Security Principles

Aaldert Hofman & Ben Elsinga
Technology Services
Capgemini Nederland B.V.

Ben.Elsinga@capgemini.nl
Aaldert.Hofman@capgemini.nl

1 INTRODUCTION

Organisations often lack a clear vision on how they should approach security at corporate and enterprise level, based on business drivers and actual context. The underlying problem is that language to express the security on strategy level is missing.

This paper provides terminology to define such a language, by describing a number of security principles. A security principle is defined as a high-level model to reflect an organisations perception of security.

Changes over time within the context of the organisation could change perception towards security. Security principles help organisations to be more agile and adaptive, by applying a ready made of the shelf proven set of principles to manage risks.

We group security principles in a framework of mindset, execution and architecture, including their interrelationships. The paper will also introduce two methods to select the right principles for implementation.

The structure of this paper is:

- Chapter 2 is the kernel of this paper introducing the principles and methods for selection.
- Chapter 3 discusses the methods for selection in more detail.
- Chapters 4, 5 and 6 provide an overview of mindset, architecture and execution principles.

The principles are derived from practical experience. Readers of this paper are invited to contact the authors in case of supplementary security principles.

This paper was issued to EuroPLoP 2003. We would like to thank our EuroPLoP2003 shepherd Andy Longshaw who guided us through several iterations of our submission and provided many constructive comments. At EuroPLoP2003 this paper was discussed in a workshop; comments were valuable and improved this paper considerably.

Also we would like to thank some of our colleagues within Cap Gemini Ernst & Young who provided us with input and reviewed: René Bense, Lex Dunn and Jan-Willem de Vries.

2 SECURITY PRINCIPLES

2.1 Introduction

Organisations often lack a clear vision on how to approach the security challenge on the corporate and enterprise level, based on business drivers and actual context. In order to adjust the level of security to business strategy and image, we need to know how the organisation perceives information security.

The problem is that a common language for expressing and dealing with security on a corporate level, understood by all stakeholders, is missing.

Multiple forces cause miscommunication and misunderstanding in the notion of how to address information security.

- It's only technology. A common misunderstanding (e.g. by board of directors or business managers) is that information security is only about some firewalls, anti-virus software and cryptography. That's not true.

- Diversity in stakeholders. Business managers, IT professionals, auditors, vendors, etc. are very diverse. They all think about the risk the organisation faces, but all within the context of their own profession. Miscommunication is a big risk.

- Different professional languages. Business managers, IT professionals, auditors, etc. all have their own professional language. Usually, these languages are not the same, causing miscommunication and misunderstanding.

This paper provides an introduction to security principles for expressing and dealing with security on a corporate level by providing a framework of terminology, including a method to select the most appropriate security principles to deal with security at corporate level.

Paragraph 2.1 introduces the framework for security principles.
Paragraph 2.2 introduces the methods to select security principles.

2.2 A Framework for Security Principles

A security principle in this context is defined as a high-level model to express the way the organisation thinks about security. Such a high-level model can suit the business model of the organisation, is typically summarized by a short phrase and can be explained and understood by all people (!) involved in the safety and security of the organisation. Some common examples are "Need to Know", "Perimeter Defence" or "Issue driven".

When thinking about these common examples, you'll find that it's not easy to choose. Some principles might be opposites; others might strengthen each other. That's why we thought of a framework for positioning security principles, consisting of:

1. Mindset principles at strategic level: "What is your mindset about security?"
2. Architecture principles at tactical level: "How do you want your defence?"
3. Execution principles at operational level: "How do you want to act?"

Mindset principles are used by the organisation to formulate its security strategy. The context of **architecture** principles is defined by the mindset and finally the context of the **execution** principles is highly dependant on the culture of the organization combined with the **mindset** principles the organisation uses to formulate its security strategy. Because implementing a corporate or enterprise security strategy consistently, requires a lot of change and this is where the human factor plays an important role.

