Global Information Assurance Certification Paper

Building the better mousetrap

Improving information security through process benchmarking and improvement

SANS GSEC certification
Version 1.2e

Stephen Carroll
31st July, 2001

Contents

I. Introduction

Information security has changed significantly over the last thirty years or so. Information systems have moved from a centralised, highly controlled format to an extremely decentralised (some would argue anarchic) format. The change happened slowly over the first twenty years. It then accelerated due to a number of factors including the advent of the personal computer, the GUI interface, and the rise and dominance of Microsoft. This decentralisation progressed steadily until the early nineties and the explosion of the Internet.

Initially the Internet had been restricted to academic and military sites. Sites made arrangements to connect to each other, very often placing availability as the key requisite over security.

In the early nineties the Internet opened for general admission, suddenly everyone had the ability to connect to a global network for the price of a personal computer, a modem and a subscription with a local ISP (Internet Service Provider). This reduced the level of skill required to compromise a system through easy access to cracking tools and connection to network sites.

Previously the object of network security was to keep everyone out, whereas now the priority became to let the majority of visitors through your network to select authorised areas. As the floodgates opened and more sites were compromised the trust model that had existed before 'general admission' broke down.

While many organisations exploit the potential benefits from deploying advanced technologies, only the truly successful ones understand how to manage the inherent risks.

Security products are often portrayed as the 'silver bullet', vendors rush to provide products that claim to provide '100% security'. Firewall, VPN, IDS, PKI, the list goes on and on yet still the sites fall. So where does it all gone wrong? Very simply security is a process not a product[1]. The products are quite like a television set, that is to say they are of little use until tuned for a particular purpose.

Comprehensive and lasting security works on the principle of Defence in Depth[2]. Defence in depth is the practice of layering defences to provide added protection. Defence in depth increases security by raising the level of effort and resources required to mount an effective attack. The approach places multiple barriers between an attacker and your business-critical information resources. The deeper an attacker tries to penetrate your trust model (see section III), the harder it gets. These multiple layers prevent direct attacks against important systems and avert easy reconnaissance of your networks.

In addition, a defence-in-depth strategy provides natural boundaries for the implementation of intrusion-detection technologies. Ideally the measures you implement should buy you time to detect and respond to a breach, reducing its impact.

Three key factors need to be working together to provide effective information security

1. People who maintain and provide intelligence to the,
2. Process that defines the criteria to manages the,
3. Technology designed to protect your information

The factors need to work together to support each. Unfortunately organisations only spend on tangible items (the technology) while neglecting the process and people elements of the equation. The net result? A compromise occurs and technology is blamed, yet no one ever seems to look at the big picture! The objectives of this paper are to:

- Explain the stages of process maturity
- Walkthrough an approach to benchmarking an organisations state of evolution
- Provide an outline on how to begin the process
- Provide useful references to support you on the road to benchmarking and process improvement

At the end of this paper I hope to have explained and outlined the first steps in the building measurable and lasting information security.

II. Defining process maturity

How can an organisation identify problems in managing information security? The following indicators may be a symptoms of a lacklustre 'defence in depth' strategy.

- No formal security vision, directives or policy endorsed by senior management
- No formal security standards or procedures
- Responsibility and accountability for securing information has not been assigned
- Frequent unauthorised access to data or IT resources
- No formal monitoring of security logs to identify and address potential intrusions or inappropriate use of data assets
- Inability to control access based on "need-to-have" in order to perform job duties
- Absence of audit trails to track changes to configurations or parameters

Many will argue that a structured approach is overkill and take the attitude that 'it hasn't happened up to now so why should it happen in the future'. That is like removing all the fire extinguishers from a building just because it had not suffered a fire up to that point!

The Maturity Model

Organisations wishing to build a measurable and lasting information security solution can now score their current state using the Maturity Model. This table is derived for the Carnegie Mellon software engineering capability model[3]. It allows an organisation to define its level of process management on a risk-focussed basis using specific criteria.

