Computers & Security (2004) 23, 371–376

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

The 10 deadly sins of information security management

Basie von Solms[a,*], Rossouw von Solms[b]

[a]RAU-Standard Bank Academy for Information Technology, Rand Afrikaans University, Johannesburg, South Africa
[b]Faculty for Computer Studies, PE Technikon, Port Elizabeth, South Africa

Received 1 April 2004; revised 4 May 2004; accepted 4 May 2004

KEYWORDS
Information security;
Information security management;
Information security governance;
Information security policy;
Information security risk analysis;
Information security compliance

Abstract This paper identifies 10 essential aspects, which, if not taken into account in an information security governance plan, will surely cause the plan to fail, or at least, cause serious flaws in the plan. These 10 aspects can be used as a checklist by management to ensure that a comprehensive plan has been defined and introduced.

Introduction

This paper is based on years of experience in teaching information security to a wide audience, as well as on information security consultancy projects in many companies. The paper identifies the 10 most important aspects—called the 'deadly sins of information security'—which result in companies experiencing severe problems in implementing a successful comprehensive information security plan within the company.

All 10 of these aspects are essential to take into account when implementing such an information security plan in a company, or to be evaluated when an existing information security plan seems to be having problems in being really effective.

From experience, if even one of these aspects is ignored, or not properly taken into account, serious problems in introducing and maintaining a proper information security plan in a company will surely arise.

The paper will briefly discuss each of these aspects or sins, providing some motivation on why their absence from any plan will cause information security related problems.

The paper ends with a 'tick list', which information security managers can use to evaluate the

* Corresponding author. Tel.: +27-41-504-3604; fax: +27-41-504-9604.
E-mail addresses: basie@rau.ac.za (B. von Solms), rossouw@petech.ac.za (R. von Solms).

0167-4048/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.05.002

presence/absence of these aspects from their information security plan.

The 10 deadly sins of information security

These sins are introduced below, and discussed individually in the subsequent paragraphs.

1. Not realizing that information security is a corporate governance responsibility (the buck stops right at the top)
2. Not realizing that information security is a business issue and not a technical issue
3. Not realizing the fact that information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single 'off the shelf' solution)
4. Not realizing that an information security plan must be based on identified risks
5. Not realizing (and leveraging) the important role of international best practices for information security management
6. Not realizing that a corporate information security policy is absolutely essential
7. Not realizing that information security compliance enforcement and monitoring is absolutely essential
8. Not realizing that a proper information security governance structure (organization) is absolutely essential
9. Not realizing the core importance of information security awareness amongst users
10. Not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities

Sin number 1: not realizing that information security is a corporate governance responsibility (the buck stops right at the top, and there are legal consequences)

The realization that information security governance is an essential and integral part of corporate governance has grown specifically in the last few years. The driving force has been several documents on corporate governance which have appeared recently, for e.g. the King II Report in South Africa (King) and ISACA's Control Objectives for Information and Related Technologies (COBIT).

Other papers emphasizing this integration of information security with corporate governance have also appeared, for example (von Solms, 2001).

These documents have been supported by a growing set of laws and legal requirements which have appeared internationally, specifically related to the privacy of customer, client and patient data. Some examples of such laws and legal requirements are the ECT Act in SA (ECT) and the HIPAA Act (HIPAA) in the USA.

The implication of these developments are that the Board of Directors as well as top management, have a direct corporate governance responsibility towards ensuring that all the information assets of the company are secure, and that due care and due diligence have been taken to maintain such security. Compromised company information assets can have serious financial and legal implications for a company, and executive management can be held personally liable in some cases.

Further, it is responsibility of executive management to extensively report on the protection of information assets to the Board of the company.

Consequences of committing this sin: executive management are not performing and exercising the due care and due diligence expected by them, and may open themselves up to serious personal and corporate liabilities.

