

Security Paradigm Pattern Language
Ben Elsinga, Aaldert Hofman
Technology Consulting
Cap Gemini Ernst & Young Nederland B.V.

Ben.Elsinga@cgev.nl
Aaldert.Hofman@cgev.nl

1 INTRODUCTION

In EuroPLoP 2003 we request review for only a part of this document: see section 1.3.

1.1 Intent

This pattern language describes a number of so called security paradigm patterns. A security paradigm in this context is defined as a high-level model to express the way the organisation thinks about security.

Changes over time in the context of an organisation could change the way the organisation thinks about security. Security paradigms help organisations to be more agile and adaptive, by applying a ready made of the shelf proven set of patterns to manage risks.

Note that there is a strong relationship between security paradigms and security metaphors also introduced at Europlp 2003. Security metaphors are used to create, define and explain security paradigms. Security paradigms are used to express the security strategy and make essential choices clear. Which means that a typical problem in cyberspace can be handled via the similar security challenges in the physical world. A firewall is a gate (with a guard and nasty dog) in a fence is a good example.

1.2 Motivation

Organisations often lack a clear vision on how to approach the security challenge at the corporate and enterprise level, based on business drivers and the actual context. The real problem is that the language to express the security on strategy level is missing. This paper provides this language.

1.3 Patterns introduced in this paper

This paper defines a large number of security paradigms grouped in a framework of mindset, execution and architecture paradigms, including their interrelationships. The paper will also introduce two methods to select the right paradigms for implementation.

The structure of this paper is:

- Chapter 2 is the kernel of this paper, following the general template of patterns and introducing the framework and methods for selection.

- Chapter 3 discusses the methods for selection in more detail.
- Chapter 4 provides a preview on actual paradigms: Mindset Paradigms.
- Chapter 5 provides a preview on actual paradigms: Architecture Paradigms.
- Chapter 6 provides a preview on actual paradigms: Execution Paradigms.

At EuroPLoP 2003 we request review of chapter 1, 2 and 3 (10 – 15 pages). We included chapter 4, 5 and 6 to provide you with some idea what we're talking about. These chapters are not for review yet.

1.4 Future work

As you might have guessed by now, there is still a lot to do.

First of all, EuroPLoP 2003 will review the foundation of this paper on paradigms. Hence, the result of the workshop is of uttermost importance for future work.

Then, all paradigms introduced in chapter 4, 5 and 6 will have to be documented as proper patterns. Obviously, this is quite an effort. However, we're still convinced that we can finish this within a reasonable period of time.

Another major effort is to relate the paradigms to the existing security pattern landscape as introduced in EuroPLoP 2002 and to be elaborated on in EuroPLoP 2003.

1.5 Acknowledgements

We would like to thank our EuroPLoP2003 shepherd Andy Longshaw who guided us through several iterations of our submission and provided many constructive comments. Thanks to Andy the structure of the paper improved quite a lot. As a reader you owe him thanks too, since the number of pages to review dropped drastically as well.

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 PARADIGM PATTERNS

2.1 Context

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

2.2 Problem

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

2.3 Forces

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.

2.4 Solution

This paper provides a common language for expressing and dealing with security on a corporate level by providing a framework for security paradigms, including a method to select the most appropriate security paradigms to deal with security at corporate level.

Paragraph 2.4.1 introduces the framework for security paradigms.

Paragraph 2.4.2 introduces the methods to select security paradigms.

2.4.1 A Framework for Security Paradigms

A security paradigm 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 paradigms might be contra dictionary; others might strengthen each other. That’s why we thought of a framework for positioning security paradigms, consisting of:

1. Mindset paradigms, strategic level: “What is your mindset about security?”
2. Architecture paradigms, tactical level: “How do you want your defence?”
3. Execution paradigms, operational level: “How do you want to act?”

Mindset paradigms are used by the organisation to formulate its security strategy. The context of **architecture** paradigms is defined by the mindset and finally the context of the **execution** paradigms is highly dependant on the culture of the organization combined with the **mindset** paradigms 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 explain all paradigms in these 3 categories briefly in terms of solutions and consequences. 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 paradigms.