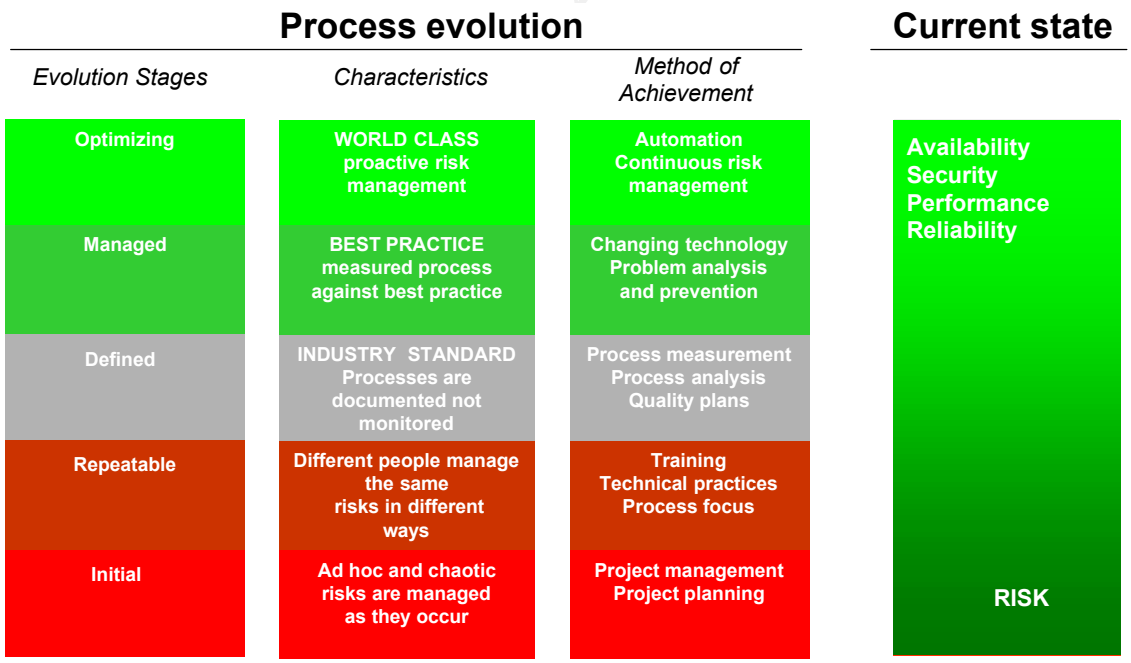

Figure I The Maturity Model

The stages of evolution

The model assumes five states of evolution for any IT management process. They range from initial (completely immature) to optimising (world-class) risk management procedures. I include a grading of the risk of compromise (1 being negligible to 10 being likely) and the possible effect on the business of a compromise.

I also outline for each evolution stage how people, process and technology support the scoring.

Evolution stage	***Risk of compromise (1-10)***	***Effect of compromise***
Initial	*10*	*Business failure*

The initial state of evolution can be defined as a completely immature environment that has not be measured or controlled in any way. It may be an organisation that has experienced rapid growth or one that has not recognised information security risks up to the initial assessment. Problems are dealt with in an ad-hoc fashion as they arise. There is a high risk of compromise with the likely effect being business failure due to lack of procedures to prevent, detect or react to an incident.

Some of the indicators include

People

- Senior management do not acknowledge the need for information security
- Personnel are not provided the appropriate training or skills to effectively administer security

Process

- Security policies, procedures and standards are not defined or documented
- A Security function does not exist and security administration is handled informally

Technology

- Security tools to protect and administer resources are not deployed effectively, if at all
- The IT environment is not secure and the integrity of the environment is unknown
- IT spending is regarded as a cost and not an investment

Examples of organisations at the initial stage

- Small enterprises (up to 250 employees)
- FOMB (Family owned & managed businesses)
- Traditional organisations recently embracing the internet
- Small companies experiencing hyper growth

Evolution stage	*Risk of compromise (1-10)*	*Effect of compromise*
Repeatable	*7*	*Business interruption*

A repeatable state of evolution is where information security is not co-ordinated across the organisation. Different parts of the organisation have different views of its information security needs. The success of information security is dependent on an individuals aptitude and attention to detail. Essentially this is where different people manage the same risks in a similar way.