Sin number 2: not realizing that the protection of information is a business issue and not a technical issue

This sin is closely related to the one discussed above, but is highlighted on its own, because it does provide another dimension to the problem. Information security related problems in a company cannot be solved by technical means alone. The sooner the management of a company grasps this fact, the sooner they will apply due care.

Unfortunately, in many cases, executive management in companies still think that technology is all that is required, and therefore 'delegates or downgrades' the issue to the technical departments, and conveniently forgets about it.

Without the proper, direct and continuous support of such executive management, as well as acting as examples of information security consciousness and awareness, the information security problem will not receive due care or be addressed satisfactorily.

Consequences of committing this sin: technology will be thrown at the information security

problem, without resulting in a total, comprehensive solution. This might also result in money wasted.

Sin number 3: not realizing the fact that information security governance is a multi-dimensional discipline

This sin is again closely related to the one discussed above, but again is significant enough to be mentioned on its own.

Information security is a multi-dimensional discipline, and all dimensions must be taken into account to ensure a proper and secure environment for a company's information assets.

The following dimensions of information security are clearly identifiable—some direct from published literature, and others indirectly from speaking to information security managers. The list of dimensions below is not necessarily complete, because the dynamic nature of information security prevents any such delineation. Some of the dimensions may overlap in terms of its content. However, the number of and precise content of dimensions are not the most important factor—the fact that there are different dimensions, and that they must collectively contribute towards a secure environment, is important.

The following dimensions can be identified without much difficulty:

* The Corporate Governance Dimension
* The Organizational Dimension
* The Policy Dimension
* The Best Practice Dimension
* The Ethical Dimension
* The Certification Dimension
* The Legal dimension
* The Insurance Dimension
* The Personnel/Human Dimension
* The Awareness Dimension
* The Technical Dimension
* The Measurement/Metrics (Compliance monitoring/Real time IT audit) Dimension
* The Audit Dimension

From this list, it is clear that most of these dimensions are of a non-technical nature, which links to the previous discussed sin.

All these dimensions must be taken into account in designing and creating a comprehensive information security plan for a company, because no single dimension, or product or tool on its own will provide a proper all inclusive solution.

Consequences in committing this sin: a 'lop sided' information security solution will be implemented, which will results in frustration as further dimensions will continuously need to be added to the solution.

Sin number 4: not realizing that an information security plan must be based on identified risks

The purpose of information security is to provide measures to mitigate the risks associated with the company's information resources. However, if the company is not very clear on precisely what the potential threats are as well as what assets they are protecting, they may basically be shooting in the dark, and spending money protecting themselves against threats which have a very low probability of occurring, and ignoring others which have a very large impact once they occur.

It is therefore essential that a company must base its information security plan on some type of risk analysis exercise. This can be a very formal, structured and comprehensive exercise, or a more high-level oriented approach in combination with international best practices. The authors, based on experience, prefer the last approach.

However, whatever approach is taken, it must be possible to motivate all actions taken, and all countermeasures suggested, in terms of some form of risk analysis for that specific company.

Consequences of committing this sin: the company may be spending money on risks which may not really be that dangerous, and ignoring others which may be extremely serious.

Sin number 5: not realizing (and leveraging) the important role of international best practices for information security governance

The typical questions the information security manager (ISM) needs and wants answers to, include:

- Against which risks must the information resources be protected?
- What set of countermeasures will provide the best protection against these risks?

These questions are very important, and must receive answers, otherwise the company may waste money on unnecessary or inefficient countermeasures.

Following international best practices for information security governance is based on the concept of 'learning from the successful information security experiences of others'. The idea is that a large percentage of information security threats,

resulting risks, and selected countermeasures are the same for all companies. If a large number of companies have documented their experiences in this area, alongside the countermeasures they have selected for the possible risks, why do a comprehensive risk analysis to probably arrive at the same result?—rather use these documented experiences directly.

- Why redo what others have done already?
- Why re-invent the wheel for well-established environments?
- Learn from and apply their experience!
- The 'bread and butter' aspects of information security are the same in most IT environments.

This is precisely what 'following a best practice' means.