2.4.2 Select the right paradigms from the framework

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

We identified two methods to select the right (combination of) paradigms given a certain context. The first one is based on a pattern and anti-pattern 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 paradigm pattern for implementation into their organisation.

2.5 Example

A small governmental agency performs an assessment on their security approach and find 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 paradigm patterns enabling e-government services while operating at an acceptable level of risk.

Instead of applying “Security as a technical issue” paradigm they shift towards “Security as a business issue” paradigm. 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, 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 a hard nut to crack because it has to do with the perception of people and the architecture of the infrastructure. The project team reads the book “Time Based Security” written by Winn Schwartau, to become familiar with the concepts. 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 medium term the governmental agency will start an architecture project to design and implement a number of security domains in the IT infrastructure itself.

2.6 Consequences

Benefits:

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

Pitfalls:

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

2.7 Implementation Issues

Although a paradigm approach will speed up analysis and helps to create a vision on how to proceed, management of the organization needs to be aware of the insecurity and willing to take action.

2.8 Related Patterns

Taxonomy	Security Taxonomy Pattern Language by Ben Elsinga and Aaldert Hofman. Submitted to EuroPLoP 2003.
Metaphor	Security Metaphor Pattern Language by Ben Elsinga and Aaldert Hofman. Submitted to EuroPLoP 2003.

References to other security patterns need to be done.

2.9 Known Uses

- The authors of this paper use security paradigms to lecture information security in practice

2.10 References

To be done.

3 FINDING THE RIGHT SECURITY PARADIGMS

3.1 Selecting paradigm patterns based on opposites

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

1. Read the solutions of the paradigm patterns and mark all paradigms that are used by the organisation you're dealing with.
2. Then walk the tables for *Mindset* paradigms and *Execution* paradigms in upcoming paragraphs and look if you can find marked paradigms (from step 1) that are actually anti-patterns. Note that we could not identify anti-pattern *Architecture* paradigms, therefore only the *Architecture* paradigms themselves are listed.
3. For all anti-patterns consider selecting the opposite pattern based on the consequences section of both the anti-pattern and it's opposite pattern.
4. Prioritize selected paradigm patterns 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 patterns listed in the table during the first implementation step, it is much better to start with the three most important mindset paradigm patterns and the two most important execution patterns to start with. Also note that changing the mindsets of people take some time. So the simpler the message the more chance to succeed.

3.1.1 Mindset paradigms patterns and anti-patterns

We identified 27 different *Mindset* paradigms, listed in terms of patterns and anti-patterns:

Pattern name	Anti-pattern name
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

3.1.2 Architecture paradigm patterns

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

Pattern name
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 paradigm patterns and anti-patterns

We identified 14 *Execution* paradigms, listed in terms of patterns and anti-patterns:

Pattern name	Anti-pattern name
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
Just do it together	Paralysis by analysis
Respond on security incidents	Ignore security incidents

3.2 Selecting paradigm patterns based on maturity levels

First of all there is some basic level of paradigms that are generally good and generally bad. These can be viewed as guiding principles irrespective of the context of the organisation.

On top of the basic level we introduce four categories of paradigms that can be applied as a group based on the maturity level of the organization. The four maturity levels are:

- IT centric 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 security paradigm patterns

We consider these paradigms patterns as generally good practice.

Pattern type	Pattern 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

3.2.2 Generally bad security paradigm anti-patterns

We consider these paradigms patterns as generally bad practice.

Pattern type	Anti-pattern 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
Execution	Paralysis by analysis
Execution	Ignore security incidents

3.2.3 Level 1: IT centric ad-hoc paradigm (anti) patterns

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 anti-patterns are applied. In CMM terminology the level can be called “ad-hoc” or “repeatable” without business alignment.

Security paradigm anti-patterns applied at this level are:

Pattern type	Anti-pattern 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

3.2.4 Level 2: IT centric and “in control” paradigm patterns

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. In CMM terminology the level can be called “defined” or “managed” without business alignment.