There is a moderate to high risk of compromise with the likely effect of serious business interruption due to poor prevention controls and a total lack of procedures to detect or react to an incident.

The indicators include

People

- Technical personnel are relied upon to obtain relevant training by themselves
- Enduser awareness training does not occur
- Senior management see information security as an time consuming task providing minimal returns, a 'have to' rather than a 'must have'

Process

- Information security is not a core objective of the organisation
- Security policies, procedures and standards are loosely defined and undocumented
- An information security unit has been formed and assigned resources on a part-time basis
- No formal or independent testing of information security preparations occurs

Technology

- A basic level of security tools are implemented and maintained by outside parties
- The IT environment is 'secured' at pre-implementation but is not reviewed on a ongoing basis
- IT spending is regarded as a luxury rather than a necessity

Examples of organisations

- Small – medium sized enterprises (under 500 employees)
- Manufacturing companies with minimal external links
- Local operations affiliated to global organisations subject to small or no compliance reviews

Evolution stage	*Risk of compromise (1-10)*	*Effect of compromise*
Defined	*5*	*Business interruption*

The defined stage is where information security is recognised and implemented. Preparations are made, a policy is provided and rolled out but the success of this approach is not measured and constantly revised. Information security is still regarded as a luxury rather than a necessity. It is seen as once off exercise, infrequently revised.

A compromise is likely to result in a significant business interruption as the company is unlikely to be familiar with advanced information security techniques such as incident handling and response techniques and does not monitor or measured its existing preparations.

People

- The members of the information security unit have the appropriate skills and aptitude for their assigned responsibilities
- Enduser awareness training is not seen as a critical factor in ensuring information security

Process

- Security management policies have been defined and documented but remain unmonitored
- Procedures and standards are documented for basic security functions
- Responsibilities for Security administration have been assigned to specific individuals
- The integrity of the environment is assumed and the security of the IT resources is not measured

Technology

- Security administration tools are deployed and utilised. Much of the functionality is enabled but automated and not managed
- The infrastructure has a good level of prevention but is weak in the areas of detection and reaction to potential incidents

Examples of such organisations

- Large organisations (over 1,000 employees)
- Small to medium to large financial institutions

Evolution stage	*Risk of compromise (1-10)*	*Effect of compromise*
Managed	3	Minimal interruption

Information security is seen as a mission critical task and aggressively managed and monitored. A core team of specialists have been recruited to the task and are provided with the tools and training to implement effective information security. Training is seen as a key success factor in protecting the organisations information.

A compromise is unlikely and would require advanced skills and would likely result in minimal interruption to the business as the company is familiar with advanced information security techniques such as incident handling and response techniques. The company has a high level of automated prevention, runs manual detection and reaction measures. It is typically an ongoing objective of these organisations to achieve automation of the latter tasks.

People

- Security policies, procedures and standards are documented for both technical staff and business users, these documents are regularly updated and conveyed to users
- Personnel are provided the appropriate training or skills to effectively administer information security

Process

- Advanced security tools are used to protect the networks, staff receive appropriate training to maintain such tools
- A Security function exists and receives support from highest levels of management

Technology

- The IT environment is highly secure and the integrity of the environment is measured and monitored
- The organisation use external resources to aggressively test the network
- Users have confidence that IT resources are secure

Examples of such organisations

- Medium to large organisations (over 1,000 employees)
- Medium to large sized financial institutions

Evolution stage	*Risk of compromise (1-10)*	*Effect of compromise*
Optimising	1	Minimal disruption

An optimised state of evolution is the result of continual development of information security and a comparison of the organisations procedures against peers in forums such as the Information Security Forum (ISF) [4]. Information is championed at board level by an appropriate posting e.g. Chief Information Officer or Chief Privacy Officer. Information Security is seen as critical to the successful operations of the organisations business.

A compromise is unlikely and would require highly advanced skills and is likely to result in minimal disruption to the business as the company employs sophisticated security tools such as Intrusion Detection Systems (IDS) and is familiar with advanced techniques such as incident handling and response. The company has automated its prevention, detection and reaction and is concentrating on honing its preparations on a continuous basis.