An international best practice (Code of Practice for Information) for information security management normally documents the knowledge of a group of people (companies) as far as their experience with information security management is concerned. It therefore reflects the practices and experiences followed by the relevant people in managing information security.

The challenge to any information security manager is therefore to do the right things right. The question asked by many such managers is: 'How do I know what the right things are?'

If it can be determined what the rights things are, how do you know you are doing it right.

Information security is not a new aspect of IT. Many people and many companies have struggled with information security over many years. In this process, they have found out what are the right things, and how to do them right.

They have therefore determined from experience what best practices are required and how to implement them effectively.

This experience had been documented in a wide set of documents, basically referred to as Standards and Guidelines. These documents are available to new information security managers, and should be used.

They can be seen as the consensus of experts in the field of information security, and generally provide an internationally accepted framework on which to base information security governance and management.

Nobody needs to re-invent the 'information security wheel'. This wheel has been developed, it is documented and should be used as such.

This does not necessarily mean that if these best practices are followed strictly that no security incidents will occur. That is of course not true, but at least an information security manager, and the top management of companies know that they are proving their due care and due diligence by following the advice of experts.

Examples of leading best practices in the area of information security are ISO17799 and ISF.

Consequences of committing this sin: unnecessary time and money is wasted to arrive at a solution which had, most probably, already been documented.

Sin number 6: not realizing that a corporate information security policy is absolutely essential

All international best practices for information security management stress the fact that a proper corporate information security policy is the heart and basis of any successful information security management plan.

Such a policy is the starting point and reference framework on which all other information security sub-policies, procedures and standards must be based.

Such a policy must be short (3—4 pages), and signed by the CEO, showing executive management's commitment and buy-in towards all information security aspects. This is the most visible way in which executive management shows their commitment towards information security in the company.

Consequences of committing this sin: all information security projects and efforts in the company will have no anchoring point and proof of high-level commitment, and will be floundering around without really making progress.

Sin number 7: not realizing that information security compliance enforcement and monitoring is absolutely essential

It is no use having a perfect corporate information security policy, with a comprehensive set of supporting sub-policies, conforming to international best practices, if it is not possible to monitor and enforce compliance to such policies.

'Un-enforced policies breed contempt' is a slogan which should be heeded.

Any information security manager should be empowered through technical and non-technical measurement tools to be able to monitor compliance to relevant information security policies, and act if any discrepancies appear.

Such monitoring and measurement tools must also not be built and dependent on annual or bi-annual internal audit reports—nobody can anymore afford to find out after 6 months that a fired employee still has access rights to the system. Such tools must be real time and provide real time monitoring and reporting.

'You can only manage that which you can measure' is directly related to this sin.

Consequences of committing this sin: a false sense of security may exist and be cultivated because 'we have all the necessary policies in place', without realizing that these policies may not be complied with.

Sin number 8: not realizing that a proper information security governance structure (organization) is absolutely essential

It is essential that a company must have a proper information security organizational structure to make an information security governance plan successful.

Such a structure has to do with the way in which information security is organized and structured in a company. The importance of such structures is stressed by several codes of best practice for information security management, which all states that the existence of a proper organizational structure, including some type of Information Security Forum, is essential for successful information security implementations. This dimension not only refers to the organizational structure itself, but also to aspects like information security related job responsibilities, communication between information security related roles and the involvement of top management with information security. It also includes clarity on what aspects of information security management are to be centralized, what aspects are to be decentralized as well as where the compliance monitoring and enforcement capability will reside (should never be part of the IT Department itself).

Consequences of committing this sin: everything related to and involving information security is automatically referred to the (single) information security manager, who really is not the owner of any information, just the custodian.

If information owners are not clearly defined, and held responsible for the security of the information under their control, severe risks do arise.

Accountability for information security must be shared by all employees, and not only the information security manager. This accountability must be spelled out clearly, and cemented into proper organizational structures.

Sin number 9: not realizing the core importance of information security awareness amongst users

Although this sin is so apparent it needs no discussion, it is still committed by many companies.