Security paradigm patterns applied at this level are:

Pattern type	Pattern 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

3.2.5 Level 3: Business aligned and “in control” paradigm patterns

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. In CMM terminology the level can be called “managed” or “optimising” including a clear business alignment. So business requirements drive security requirements, not the other way around.

Security paradigm patterns applied at this level are:

Pattern type	Pattern 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

3.2.6 Level 4: Ecosystem integrated and agile paradigm patterns

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.

In CMM terminology the level can be called “optimising” or beyond including a clear business alignment with the business partners. So business requirements of the entire value network drive security requirements. Being highly adaptive is just a way to survive in turbulent business environments and networked economies like we see today.

Security paradigm anti-patterns applied at this level are:

Pattern type	Pattern 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 PREVIEW ON MINDSET PARADIGM PATTERNS

4.1 Introducing Mindset Paradigms

Mindset paradigm patterns can be used to build corporate security strategy. Security strategies are composed of a combination of security paradigms, selected on specific context.

The success of the application of a particular security strategy is highly dependant 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, especially the maturity of the ICT processes. Human and cultural aspects are very important as well. This is why it makes sense to document and exchange security paradigms in a design pattern format and to save valuable time to implement the right security measures needed in the ever-changing business processes.

Mindset paradigm patterns are interesting since they all address exactly the same problem:

What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards?

So, if all mindset paradigm patterns address the same problem, where's the difference? Well, they differ in context. The context of the organisation, described in dimensions connectivity, volatility, trustworthiness, determines the solution: the choice of the paradigm. In the next paragraph the three dimensions of the context of mindset paradigms are further defined.

4.2 The context of mindset paradigms

Note that some mindset paradigm patterns share exactly the same context. Some of them are in this case patterns (best-practices) and some of them are anti-patterns (bad practices). The reader should in this case carefully read the consequences of the pattern to decide which pattern to select and which to reject. The readers experienced in the field of security will probably notice that the anti-patterns (bad practices) are currently the most "successful" paradigm patterns. We recognized this problem; this is why patterns (best-practices) and anti-patterns (bad practices) are documented in the same pattern language.

4.2.1 Connectivity

Value	Explanation
Highly connected	There is a number of strongly coupled electronic connections to the outside world, including formal information exchanges, like XML messages, EDI transactions, business transactions, an interactive web-site, etc.
Connected	There are a number of loosely coupled electronic connections to the outside world, e.g. informal systems like, e-mail, document exchange, a passive web-site, etc.
Isolated	No or only a few electronic connections to the outside world.
No differentiator	Connectivity is no major differentiator for the selection of this mindset paradigm.

4.2.2 Volatility

Value	Explanation
Highly volatile	The business environment of the organisation changes very rapidly with an every increasing speed. Changes themselves are unpredictable; the organisation is confronted with permanent change.
Volatile	The environment of the organisation changes rapidly but with a predictable speed and rhythm. Between the moments of change there are some periods of stability.
Static world	The environment of the organisation changes very slowly or doesn't change at all
No differentiator	Volatility is no major differentiator for the selection of this mindset paradigm.

4.2.3 Trustworthiness

Value	Explanation
Enabler	Security efforts can be easily linked to business processes; business management perceives security as an important aspect of their products or services. The product or services themselves or the supporting processes are information intense.
Burden	It is hard to relate security efforts to business processes; business management perceives security as a technical issue and a cost factor that should be minimized.
Open minded	The organisation is willing and eager to improve it's security based on the comments of others.
Everybody's friend	Security requirement are pretty low, controlling access does nit have priority.
Suspicious mind	Only a very small group of people is trusted, the rest is not trusted and excluded of information about how the security is organised. There is a strong emphasis on controlling access.
Safety critical	Security requirement are very high, an incident can result in a loss of lives.
Mission critical	Security requirement are very high, an incident can result in an important business discontinuity for the organisation itself and possibly a lot of other organisations.
No differentiator	Trustworthiness is no major differentiator for the selection of this mindset paradigm.