Chapter 4 through 6 introduce all principles from these categories. They all address the same problem: "how to express the way we think about security"; that's why there is no "problem" section included in the principles.

2.3 Selecting the right principles

Selecting the right principle(s) is not easy. Some principles overlap, some are each other's opposite, some use the same words for different subjects; some principles aim at different areas of information security.

We identified two methods to select the right (combination of) principles given a certain context. The first one is based on a best and worst practice approach. The second one is based on an approach that gives organisations the ability to "grow" in security level based on their business requirements. Both methods will be described in chapter 3 in more detail. Even a combination of these methods is possible, although we did not look into that one.

Chapter 3 will guide the reader how to select the right principle.

2.4 Example

A small governmental agency performs an assessment on their security approach and finds they apply "Security as a technical issue", "Risk unawareness" and "Fortress mentality".

Since they want to provide e-government services to their citizens they realise that they will put their mission critical information systems at risk if they do not change their mindset towards security. They decide to apply mindset principles enabling e-government services while operating at an acceptable level of risk.

Instead of applying "Security as a technical issue" principle they shift towards "Security as a business issue" principle. As a consequence security is on the agenda of the management team every month. They will adopt a risk management approach for all new business processes. A project team facilitates this change; line management is responsible for results.

The "Risk unawareness" mindset needs to be changed to the "Manage risk" mindset. It's just not enough to perform a risk assessment for new business processes only. Because the governmental agency is small they want to use a practical approach. First of all, an awareness programme is launched for all employees including management. Secondly all vital information systems are analysed using an interactive approach, stimulating awareness as well. The risk assessments lead to an improvement plan where the management team has to decide upon.

The “Fortress mentality” mindset is hard to deal with because it has to do with the perception of people and the architecture of the infrastructure. As a first step they decide to review all current preventive security measures and brainstorm how preventive security measures can be complemented with adequate detection and response. On the medium term the governmental agency will start an architecture project to design and implement a number of security domains in the IT infrastructure itself.

2.5 Consequences of using principles

Benefits:

- Well-named principles are almost self-explaining and might even replace existing policies and documents.
- Paradigms provide a very powerful mechanism to formulate a security strategy and communicate this strategy to a broad audience.
- Paradigms can be combined into scenarios, which makes it easier for the organization to make a roadmap and evaluate possible options on forehand.
- All principles can be related to lower level security principle, which enable sharing of best practices and continuous improvement.

Pitfalls:

- Like all other security solutions, the security principle language is no silver bullet.
- Because not all security principles are documented in full detail and related to lower level security principle, for the time being creativity and expert information is needed to implement security principles at the working level.

3 FINDING THE RIGHT SECURITY PRINCIPLES

3.1 Selecting principles based on opposites

We start with a simple approach to select principles to improve the corporate security level.

1. Read the solutions of the principles and mark all principles that are used by the organisation you're dealing with.
2. Then walk the tables for ***Mindset*** principles and ***Execution*** principles in upcoming paragraphs and look if you can find marked principles (from step 1) that are actually bad practices. Note that we could not identify bad practice ***Architecture*** principles, therefore only the ***Architecture*** principles themselves are listed.
3. For all bad practices consider selecting the opposite principle.
4. Prioritize selected principles and plan to implement them.
5. Obtain senior management commitment to execute the plan accordingly.

Note that it does not make sense to select and implement all the principles listed in the table during first implementation. It is much better to start with the three most important mindset principles and the two most important execution principles. Also note that changing mindset of people takes time. The simpler the message the more chance to succeed.