No proper awareness programs exist, and users are unaware of the risks of using the company's IT infrastructure, and the potential damage they can cause.

Furthermore they are often not even aware of the information security policies, procedures and standards existing in the company.

Users cannot be held responsible for security problems if they are not told what such security problems are, and what they should do to prevent them.

In many cases it is realized that money spent on comprehensive user information security awareness programs is some of the best money spent on information security.

Consequences of committing this sin: many information security related intensions will fail to materialize if users are not properly educated in this regard.

Sin number 10: not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities

This sin is closely related to sin numbers 7 and 8 above, but is so important that it warrants it be listed separately.

Very often, executive management appoints an information security manager, and expects such a person to do everything alone.

This is not possible, because of the complexity and multi-dimensionality of information security. Understanding and deliberately trying to prevent the sins discussed above, will go a long way in preventing this one.

Consequences of committing this sin: information security managers realize soon that they cannot do their job properly, and either move on, or move out of information security. This opens the company up to severe risks because no continuity exists as well as the fact that the security plan never gets fully implemented.

Conclusion

Creating and implementing a proper information security program is not necessarily rocket science—most of the important components that should be part of such a program are basically common sense. However, very often these common sense issues are ignored because there is a lack of understanding and realizing how essential they are.

This paper attempted to put all these essential components into place.

The following 'tick list' can be used to evaluate your company's information security plan in terms of the 10 deadly sins discussed above.

Our company's information security plan fully takes into account that:

Information security is a corporate governance responsibility (the buck stops right at the top)	Yes	No
Information is a business and not a technical problem	Yes	No
Information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single 'off the shelf' solution)	Yes	No
Information security plan must be based on proper risk analysis	Yes	No
International best practices for information security governance drives our plan	Yes	No
A corporate information security policy is absolutely essential	Yes	No
Information security compliance enforcement and monitoring is absolutely essential	Yes	No
A proper information security governance structure (organization) is absolutely essential	Yes	No
Information security awareness amongst users is core to the success of our plan	Yes	No
Our information security manager is empowered with the infrastructure, tools and supporting mechanisms to properly perform his/her responsibilities	Yes	No

If the answer to any of the above is 'no', serious attention must be given to revisit and re-evaluate that aspect, as well as the complete information security governance plan.

References

COBIT. Available from: www.isaca.org.
ECT. Available from: www.doc.gov.za.
HIPAA. Available from: www.hhs.gov/ocr/hipaa.
ISO17799. Available from: www.iso.ch.
ISF. Available from: www.isfsecuritystandard.com.
King. Available from: www.iodsa.co.za.
von Solms SH. Corporate governance and information security. Comput Secur 2001;20:215—8.

Prof SH (Basie) von Solms holds a PhD in Computer Science, and has been Chairman of the Rand Afrikaans University-Standard Bank Academy for Information Technology at the Rand Afrikaans University in Johannesburg, South Africa, since 1978. Prof von Solms is the present Vice-President of IFIP, the International Federation for Information Processing, and the immediate past Chairman of Technical Committee 11 (Information Security), of the IFIP. He is also a member of the General Assembly of IFIP. Prof von Solms has been a consultant to industry on the subject of Information Security for the last 10 years. He is a member of the British Computer Society, a Fellow of the Computer Society of South Africa, and a SAATCA Certified Auditor for ISO 17799, the international Code of Practice for Information Security Management.

Professor Rossouw von Solms is the Head of Department of Information Technology at Port Elizabeth Technikon, in South Africa. He holds a PhD from the Rand Afrikaans University. He has been a member of the International Federation for Information Processing (IFIP) TC 11 committee since 1995. He is a founder member of the Technikon Computer Lecturer's Association (TECLA) and is an executive member ever since. He is also a Vice-President of the South African Institute for Computer Science and Information Technology (SAICSIT). He has published many papers in international journals and presented numerous papers at national and international conferences in the field of Information Security Management.