4.3 Security as a business issue

4.3.1 Context

Connectivity: Highly connected
Volatility: Volatile or highly volatile
Trustworthiness: Enabler

4.3.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.3.3 Forces

To be done.

4.3.4 Solution

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 the boundaries of the organizations towards customers, partners and citizens depending on the type of organization. Security is a subject that is on the agenda of the management team. The team is committed to keep the security level in balance with the actual threat level to the business processes. Security is a subject that plays an important role in every business contact of the organisation. What should be protected is the question and now how do we protect in a technical sense. 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.

4.3.5 Example

To be done.

4.3.6 Consequences

Positive aspects:

- Business processes get optimal support from IT
- Security is in the minds AND within technology
- Risks are managed based on real business values
- Making decisions and allocating resources for it because easier based the justification for the investment is clear
- Security is an integral part of the change process

Pitfalls:

- People that still think that security is about technology
- Processes and terminology that is not fully understood by all stakeholders

4.4 Security as a technical issue

4.4.1 Context

Connectivity: Connected or isolated
Volatility: Volatile or static world
Trustworthiness: Burden

4.4.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.4.3 Forces

To be done.

4.4.4 Solution

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. The CIO, ICT / information manager is the problem owner and that should stay this way. People from the ICT department are aware of the problem they think. If something goes wrong the IT department gets the blame. The issue is here, how can we protect in a technical sense with an almost 100 percent certainty that nothing can go wrong. What needs to be protected and why is not an issue. Projects tend to delay because security is a bottleneck and have to be sorted out thoroughly. Business people ask themselves why is security always the problem?

4.4.5 Example

To be done.

4.4.6 Consequences

Positive aspects:

- Technical issues seem to be easier to solve than more complex issues (technical and non-technical)
- Results are easier to measure

Pitfalls:

- Problems to find justification for investments and make decisions for security
- Money that is spent to thing that do not have real value to the business
- No awareness and/or commitment from end-users and general management
- Security procedures are ineffective so governance on security measures will be a problem
- Business oriented risks (involving people) are not covered

4.5 Need to protect

4.5.1 Context

Connectivity: Connected or highly connected

Volatility: Volatile or highly volatile

Trustworthiness: No differentiator

4.5.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.5.3 Forces

To be done.

4.5.4 Solution

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

4.5.5 Example

To be done.

4.5.6 Consequences

Positive aspects:

- Cost effective way of doing security, only those assets that need protection get protection
- More convenient for the user, the interference costs will be lower

Pitfalls:

- Security procedures not in place to do risks assessment and classification
- Need to protect may change through time for a particular information asset
- The IT architecture must be able to facilitate a need to protect paradigm instead of a all or nothing strategy
- Additional governance costs to administer the level of protection and to keep them aligned with the business need.
- To complex classification models that are not fully understood by the stakeholders

4.6 Need to know

4.6.1 Context

Connectivity: Isolated or connected
Volatility: Static world or volatile
Trustworthiness: Suspicious mind

4.6.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.6.3 Forces

To be done.

4.6.4 Solution

A person only gets the privilege to use a particular information asset if there is really a business need for it, e.g. the person really needs this information asset to do the job. The idea behind this paradigm is that if people can access more information assets than they need to fulfil their job that 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 paradigm is: Nothing is permitted unless explicitly authorised.

4.6.5 Example

Just as you wouldn't give a random employee the keys to the CEO's office, don't give the person access to the CEO's files.

4.6.6 Consequences

Positive aspects:

- A theoretical high level of security can be achieved if the organisation is fully committed to enforce this paradigm

Pitfalls:

- Not convenient for the user, the interference costs will be high
- The paradigm will slow down the speed in business processes
- People don't receive information because they do not know that the information is available (only they are not authorized for it)
- People will do sabotage on the paradigm the enhance their own performance
- Security procedures not in place to do risks assessment and classification
- Need to know may change through time for a particular information asset
- IT must be able to facilitate “need to know” instead of a all or nothing strategy
- Additional governance costs to administer the level of protection and to keep them aligned with the business need
- To complex classification models that are not fully understood by the stakeholders
- If the organisation is not committed to this paradigm, it will not work.