3.1.1 Mindset principles

We identified 27 different ***Mindset*** principles, listed in terms of best practices and bad practices:

Best practice	Bad practice
Security as a business issue	Security as a technical issue
Need to protect Need to know	Uncontrolled access
Manage risk	Risk unawareness Risk avoidance
End to end security Entity to entity security	Point solutions
Obey the law	Violate the law
Safety before security	Safety unawareness
Keep it open	Security by obscurity
Keep it simple	Make it complex
Fail securely	Trust your security
Security goals before means	Trust your vendor
Time Based Security	Fortress mentality
Trust nobody	Trust your employees

Although we know that the world is not simply black or white, we deliberately choose to present the principles as either good or bad, just to position them as clearly as possible. Probably you can think of specific situations where good practices turned out bad or where bad practices turned out to be good after all. That's life.

3.1.2 Architecture principles

We identified 10 ***Architecture*** principles, but did not find bad practices. We still wonder why it is easy to identify bad practices for Mindset and Execution principles, but not for ***Architecture*** principles. Perhaps ***Architecture*** principles have already been through an implicit selection process before they are described and published.

Best practice
Security guard
Perimeter defence
Divide and conquer
The network as a battleground
Peace or war
Immune system
Layered security
Defence in depth
Watch the Watchers
Enlist the Users

3.1.3 Execution principles

We identified 14 ***Execution*** principles, listed in terms of good and bad practices:

Good practice	Bad practice
Return on investment	Security at any price
Security in every change	Security as a desert
Proactive governance	Ignore security patches
Mature through time	Wait for the auditor
Issue driven	Top down approach only
Just do it together	Paralysis by analysis
Respond on security incidents	Ignore security incidents

3.2 Selecting principles based on maturity levels

A more advanced approach is to introduce four categories of principles that can be applied as a group based on the maturity level of the organization. The four maturity levels are:

- IT centric, but ad-hoc
- IT centric and “in control”
- Business aligned and “in control”
- Ecosystem integrated and agile

Most practical is to have a workshop with senior management to determine the level they want to implement within three years. Another important stake in the ground is the level of departure. If senior management wants to make more steps in the coming three years, make sure that you plan the arrival of the intermediate maturity levels as well.

3.2.1 Generally good and bad security principles

We consider these principles as generally good, despite the level of maturity.

Principle type	Principle name
Mindset	Obey the law
Mindset	Safety before security
Mindset	Keep it open
Mindset	Keep it simple
Mindset	Trust nobody
Architecture	Perimeter defence
Execution	Proactive governance
Execution	Just do it together
Execution	Respond on security incidents

Likewise, we consider these principles as generally bad, despite the level of maturity.

Principle type	Bad practice name
Mindset	Risk avoidance
Mindset	Violate the law
Mindset	Safety unawareness
Mindset	Security by obscurity
Mindset	Make it complex
Mindset	Trust your security
Mindset	Trust your employees
Execution	Security at any price
Execution	Ignore security patches
Execution	Top down approach only
Execution	Paralysis by analysis
Execution	Ignore security incidents

3.2.2 IT centric ad-hoc (anti) principles

At the IT centric ad-hoc maturity level, security is viewed as a technical issue only and security is solved on an ad-hoc basis without managed change processes or an overall security vision or plan. You will probably not be surprised that at this level a lot of bad practices are applied. Security principle bad practices applied at this level are:

Principle type	Bad practice name
Mindset	Security as a technical issue
Mindset	Uncontrolled access
Mindset	Risk unawareness
Mindset	Point solutions
Mindset	Trust your vendor
Mindset	Fortress mentality
Execution	Security as a desert
Execution	Wait for the auditor

3.2.3 IT centric and "in control" principles

At IT centric and "in control" maturity level, security is viewed as a technical issue but there are formal change processes and a structured process is in place to manage security. Although mindset at this level is very technology oriented, technical risks are managed. Security principles applied at this level are:

Principle type	Principle name
Mindset	Need to know
Mindset	Manage risk
Mindset	End to end security
Mindset	Time Based Security
Architecture	Layered security
Architecture	Enlist the Users
Execution	Security in every change
Execution	Mature through time
Execution	Issue driven