People

- Enduser awareness training is seen as a key factor in ensuring information security
- The Security Management function has the appropriate segregation of duties and reports to the appropriate level of management
- Staff awareness programs are used (visual or login banners, email reminders)

Process

- A Security function exists and receives support from highest levels of management
- Security processes and controls are reviewed frequently to identify potential weaknesses and eliminate or reduce them to a manageable level
- The organisation use external resources to aggressively test network defences

Technology

- Security tools are deployed to allow a single point of administration for access to IT resources (e.g. Tivoli Secureway or CA Unicenter)
- The IT environment is highly secure and the environments integrity is measured
- Users have confidence that IT resources are secure

Examples of such organisations

- Organisations whose key asset is information (Communications, Military, Software)
- Large organisations (over 1,000 employees)
- Mature high technology companies

III. Building the trust model and setting the maturity scorecard

The trust model

Once you have defined how the maturity model might apply to your organisation you need to decide the key performance domains against which you will score the organisation. The criteria selected are at your discretion but should include the key components of your organisations trust model.

The best place to start is to build your organisations trust model (see figure II). This segments and appropriates a risk classification to each domain connected in and out of your internal information systems.

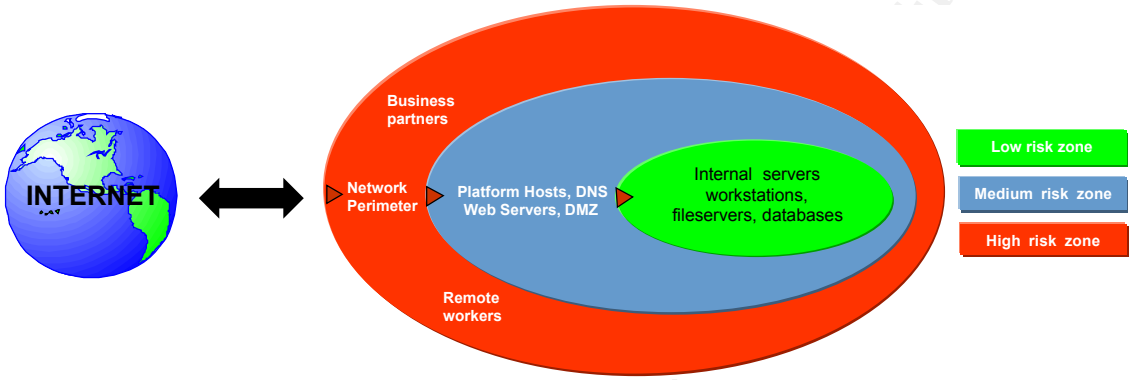

Figure II Example of an information security trust model

The approach works because each of the functional domains are examined in terms of people, process, and technology and are assessed beginning from the infrastructure's outermost perimeter and ending at its most sheltered, the heart of the organisations information systems. Once the organisation has documented the trust model it can then get to work. The best place to start is to break the trust model into three risk areas[1] (high, medium and low) and document the components of each area (see table I).

Red	High – closest connection to the internet resulting in area of least control for the organisation	External routers, Firewalls Remote workers, business partners
Blue	Medium – provides the gateway from the internal gateway and the Internet	External DNS/ LDAP Internal routers, Webservers
Green	Low – the internal network is the core of the organisations information systems	Internal DNS Production/ development servers Workstations/ Internal datastores

[1] Assigning risk ratings to the trust model is quite an emotive and subjective area. The CSI/FBI information security survey estimates that up to and over 80% of compromises can be traced to an internal resource. I have given the internal network a low risk rating, as it is the area over which an organisation should have most control.

Table I Examples of the trust model

Section IV (rolling out the benchmarking process) further explains the specific steps to this process. Once this exercise is completed you must then segregate the elements in specific measurable criteria (called domains). This can be done using the Maturity Scorecard.