4.7 Uncontrolled access

4.7.1 Context

Connectivity: No differentiator
Volatility: No differentiator
Trustworthiness: Everybody's friend

4.7.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: "What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards".

4.7.3 Forces

To be done.

4.7.4 Solution

There are no formal procedures for authorisation management. It is not clear which persons in the organisation are authorising other persons. There is a big amount of trust in the organization that nobody will misuse their rights to look and use a lot of information and applications; more than is strictly needed to perform a specific role. The culture is open, nobody has problems which the fact that the amount of information sharing is very high. Efficiency and simplicity in doing the job is more important than doing it securely. Management is not committed to information security at all.

4.7.5 Example

To be done.

4.7.6 Consequences

Positive aspects:

- Information will flow fast through the organisation
- Knowledge working is easy
- Security costs are low in terms of procedures and technology
- The infrastructure are simple, easy to use and governance costs are low

Pitfalls:

- Infrastructure is very vulnerable to attacks of humans and machines
- Privacy of people is not protected
- Sensitive information will leak easily
- Integrity of information can not be assured
- Infrastructure and information can be misused easily by internal and external users
- Large fraud risks which is hard to detect and prosecuted
- Threat to the continuity of the organisation if the organisation is dependent on its information infrastructure
- Organisation will be held liable by external parties if something goes wrong

4.8 Manage risk

4.8.1 Context

Connectivity: Connected or highly connected
Volatility: Volatile or highly volatile
Trustworthiness: Enabler , mission critical of safety critical

4.8.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.8.3 Forces

To be done.

4.8.4 Solution

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.

4.8.5 Example

The goal cannot be to avoid all risks to the network – that's simply unrealistic. Instead, accept and embrace these two undeniable truths.

4.8.6 Consequences

Positive aspects:

- A defined level of security can be achieved
- Money is spend more efficient, decisions are more clear and explicit
- Security is an integral part of change
- People of all levels and disciplines will be involved improving awareness, commitment and a complete and holistic view on the problem
- It's easier to prioritise security measure in case of very limited budgets for security
- Managing risks promotes creative thinking and finding much cheaper and/or effective security controls

Pitfalls:

- Management that do not dare/want to accept risk
- To much granularity in the analysis
- Time and money needed to perform analysis
- Incompetent personal performing the analysis
- Not all stakeholders are involved in the analysis

- To complex classification models that are not fully understood by the stakeholders
- Risks that are not managed on a continuous basis
- Risks analysis is performed with different methods / tools because different (external) parties are involve
- A technocratic approach in terms of “a tools that will generate all the answers”
- Not all relevant risks are known
- To much risks are included in the analysis
- People / organisations that are not enough rewarded for the quality of the risk management process

4.9 Risk avoidance

4.9.1 Context

Connectivity: Isolated or connected
Volatility: Static world or volatile
Trustworthiness: Burden, suspicious mind, safety critical or mission critical

4.9.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.9.3 Forces

To be done.

4.9.4 Solution

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 or 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 budget. 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.

4.9.5 Example

To be done.

4.9.6 Consequences

Positive aspects:

- Products and services having high quality

Pitfalls:

- Too much granularity in the analysis
- Products and services that are outdated and too expensive
- Governance is expensive
- Product and service development is very slow or will be frustrated

4.10 Risk unawareness

4.10.1 Context

Connectivity: Isolated
Volatility: Static world
Trustworthiness: Burden or everybody's friend

4.10.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: "What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards".

4.10.3 Forces

To be done.

4.10.4 Solution

People in the organisation are not aware that identifying risk and managing it, 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 do their job with the computer and the thing does what it should do.

4.10.5 Example

To be done.