3.2.4 Business aligned and "in control" principles

At business aligned and "in control" maturity level, security is viewed as a business issue. Security is really an issue within the boardroom. The level of security is of strategic importance for the organization and is also broadly perceived this way. There are formal change processes in place and a security organization to manage security. Business requirements drive security requirements, not the other way around. Security principles applied at this level are:

Principle type	Principle name
Mindset	Security as a business issue
Mindset	Need to protect
Mindset	Manage risk
Mindset	End to end security
Mindset	Fail securely
Mindset	Security goals before means
Mindset	Time Based Security
Architecture	Security guard
Architecture	Divide and conquer
Architecture	Layered security
Architecture	Defence in depth
Architecture	Watch the Watchers
Architecture	Enlist the Users
Execution	Return on investment
Execution	Security in every change
Execution	Mature through time
Execution	Issue driven

3.2.5 Ecosystem integrated and agile principles

At ecosystem integrated and agile maturity level, security is viewed as a business issue and at the same time business is highly dependent on co-operation with business partners. So a network of organizations has to work together to provide added value to the customer. Continuity problems and leakage of confidential information within one organization will have a negative effect on all the organizations that profit from the value chain.

Because of the amount of electronic interaction of the target organization with a lot of other organizations, security needs to be agile as well. It must be easy to adopt and differentiate the security level based on the characteristics of the communication partners. Risks are eminent but the target organizations have a lot of mechanisms in place to control security incidents of different sorts and severity in near real time.

Business requirements of the entire value chain drive security requirements. Being highly adaptive is just a way to survive in turbulent business environments and networked economies like we see today.

Security principle practices applied at this level are:

Principle type	Principle name
Mindset	Security as a business issue
Mindset	Need to protect
Mindset	Manage risk
Mindset	Entity to entity security
Mindset	Fail securely
Mindset	Security goals before means
Mindset	Time Based Security
Architecture	Security guard
Architecture	Divide and conquer
Architecture	The network as a battleground
Architecture	Peace or war
Architecture	Immune system
Architecture	Layered security
Architecture	Defence in depth
Architecture	Watch the Watchers
Architecture	Enlist the Users
Execution	Return on investment
Execution	Security in every change
Execution	Mature through time
Execution	Issue driven

4 INTRODUCING MINDSET PRINCIPLES

Embedding security in an organization can be done in many ways. Whether or not this is successful, depends on non-technical aspects like the type of organisation, the environment, regulations, the type of business, the maturity of the management functions and business processes and maturity of IT processes. Besides this, human and cultural aspects are very important as well.

This wide range of factors makes it sensible to document how you perceive security to create a clear and uniform starting point in embedding security in the organization. Mindset principles can be used to build a corporate security strategy, building perception on security.

This chapter introduces a collection of mindset principles.

4.1 Security is a business issue

In the mindset of general management security is perceived as an enabler for new business and/or improved business processes. Business processes can easily cross boundaries of organizations towards customers, partners and citizens. Security is on the agenda of the management team. The team is committed to keep the level of security in balance with the actual level of threats to business processes. Security is an important subject in every business contact of the organisation. For every new business initiative a (smart) risk analysis is performed to make sure that risks are managed from the business perspective. Security isn't about risk avoidance; it's about risk management.

4.2 Security is a technical issue

In the mindset of general management security is perceived as a pure technical issue. A technical problem needs to be resolved with technology; the IT department is the main source of action. Security is not on the agenda of the general management team and business requirements are weak. IT management owns the problem; the IT department knows everything about technical issues. Of course, they're the one to blame when incidents occur. Their challenge is to protect with technical means a 100 percent security. Projects tend to delay because security is a bottleneck and have to be sorted out thoroughly. Business people wonder why security hampers new business activities.

4.3 Need to protect

The organisation performs a corporate risk assessment to determine which information assets are very important for the organization or its stakeholders. This analysis will also supply the information why certain information assets are important. Quality aspects determined are: *Confidentiality*, *Integrity* and *Availability*. When the risk threshold set by the business owner is exceeded, the asset will be protected accordingly. The stance of this principle is: Everything is permitted unless explicitly forbidden.

