO ... ONE DAY)
   - Security "Direction"

b. If so, compare current policy with that of ISO.
   - Security policy "review" or enhancement

c. Determine Gap Analysis with a recognised benchmark (e.g. ISO) and do a simple risk analysis as well (how vulnerable, how real is the threat, etc)

d. Determine what measures are FEASIBLE & Acceptable under the legal and cultural constraints... e.g. one may install state-of-the-art Intrusion Detection System (or IDS) but may NOT have the means nor legal backing to take action or prosecute, then may be other measures could be considered.

d. Once the necessary policy decisions can be made on the various Non-compliance ;-) or gaps, <Firm_A> may then consider how and when the remedial and/or preventive measures may be taken.

e. In parallel, while deciding on the operational side, <Firm_A> may look at securing the Systems and Network side and implement all the measures.

   Typically, this is done at the technical level and the common sites that security techies use to secure their systems include (the more popular ones) :

   1. The Twenty Most Critical Internet Security Vulnerabilities
      (Updated) ~ The Experts' Consensus
      Version 3.21 October 17, 2002, compiled by SANS/FBI
      Copyright © 2001-2002, The SANS Institute

      To view, visit http://www.sans.org/top20/

      (RW: From a security techie perspective, this is the minimum standard.
      It covers the things to do in order to secure a system or network.
      Btw, SANS = SysAdmin, Audit, Network Security)

   2. Common Vulnerabilities and Exposures (CVE®) ... :
      A list of standardized names for vulnerabilities and other information security exposures — CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

      A Dictionary, NOT a Database
      A Community-Wide Effort
      Freely Available for Review or Download

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Definitions "cut & pasted" from http://cve.mitre.org/
Current CVE Version: 20020625 with Total Entries: 2223

(RW : essentially this lists ALL the current and previous know bugs or security problems that has been uncovered and published by people all over the world. As you can see, it's NOT a small task..)

There are others as well, e.g. CERT (Computer Emergency Response Team, Bugtraq, and other "bugs lists" from the vendors of CISCO, MS, etc)

C. Who, When and What to implement ?
==========

Again, here the issues are clear and in my humble opinion, it is difficult but if <Firm_A> has the will, implementation can be done in phases, starting with the issues that <Firm_A> thinks is most important. <Firm_A>, like many other companies in the world, may NOT be able to achieve 100% security but with the implementation of the key measures, <Firm_A> will be certainly be "better off" than it is today.

From my perspective, I feel that integrity of the system is most important and neutral at this stage so I would like to recommend Tripwire (a common tool used by security techies to record images of systems - for "filing" or comparison later - or even to be used as evidence, if necessary).

Here are the information on Tripwire for your info. I would also be passing brochures, etc to you guys directly. Please feel free to contact them directly if necessary. There are also other similar tools but Tripwire is the most well known - mentioned in Information security books and courses.

<<Attachment : Tripwire for Layered Security Strategy.pdf>>

The white paper entitled : Tripwire for Layered Security Strategy is fyi. Although a little technical, it provides some technical explanations on Information Integrity and IDS in general. It also covers other more technical topics like Vulnerability Assessments, etc.

By the way, "Layered Security Strategy" is Tripwire's way of describing a common Security concept called : Defense in Depth - meaning have several "lines of defense" against attacks.

D. What is IDS (Intrusion Detection Systems) ? and why ISS Real Secure ?
==========

Intrusion Detection as the name implies means finding out if someone has been INSIDE the firewall doing damage to systems or networks or changing data or information, etc. through the use of known techniques or "signatures".

ISS Real Secure is typically recommended (and first suggested by <Firm_A> Security Team) because it is quite popular and scored the highest marks in an independent test by The NSS Group - "Europe's foremost independent network and security testing organisation".

Version 3 of the IDS Group Test dated July 2002 (may be a little techie) is found on the web site of NSS - Registration is free but needed.

http://www.nss.co.uk/ids/edition3/introduction.htm#INTRODUCTION

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The report basically compares the popular IDS products and sort of rate them after testing them based on a set of criteria. Visit the NSS site for more info - http://www.nss.co.uk.

A key point about IDS, from a management view, is found in one paragraph (about page 11 of 14 in a printed copy of the report) :

"Intrusion Detection Systems are good at sounding alarms, but unless there is someone around who is prepared – and trained – to respond (even if it is only to determine that the alert is a false positive), it is no better than a car alarm that everyone ignores. An effective response is every bit as important as detecting the attack in the first place."