4.10.6 Consequences

Positive aspects:

- People tend to sleep well as long as no serious disaster happens

Pitfalls:

- Inadequate level of security
- Money for security will be spend on the wrong things

4.11 Entity to entity security

4.11.1 Context

Connectivity: Connected or highly connected
Volatility: Volatile or highly volatile
Trustworthiness: Enabler, safety critical or mission critical

4.11.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.11.3 Forces

To be done.

4.11.4 Solution

Instead of trust between machines (end-to-end security) there must be trust between the business actors themselves. Let say the people behind the machines. Entity-to-entity security can be build on end-to-end security but is 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, an open communication culture and the amount of management commitment to maintain the trust relationship.

4.11.5 Example

To be done.

4.11.6 Consequences

Positive aspects:

- Trust between entities enhance information exchange and business processes between organizations
- Multiple levels of trust can be are supported enhancing the flexibility of the organisations to differentiate between communication partners

Pitfalls:

- Paradigm might not be supported by all levels of the organization or between organisations
- Legal aspects
- Responsibilities that are not clear

4.12 End to end security

4.12.1 Context

Connectivity: Connected or highly connected
Volatility: Volatile or highly volatile
Trustworthiness: Burden, safety critical or mission critical

4.12.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.12.3 Forces

To be done.

4.12.4 Solution

The whole chain from the initiating machine, through the different network components until the machine that serves the request needs to be secure. The whole chain needs to be strong enough. Quality attributes like confidentiality, integrity, availability and auditability are designed and implemented and must be delivered by the entire chain of components. 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.

4.12.5 Example

To be done.

4.12.6 Consequences

Positive aspects:

- Security vulnerabilities will be detected because the entire chain is analysed
- Clear responsibilities in terms of who is accountable for what
- Instrument to improve service levels between organisations and make them more explicit

Pitfalls:

- Too much granularity in the analysis
- Time and money needed to perform analysis
- Incompetent personnel performing the analysis
- Not all stakeholders are involved in the analysis
- Inadequate domain partitioning
- Responsibilities that are not clear

4.13 Point solutions

4.13.1 Context

Connectivity: Isolated
Volatility: Static world
Trustworthiness: Burden

4.13.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.13.3 Forces

To be done.

4.13.4 Solution

If there is a security problem, the organization buys a product for it to solve the problem. There is not a 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 which are overlapping in functionality, there are some security vulnerabilities, it is hard to integrate information systems because the security solution is 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.

4.13.5 Example

To be done.

4.13.6 Consequences

Positive aspects:

- Organisation do now spend much time and money on analysis

Pitfalls:

- Undefined level of security
- Risks are not managed based on business need
- A large variety of security products which are overlapping in functionality
- High governance costs
- Hard to manage security on a corporate level

4.14 Obey the law

4.14.1 Context

Connectivity: No differentiator
Volatility: No differentiator
Trustworthiness: Enabler, safety critical or mission critical

4.14.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.14.3 Forces

To be done.

4.14.4 Solution

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.

4.14.5 Example

To be done.

4.14.6 Consequences

Positive aspects:

- The organisation takes it's responsibility
- Higher level of protection
- Privacy of people that will be respected
- Corporate imago that will be better
- Organisation becomes more transparent

Pitfalls:

- Time and money spend
- Hard to keep knowledge up to date
- Hard to assess the impact of a law
- Conflicting priorities, obeying the law versus making money

4.15 Violate the law

4.15.1 Context

Connectivity: Isolated
Volatility: Static world
Trustworthiness: Burden

4.15.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.15.3 Forces

To be done.

4.15.4 Solution

Drivers to obey the law are missing for a number of reasons. People are not familiar with most of the details of the law or don't give priority to it because the law will not be enforced anyhow. Computer laws can be 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.

4.15.5 Example

To be done.

4.15.6 Consequences

Positive aspects:

- Less time and money spend on compliancy

Pitfalls:

- Risks to business continuity
- Threat to the corporate imago
- The organisation will not be trusted by others
- Privacy en safety of people that will be protected

4.16 Safety before security

4.16.1 Context

Connectivity: No differentiator
Volatility: No differentiator
Trustworthiness: Safety critical

4.16.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.16.3 Forces

To be done.