The maturity scorecard

The maturity scorecard allows you to visually score and track progress against set criteria (the process maturity level) across a number of domains (see figure III). The approach is derived from the Maturity Model that the Software Engineering Institute defined for the maturity of the software development capability[5] The scorecard allows an organisation to make a business case for IT investment by scoring each element against agreed objectives. The organisation defines the IT management process, in this case information security,

- The current status of the organisation – where the organisation is today
- The current status of (best in class) the industry –the comparison
- The current status of international standards –additional comparison
- The organisations strategy for improvement – where the organisation wants to be and how long it expects to take getting there

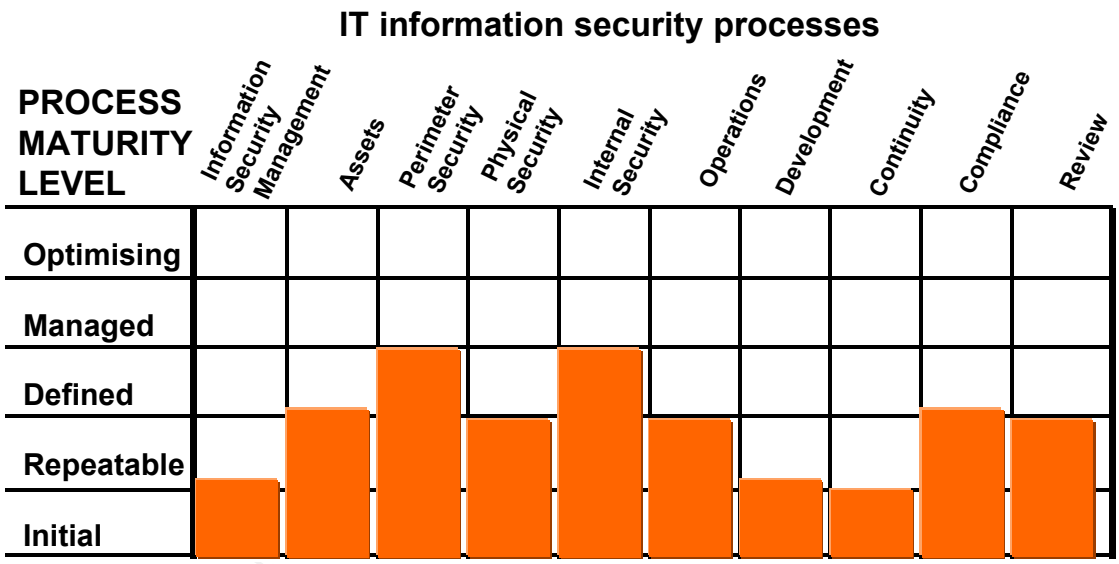

Figure III Example of a maturity scorecard

It is important to remember that information security cannot simply be a fix but a change in the way that you manage the confidentiality and availability of your information. This Maturity model and scorecard has been further developed by a number of parties including Andersen (www.andersen.com) and ISACA[6] for scoring and measuring IT management process performance.

0	Non-existent	Management processes are not applied at all.
1	Initial	Processes are ad-hoc and disorganised.
2	Repeatable	Processes follow a regular pattern, different people manage the same risk in similar ways.
3	Defined	Processes are documented and communicated, but unmeasured.
4	Managed	Processes are monitored and measured and revised relative to success.
5	Optimised	Best practices are followed automated, and aggressively measured against peer and industry groups. The process is seen as a key business objective.

Table 2 Explaining the levels of process maturity

The rational behind selecting the criteria

The organisation decides what domains to benchmark. This is then compared against industry or best practice or simply measured against its own specific requirements or objectives.

Operations	How is information security integrated in day to day operations? What levels of controls (e.g. preventative, detective and reactive), are placed around managing operations? How is the success of these measures monitored and reported
Continuity	Do contingency preparations accommodate security specific tasks such as incident response of forensic procedures? How often are the preparations tested and how are the tests scored and reported?
Review	What level of tools and techniques are used to interrogate and monitor the effectiveness of information security? What is the formal review process around information security? Who is the audience to receive this information? What level of importance is placed on the results?

Table 2 Examples of the rationale determining process maturity

Once the domains are chosen and the objectives set it is time to carry out the initial benchmarking and then set objectives for process improvement.