4.4 Need to know

A person only gets privilege to use a particular information asset if there is really a business need for it, e.g. the person really needs the information asset to do the job. The rationale is that if people can access more information assets than they need to fulfil their job, the risk of security incidents will increase. Authorisation processes are strict, formal and highly granular. Role based access is used to enlighten the governance burden. The stance of this principle is: Nothing is permitted unless explicitly granted.

4.5 Uncontrolled access

There are no formal procedures for authorisation management. It is not clear which persons in the organisation are authorising other persons. There is a lot of trust within the organization that nobody will misuse their rights. The culture is open, nobody has a problem with the fact that information is widely shared. Efficiency and simplicity in doing the job is more important than security. Management is not committed to information security at all.

4.6 Manage risk

Risk is the item that needs to be managed. The organisation wants to be "in control". People and organisational units are appraised on how they are able to manage risk. If an organisational unit believe it is "in control", then the evidence for that needs to be delivered as well. Costs for security need to be balanced against the benefits. Risk is not something to be afraid of, as long this risk is identified, analysed and managed. Incidents are carefully analysed to make sure that risk models are accurate enough. Information assets are protected according to the value for the business of the organisation.

4.7 Risk avoidance

Risk is something to be afraid of. If something goes wrong then the major question is: "Who gets the blame?" People need to be near 100 percent sure that an initiative does not give problems before a product of service will be released. 100% security doesn't exist. 100%-delta does. The art of information security is to make this delta as close to the real need as possible with a cost in proportion to the damage that would be caused to the business if these security measures weren't taken at all.

If the cost of near 100 percent risk avoidance is higher than the benefits than we simply delay, cancel the project or ask for more budgets. People who can convince others that there is still a security hole in the product are rewarded. If you think that things might work then you are in danger. Reviews are very formal, quality is far more important than time.

4.8 Risk unawareness

People are not aware that identifying and managing risk, can be a valuable instrument for a cost effective security level. Also the threats that are inherent to information systems and network infrastructures are not or not fully understood. If an incident really becomes a disaster, the organization is not prepared for it. Information security is not on the agenda of senior management. Computers never make errors and it will stay this way. Computer literacy is not very high: people are happy if they can get along with their computer.

4.9 Entity to entity security

Instead of trust between machines (end-to-end security) there must be trust between the business actors themselves. Let's say the people behind the machines. Entity-to-entity security can build on end-to-end security, but it's more than that. Creating trust between people is a hard job; losing trust can easily be done. Non-technical aspects play a role here like among others, the type of business relationship, the way incidents are detected and handled, positive public relations, open communications and management commitment to maintain the trust relationship.

4.10 End to end security

The complete chain from initiating machine, through different network components until the machine that serves the request needs to be secure. All links of the chain need to be strong enough. Quality attributes like confidentiality, integrity, availability and auditability are designed and implemented and must be delivered by the entire chain. Based on the end-to-end characteristics, the quality attributes of the intermediate components are derived. If multiple organisations are responsible for part of the infrastructure than then derived end-to-end characteristics will be part of the service level agreements and agreed security measures.

4.11 Point solutions

If there is a security problem, the organization will buy a product to solve the problem. There is no complete overview of the overall security solution, e.g. ICT architecture. If a product does not fulfil the requirements, the organization buys a new one. There is a large variety of security products overlapping in functionality, there are some security vulnerabilities, it is hard to integrate systems because security solutions are not interoperable. Governance needs to be performed on a per product basis. There is no corporate management framework where security products can be managed centrally. Synergy is not the issue. The organisation has a lot of budget holders who can buy the security product they like at that moment.