4.16.4 Solution

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.

4.16.5 Example

To be done.

4.16.6 Consequences

Positive aspects:

- Safety of people that will be protected
- Good corporate image

Pitfalls:

- Time and money spend to reach the right level of safety
- Formal procedures that are outdated
- Priority clash between saving lives and making money

4.17 Safety unawareness

4.17.1 Context

Connectivity: No differentiator
Volatility: No differentiator
Trustworthiness: Safety critical

4.17.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.17.3 Forces

To be done.

4.17.4 Solution

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 happen or think, “This is really bad luck”.

4.17.5 Example

To be done.

4.17.6 Consequences

Positive aspects:

- People tend to sleep well as long as no serious disaster happens

Pitfalls:

- Lives are at stake
- Tension between safety level and money spend

4.18 Keep it open

4.18.1 Context

Connectivity: Connected or highly connected
Volatility: Volatile or highly volatile
Trustworthiness: Open minded

4.18.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.18.3 Forces

To be done.

4.18.4 Solution

Everybody who is interested can know the security solution. The solution is well understood and verified by a lot of people. The strength of the security solution is determined by the secrecy of the key(s) that are parameters for the security solution. 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. Keeping the algorithm secret is often tried, but never successfully.

4.18.5 Example

Applying and sharing security patterns is an example of a “Keep it open” mindset.

4.18.6 Consequences

Positive aspects:

- Security solutions are well known and can be verified
- Better interoperability between components
- Cost effective

Pitfalls:

- Making keys too easy to break
- Quantum leaps in processing power capabilities

4.19 Security by obscurity

Can also be called: **Leverage Unpredictability**

4.19.1 Context

Connectivity: Isolated or connected
Volatility: Static world or volatile
Trustworthiness: Suspicious mind

4.19.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.19.3 Forces

To be done.

4.19.4 Solution

The strength of the security solution is completely based on the fact that only a 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 for them. The real prove is in the eating of the pudding, so the real world will determine how strong the solution is.

4.19.5 Example

You know your network; your attacker doesn't. This is your big advantage. Make his job harder by disguising things, adding honey pots and booby traps, etc.

4.19.6 Consequences

Positive aspects:

- Make security obscure is often a cheap and easy solution

Pitfalls:

- Security becomes very weak as soon as the “secret” is known or discovered by accident

4.20 Keep it simple

4.20.1 Context

Connectivity: Connected or highly connected
Volatility: Volatile or highly volatile
Trustworthiness: No differentiator

4.20.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.20.3 Forces

To be done.

4.20.4 Solution

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.

4.20.5 Example

To be done.

4.20.6 Consequences

Positive aspects:

- Solution is easy to understand and verify

Pitfalls:

- If the solution is too simple it will not work

4.21 Make it complex

4.21.1 Context

Connectivity: Isolated
Volatility: Static world
Trustworthiness: Suspicious mind

4.21.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.21.3 Forces

To be done.

4.21.4 Solution

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.

4.21.5 Example

Install deception toolkits to give false information to the attacker.

4.21.6 Consequences

Positive aspects:

- Attacker might need more time to know what is going on

Pitfalls:

- Inherent security weaknesses because it is hard to verify the security solution
- Governance costs will be high because of the complexity

4.22 Fail securely

Can also be called: **Ductile security**

4.22.1 Context

Connectivity: No differentiator
Volatility: No differentiator
Trustworthiness: Enabler, mission critical or safety critical

4.22.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.22.3 Forces

To be done.

4.22.4 Solution

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 security solution will detect when the primary security protection fails and will kick down to the secondary security protection and/or risk avoidance scenario.

4.22.5 Example

- Design your networks so that when products fail, they fail in a secure manner. When an ATM fails, it shuts down; it doesn't spew money out its slot. Use security mechanisms that adapt to the situation, they shape and react differently when treated differently. A cool and sturdy guard can sometimes alter in a horrendous fighting machine.
- Don't rely on single solutions. Use multiple complementary security products, so that a failure in one does not mean total insecurity. If one domain is compromised the intruder or intrusion can be fenced in.