IV Rolling out the benchmarking process

Rolling out the plans

Once you know the domains to be scored you need to build a realistic and workable plan to both score and measure progress on an ongoing basis. Each of the domains are likely to have an assigned owner e.g. review may be internal audit or physical security handled by facilities management. I recommend the following steps

A good place to start is to build a system documentation file. This documentation would include:

- IT Policies standards and procedures
- IT organisation chart
- Security exception reports
- Network topology
- Application inventory
- Hardware and software register

These documents allow you to build an understanding of the environment and effectively apply the benchmarking process. The steps in the process are

- Interview domain owner to gain a high level view
- Identify key personnel to assist you in building detailed knowledge
- Work with those personnel to build a profile of the domain
- From this profile build and complete a workplan detailing objectives to measure the process maturity

It is likely to take 2-3 focussed days of work to assess each of the maturity scorecard section (ignoring project or scope creep). As there are ten sections, this can result in over 30 mandays of work. It is important that you schedule this time on a full or part time basis and arrange the meetings well in advance.

The work can be done by internal resources or outsourced to a specialist firm (e.g. Big Five consulting firm or boutique security firm). Very often the task is outsourced to prove a point to senior management and provide an independent air over the results. This has many advantages including

- Skill transfer: the ability to leverage off the skills and experience of the external parties
- Project risk: external parties are contracted to deliver specific tasks within a defined period, allowing you to concentrate on your core business
- Independence: eliminating the risk of office politics or personalities clouding the results

But beware, it is important that you tightly define the scope of the work you want carried out and check the credentials and references of any individuals or firms that may be accessing your systems.

The toolkit

In order to carryout the work I also recommend that you build a toolkit to enable you to effectively benchmark the environment around you. The various tools I would recommend include:

Secrets and lies	Provides a realistic and objective overview to information security and related risk management processes.
CERT security modules[7] SANS[8] Bookstore NSA[2] Windows 2000 guides	Documents outlining how to secure systems to a level of best practice.
Solarwinds (www.solarwinds.net)	Provides numerous network auditing tools and utilities.
SANS Incident response and handling guide[10]	Best practice on recovering from a possible compromise.
Nessus (www.nessus.org)	Freeware package for identifying system vulnerabilities.
ISS (www.iss.net)	License based vulnerability scanner.
Microsoft office	For documentation, presentation and planning tools.
Andersen Global Best Practices (www.globalbestpractices.com)	Provides additional best practice guidelines on various business areas.
Business Continuity Management	Explains and provides examples for business continuity management.

Table III Toolkit for benchmarking information security

Be realistic

It is important to be realistic when assessing the level of resources that will be assigned to the task of benchmarking information security within the organisation. The process can be quite time consuming and is highly dependent on the level of accurate documentation. It is vital that you obtain the trust and the buyin of the staff running the systems.

Once the initial benchmark has been carried out and scored agree the results with each domain owner (e.g. IT review owner may be internal audit). It is important to remember that you should stay as independent as possible. If you provide recommendations it is vital that the domain owners take responsibility for them.

Once the initial score has been determined you can then set objectives to improve security across certain domains for example, improve security and continuity while maintaining the review domain. The explicit steps are

1. Agree scores and set forward objectives with domain owners
2. Scope and budget necessary resources
3. Present and agree results with the board or project sponsor
4. Schedule work with domain owners

It is important to work with the organisation as a whole as you are trying to implement a lasting change for information security. Therefore the key things to remember include

DO

- gather as much documentation as possible
- utilise all available tools to automate tasks
- work with the domain resources as they are the experts on the ground
- schedule both your and the domain teams time realistically.

DO NOT

- expect to have all the answers
- step on toes unnecessarily
- arrive at a doorstep unannounced and expect a positive response

The more effective the project management, the more valuable the survey results will be as they will be delivered in a timely manner.

V. Conclusions

It is important to remember that there is no such thing as a secure computer system. If you want 100% security, unplug the computer system. What you can do is manage the risk and minimise to consequence of compromise or incident.

Many organisations address information security by investing in the latest technology and expecting their worries and concerns to disappear. This can lead to a reactive management process that tends to detect problems or issues 'after the fact'. If you try to manage information security on a reactive basis you are likely to get nowhere fast. If you step back and take a holistic approach and set realistic objectives then you have a much greater likelihood of success.