4.12 Obey the law

The organisation makes sure that the laws of the countries where the organisation needs to comply to are implemented. Not obeying to the law would impose too much risk regarding the corporate image. Also the trust of the stakeholders into the organization would vanish if rules were not obeyed. Every initiative or project is double checked against the law. The organization has a strong legal department and internal auditing department to make sure that laws are implemented properly. External and specialized advice is requested as well.

4.13 Violate the law

Drivers to obey the law are missing for a number of reasons. People are not familiar with law in details or don't give priority because law will not be enforced. Computer law is too complicated or organizations are willing to pay the penalty if they are caught. The chance of being caught times the penalty is much lower than the business benefits of not obeying the law. The organization can also be under high pressure, there is no time, money or resources to obey the law. If the organization is caught it will not really hurt the corporate image. Everybody drives too fast with their cars so why comply with computer laws. Rationale of the law is not understood or recognized.

4.14 Safety before security

The organization gives more priority to the security of life-critical systems than the security of non life-critical systems. Life-critical systems are subject to a thorough security, statistical analysis, reviews and formal evaluation. Infrastructure of life-critical systems is preferably separated from non life-critical systems infrastructure, although there's pressure to combine them for the sake of cost reduction, minimization of governance and user convenience.

4.15 Safety unawareness

People are unaware that safety critical information systems need a higher security level than security critical systems. Networks and information systems are shared between them. If somebody is injured or dead because of an incident, everybody is amazed and is wondering how this could ever happen or think, "This is really bad luck".

4.16 Keep it open

Everyone interested can learn the security solution, well understood and verified by a lot of people. Strength is determined by the secrecy of the key(s). The key length will be long enough to prevent brute force attacks together with additional security measures to keep the key(s) secret. The problem is to keep the key secret.

4.17 Security by obscurity

The strength of the security solution is completely based on the fact that only very few people know what the security solution is. There is no way for other people to review the security solution because it is hidden. The proof of the pudding is in the eating, so real world will determine how strong the solution is.

4.18 Keep it simple

Embrace Simplicity. Keep things as simple as absolutely possible. Security is a chain; the weakest link breaks it. Simplicity means fewer links. Complexity is the enemy of security.

4.19 Make it complex

The security solution is more complex than necessary in the hope that an attacker will have more problems attacking a complex solution than a simple one.

4.20 Fail securely

Everything that can fail will fail; the only question is when the security solution fails. In case of failure the solution will still have a set of predefined security characteristics even when the primary security defence will fail. The solution will detect when primary protection fails and will transfer to the secondary security protection and/or risk avoidance scenario.

4.21 Trust your security

People think that the security solution is bullet proof. Nobody is considering the situation that the security solution might fail. Failing security will result in business discontinuity in most cases. There is a larger emphasis on preventive security measures. Detection, repression, correction and evaluation are not developed very well. Multiple security defences are not applied. The first defence is perceived as being strong enough.

4.22 Security goals before means

The organization sets clear business goals and derives the end-to-end security characteristics from them. Additional risk analysis will give the input for a logical security solution. Security services required can still be easily correlated to business requirements. Only if the logical security solution is clear and well understood by business people, the organisation looks for products that can be used to implement the logical security solution. The security product is explicitly evaluated against the well-understood security requirements. The logical security solution (e.g. architecture) is the stable factor through time.

4.23 Trust your vendor

If the vendor of a security product claims the product is secure enough then the organization will use the product. There is no need to obtain security requirements or perform risk analysis because the vendor of the security solution can be trusted. The vendor is dominant and knows what is good for the organisation. Security is a technical problem that can be solved by the right product of a trusted vendor. Note that this solution can be found in day-to-day life.

4.24 Time based security

The organization is aware that security measures will fail. They only question is when. If the attacker (internal and external) has enough time and resources, the attacker will break the first security defence. The only thing the organization can do is delaying a successful attempt to break the security. This is why the organisation applies detection mechanisms to know when the attack starts. Time to detect and react should be smaller that the time the attacker needs for a successful attack.