FYI, a "false positive" is a techie term for a "false alarm"...

Finally
======

I think that is sufficient for now... before I overload your brains ;-).

As mentioned, do let me know if you want me to continue, in which case, I would gladly do so in subsequent emails - esp. on topics of <Firm_A>'s interest. My charter for the trips DO NOT presently include security matters, so may I seek <Firm_A>'s official authorization if <Firm_A> wants me to do the Information Security-related work and/or implementation.

In all cases, on an information sharing basis, I have no problems sharing with you guys all that I know (or don't know) as is needed from myself.

Again, I'm not an Expert in this field, so the above notes are only my info-sharing and suggestions and that you guys Decide what's Best for <Firm_A>, please... especially on product procurement, etc. Please also verify them for yourselves if needed.

Many Thanks for your attention and sorry for the long email. .. and information bombardment... ;-) I just hope the info helps you !

Cheers and have a nice day !

Raymond Wee

Author's note : The above is shared with the manager and financial controller, whose basic training were not in the IT field unlike the author. This email was the result of a query that came up after they found out that the author had recently taken and passed the CISSP (Certified Information Systems Security Professional) examinations.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

End notes

[1] Transparency International. "The 2002 Transparency International Corruption Perceptions Index". http://www.infoplease.com/ipa/A0781359.html (23 Nov 2002)

[2] Northcutt, Stephen., Zeltser, Lenny., Winters, Scott., Frederick, Karen Kent., Ritchey, Ronald W., Inside Network Perimeter Security : The Definitive Guide to Firewalls, VPNs, Routers and Intrustion Detection Systems. Indianapolis : New Riders Publishing, First Edition, June 28, 2002. Page 13.

[3] The programmer is a developer of the proprietary front-end-software application who is a sub-contractor to Firm_A. As a deliverable under their contract with Firm_A, all the source codes, program specifications and related documentation will be handed over to Firm_A in the near future. He preferred to remain anonymous for purposes of this paper.

[4] Steel, Chad M. "Implementation of a Secure Web Environment for a Government Agency". GSEC Practical Assignment. July 10, 2002. http://rr.sans.org/casestudies/gov_agency.php (23 Nov 02)

[5] Among the information papers shared included :

a. Tripwire Inc. "Data Integrity Assurance In A Layered Security Strategy - Providing The Essential Foundation for Data Security". PDF Version 1.3, August 9, 2002. http://www.tripwire.com/files/literature/white_papers/Layered_Security.pdf (16 Nov 2002)

b. Tripwire Inc. "Data and Network Integrity Assessment Tools: Fundamental Protection for Business-Critical Systems, Data and Applications". PDF Version 1.2, February 6, 2001. http://www.tripwire.com/files/literature/white_papers/DNI_tools.pdf (24 Nov 2002)

c. Tripwire Inc. "How Tripwire supports standards set by BS7799 / ISO17799". PDF Version 1.2, May 30, 2001. http://www.tripwire.com/files/literature/white_papers/How_Tripwire_Supports_ISO17799.pdf (24 Nov 2002)

[6] The British Standard. "Information Security Management - Part 2 : Specification for information security management systems ", **BS 7799-2:1999**, Incorporating Amendment No. 1, February 2001. Page 2, Figure 1 - Establishing a management framework.

[7] Documents shared with the technical teams included :

The SANS Institute "Solaris Security : Step-by-Step Guide", The SANS Institute, Version 2.0, February 2001

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The SANS Institute "Windows NT Security : Step-by-Step Guide", The SANS Institute, Version 3.03, February 2001

The SANS Institute. "Disaster Recovery and Business Continuity: Step-by-Step Guide", The SANS Institute, Version 1.0, February 2002.

The SANS Institute. "Computer Security Incident Handling: Step-by-Step", The SANS Institute, Version 2.2, October 2001.

[8] Ross, Jeanne W., Weill, Peter. "Six IT Decisions Your IT People Shouldn't Make" Harvard Business Review November 2002 (2002) : page 87.

[9] The GSEC course and certification (Global Information Assurance Certification / GIAC Security Essential Course) is administered by The SANS (Sysadmin, Audit, Network, Security) Institute. Kindly visit http://www.sans.org for more details.

[10] The CISSP certification is administered by International Information Systems Security Certification Consortium, Inc or (ISC)[2]. Kindly visit the web site at http://www.isc1.org for more details

© SANS Institute 2003, Author retains full rights.