The organisations that are successfully managing the risks to their information security look to get the right mix of

- People who maintain and provide intelligence to the,
- Process that defines the criteria to manages the
- Technology designed to protect your information

This paper should have provided the basis for a sensible approach to building lasting information security by

1. Explaining process maturity and how it relates to information security
2. Providing an approach to building a trust model on which you can identify and stratify key risk areas
3. Setting out the next steps when initiating a benchmarking process
4. Providing useful references to support you on the road to benchmarking and process improvement

It is important to remember that this change in how you benchmark and improve information security will not happen overnight. However over time you will note improvement in time and efficiency when managing the process.

The improvements you gain through process management can then be used to strategically manage your information resources rather than applying the majority of your resources to operational issues and that is where the true value of this exercise will be found.

VI. References

Introduction

This section is structured reference section to act as a bibliography of references made during the paper and more importantly as a guide to aid readers in sourcing information that I have found useful when benchmarking and implementing information security process management.

[1] Schnier, Bruce. “Secrets and Lies”. John Wiley and Sons. ISBN: 0471253111. 1 September 2000. Secrets and Lies is a thorough backgrounder in all aspects of network security, an extremely wide remit that stretches from passwords to encryption, passing through authentication and attack trees along the way. The book is divided in to three broad categories.

The Landscape, which covers attacks, adversaries and the need for security; Technologies, which discusses cryptography, authentication, network security, secure hardware and security tricks; and concludes with Strategies, which looks at vulnerabilities, risk assessment, security policies and the future of security.

[2] The National Security Agency. ”Security Recommendation Guides”. July 2000. www.nsa.gov. The NSA has developed security recommendation guides for Microsoft Windows NT/Windows 2000 and other systems in the form of configuration guides. It also provides an excellent white paper on an approach to a Defence in Depth strategy.

[3] The Information Security and Control Association (ISACA). “COBIT Version 3”. www.isaca.org/cobit. With more than 22,000 members in over 100 countries, the Information Systems Audit and Control Association® (ISACA™) is a recognised global leader in IT governance, control and assurance. Founded in 1969, ISACA sponsors international conferences, administers the globally respected CISA® (Certified Information Systems Auditor™) designation earned by more than 24,000 professionals worldwide, and develops globally-applicable Information Systems (IS) Auditing and Control Standards.

COBIT (Control Objectives for IT) provides the critical insight needed to delineate a clear policy and good practice for IT controls. The guide includes statements of desired results or purposes to be achieved by implementing the 318 specific, detailed control objectives throughout 34 IT processes.

[4] Information Security Forum, www.securityforum.org. The Information Security Forum is an independent, not-for-profit association of the world's leading organisations. The Forum's Information Security Status Survey provides a practical, business-oriented view of information security, assessing performance against best practice.

It offers a unique benchmark by which to measure a company's performance against that of other leading organisations - in specific sectors and in other industries.

[5] Carnegie Mellon University. “Capability Maturity Model [sm] for Software”. Version 1.1. Technical Report CMU/SEI-93-TR-024. Software Engineering Institute. Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The Capability Maturity Model® (CMM®) provides a framework for organising these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement. The five maturity levels define an ordinal scale for measuring the maturity of an organisation’s software process and for evaluating its software process capability. They also help an organisation prioritise its improvement efforts

[7] The Carnegie Mellon Emergency Response Team. “Security Practices & evaluations”. www.cert.org. The CERT/CC is part of the Networked System Survivability (NSS) Program located at the Software Engineering Institute (SEI), a federally funded research and development centre (FFRDC) operated by Carnegie Mellon University (CMU).

The CERT/CC is a major reporting centre for Internet security problems. Staff members provide technical assistance and co-ordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyses product vulnerabilities, publishes technical documents, and presents training courses.

The CERT® Guide to System and Network Security Practices, published by Addison-Wesley and available at walk-in and online bookstores. Using a practical, phased approach, the book shows administrators how to protect systems and networks against malicious and inadvertent compromise based on security incidents reported to the CERT/CC.

[8] The SANS Institute (System Administration, Networking, and Security.1989. www.sans.org. The SANS Institute is a co-operative research and education organisation through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face.

Their publications provide step-by-step guidance based on the consensus and testing of dozens of active practitioners in large and small organisations throughout the world.