4.25 Fortress mentality

Security measures are mainly concentrated towards the boundary of the organization. The outside world is the cause of all security incidents. All the internal employees can be trusted for 100 percent. There is no need to enhance the security level within the organisation because the security fence towards the outside world will handle all possible attacks now and in the future. Interactivity with the outside world is minimised to avoid risk.

4.26 Trust nobody

Nobody can be trusted. Loyal employees cannot be trusted if the reward for fraud is high and change of being detected is low. The organization does not want to bring their employees into temptation. Four eye principles are applied for critical transactions. The internal security is as high as the security towards the outside world. There is a strong focus towards compliance, formal procedures and internal control. Detection, response mechanisms and disciplinary actions are applied to make fraud unattractive.

4.27 Trust your employees

Employees might be screened before contracted. Then they will be trusted for life. There is no need to reduce risks that are related to internal employees. Employees are more loyal to the organisation they work for than towards themselves. A lot of organisations have built their security on this principle. Note that this solution can be found in day-to-day life. The principle writers do not want to suggest that this principle is the first option to think of.

5 INTRODUCING ARCHITECTURE PRINCIPLES

Selecting and setting a proper mindset is a good start, but you need more to implement security throughout your complete IT infrastructure. You need some guiding principles on whether or not to implement security controls, how, where and when to implement them. Architecture principles help you to express how security should be embedded in your IT.

This chapter introduces architecture principles.

5.1 Security guard

The security guard centrally screens requests for business services. The guard has the intelligence to detect malicious requests. If the guard authorises the request it can be trusted. The guard will implement the security policy; the rest of the business logic can be simple and does not need to handle security exceptions.

5.2 Perimeter defence

A special security zone is applied to protect the inside from the outside. The idea is that the bad-guys are outside and the good-guys are on the inside. A perimeter defence consists of a number of components depending on its design. Firewalls are used to control the traffic from and to the perimeter defence. If a perimeter defence is the main security protection then it's like building a fortress, hard from the outside and soft from the inside.

5.3 Divide and conquer

The corporate security problem is divided into a number of smaller ones by introducing the concept of security domain. A security domain can be based on a number of criteria like platforms, organisation boundary, geographic location, etc. Security domains can be nested and every security domain has its own specific security policy and derived procedures. If a domain does not have its own security policy the security policy of the next higher-level domain will be applied. Interactions between security domains are subject to so called window policies and derived procedures.

5.4 The network as a battleground

The network is viewed as a military arena. Military concepts are applied to protect the information assets, like "defence in depth", "early warning", "deception" and "stealth" techniques. Also fighting back is one of the options. A response team leader uses the network diagram the same way as generals use their maps of a terrain during a campaign.

5.5 Peace or war

The security policy of the organisation is not static but state full. If there is peace the policy for "business as usual" is applied and enforced. In case of an emergency the organisation "switches" to a higher state of alert with a stricter security policy. Defending the organisation has priority over a fast business response.

5.6 Immune system

The organization is protected the same way a human body protects itself against diseases. The protection system evolves as the time progresses. Feedback, detection and (formal) evaluations are used to improve the protection system.

5.7 Layered security

The security solution is build up by applying a number of layers of protection and/or abstraction. In this way the attacker has to break through a number of protection layers and at the same time the layers themselves can be relatively modular and simple.

5.8 Defence in depth

The security solution is build up by applying a number of layers of protecting. Essential with the defence in depth is that security mechanisms are protected by other security mechanisms. The defence in depth principle can be an extension of the time based security principle.

5.9 Watch the Watchers

Audit your own processes regularly. Guard the guards and double check security measures taken in the past on effectiveness and boldness. Watch the watchers can be viewed as an extension to the “trust nobody” mindset principle.

5.10 Enlist the Users

Security can't work if the users aren't on your side. Social engineering attacks are often the most damaging of any attack, and can only be defended against with user education. So security awareness training programs are very important weapons on the security battleground. Users are asked to report security incidents and weaknesses immediately. The users are the (human) sensors of the protection system.

6 INTRODUCING EXECUTION PRINCIPLES

After setting mindset and architecture perception, there's still an important issue left: day to day usage of your IT requires guidance on how to handle security at execution time. Apart from this, execution principles are quite interesting because they show how transformation of security level will look like.

This chapter introduces Execution principles.

6.1 Return on investment

Every security solution requires economic justification. Risk analysis techniques are used to calculate "cost" of the solution versus "value" of the security solution. The organisation correlates the set of security measures with the business processes that are enabled. The cost and benefits of security measures are well understood.

6.2 Security at any price

Security is viewed as a binary concept. It's secure or not secure at all. It might be that impact of compromised security is simply too high, if the organisation is non-commercial and there is no need for economic justification. In case of safety critical systems it is even impossible or not ethical to calculate economic justification.

6.3 Security in every change

Most effective moment to incorporate security is at the moment the asset is "born". It is like implanting the right DNA when a cell is created. It is easier and more cost effective to change or create information assets the right way from the start than afterwards. Security is integrated in change procedures and project management methodologies. Risk analyses techniques are used to determine the right level of protection, aligned with business needs. Security requirements can even influence important design considerations.

6.4 Security as a desert

Information assets and business processes are created based on required functionality. There is no attention for security during creation or change of information asset or business process. Perception is that security can be bolded on the solution if really necessary. It's more like hiring more agents as soon as people feel that the situation becomes unsafe.

6.5 Proactive governance

There are special governance processes in place to make sure that security patches issued by solution providers are installed as soon as possible. Security is viewed as an important aspect to ensure business continuity on the medium term.

6.6 Ignore security patches

Security patches issued by solution providers are installed late or not at all. Short-term business continuity is much more important than actual security level. Patching security has no priority. Business managers are unaware that security patches should get priority.

6.7 Mature through time

The organisation proactively seeks ways to improve its security in a fundamental way. Maturity models are used to identify current level of security; targets for future security levels are set and agreed. There is formal planning, execution and reviewing process to make sure the new security level is reached. Security is seen as a subject with multiple comfort levels.

6.8 Wait for the auditor

The organisation uses an auditing process to improve its security if needed. Security measures are implemented afterwards if they are implemented at all. There is no real attention to security during change processes.

6.9 Issue driven

The organisation recognizes that securing everything is not feasible. Resources need to be used most effectively. Differences between “As Is” and “To Be” are seen as a security issue and prioritised and clustered based on risk management techniques. The most important and/or the easiest to solve issues get highest priority.

6.10 Top Down Approach Only

Security is improved exactly according to the book. A corporate security policy is signed off. Security baselines are written and enforced. Every system is subject to risk analysis. Security controls resulting from risk analysis are incorporated in a security plan. The plan is executed and controls are implemented. In the end the auditor audits the results of the process.

6.11 Just do it together

The organisation follows top down, but recognizes that this requires too much time and money. Awareness is an issue and security controls can’t be implemented all at once. A more practical approach is taken. A security baseline is implemented and analysis is performed on critical information systems. Workshops are used to mobilize people, make them aware and speed up the process. Twenty percent of the time results in 80 percent of security controls.

6.12 Paralysis by analysis

Thinking about security is much more important than really making things more secure. People spend so much time and money analysing threats and designing security. There is no time or money to implement the solution. When finally a control is realised, the world has changed and the solution is outdated. Security is an intellectual challenge.

6.13 Respond on security incidents

Security incidents are pro-actively detected, administered and managed. For the organisation security incidents are an important feedback on how good the organisation is protected. Security incidents are evaluated and are an opportunity for improvement.

6.14 Ignore security incidents

Security incidents are not pro-actively detected, administered and managed. Incidents are things people do not like to talk about or remember. Success is what counts. Incidents mean trouble that should be ignored as soon as possible.