4.22.6 Consequences

Positive aspects:

- Even if the primary level of protection fails, the solution is still secure

Pitfalls:

- A lot of successful well known security mechanisms do not fail securely

4.23 Trust your security

4.23.1 Context

Connectivity: Isolated
Volatility: Static world
Trustworthiness: Burden

4.23.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.23.3 Forces

To be done.

4.23.4 Solution

People think that the security solution is bullet proof. Nobody is considering the situation that the security solution might fail. A failing security solution will result in business discontinuity in most of the 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.

4.23.5 Example

To be done.

4.23.6 Consequences

Positive aspects:

- The number of measures are relatively small

Pitfalls:

- A false sense of security leads to insecurity
- Weak detection and response

4.24 Security goals before means

4.24.1 Context

Connectivity: Connected or highly connected
Volatility: Volatile or highly volatile
Trustworthiness: Enabler, safety critical or mission critical

4.24.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.24.3 Forces

To be done.

4.24.4 Solution

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.

4.24.5 Example

To be done.

4.24.6 Consequences

Positive aspects:

- New security products can easily interchange outdated security products as long as the new products can full-fill the logical security requirements.
- More assurance that the right products are implemented

Pitfalls:

- Too much time and money spend on analysis

4.25 Trust your vendor

4.25.1 Context

Connectivity: Isolated or connected
Volatility: Static world or volatile
Trustworthiness: Everybody's friend

4.25.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: "What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards".

4.25.3 Forces

To be done.

4.25.4 Solution

If the vendor of a security product says the product is secure enough then the organization will use the product. There is also no need to obtain security requirements or perform a 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.

4.25.5 Example

To be done.

4.25.6 Consequences

Positive aspects:

- Organisation do not spend much time and money on analysis

Pitfalls:

- Undefined level of security
- Risks are not managed based on business need
- Hard to manage security on a corporate level

4.26 Time based security

4.26.1 Context

Connectivity: No differentiator
Volatility: No differentiator
Trustworthiness: Enabler, mission critical or safety critical

4.26.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.26.3 Forces

To be done.

4.26.4 Solution

The organization is aware that security measures will fail. The 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 than the time the attacker needs for a successful attack.

4.26.5 Example

To be done.

4.26.6 Consequences

Positive aspects:

- If the concepts are applied in the right way, people can really measure the success of preventive security controls
- The concepts can be easily explained to the management level so awareness can be raised (e.g. a firewall only is not enough)
- Implementation costs and interference costs for preventive security measures can be lower if smart detection and response mechanisms are applied. Leading to more user convenience and more business in the end.
- Security controls themselves can also be protected by the time based security concepts (e.g. defence in depth)

Pitfalls:

- Not all security incidents are related to attacks by hackers
- Detection mechanisms may cause a lot of false alarms, increasing governance costs
- Response mechanisms need a lot of procedural agreements and management commitments
- Multiple parties may be involved for a good detection and response

4.27 Fortress mentality

4.27.1 Context

Connectivity: Isolated
Volatility: Static world
Trustworthiness: Burden

4.27.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.27.3 Forces

To be done.

4.27.4 Solution

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.

4.27.5 Example

To be done.

4.27.6 Consequences

Positive aspects:

- The solution is easy because security controls are mainly concentrated around the boundary of the infrastructure
- If the architecture is designed well, the security interaction with the outside world can be managed centrally
- Detection and response mechanisms are easier to implement around the boundaries of the organisation than within the infrastructure itself
- Security within the organisation can be simplified (only if internal staff can be trusted and the security fence works correctly)

Pitfalls:

- The security fence around the organisation limits interaction with the world outside
- Creating and maintaining the rules for the security fence is a hard job that need a lot of support and commitment from the organization
- The security fence might become a performance bottleneck
- Most of the security incidents originate from the inside and not from the outside
- The security fence is very vulnerable for alternate connections that are not controlled by the security policy

4.28 Trust nobody

4.28.1 Context

Connectivity: No differentiator
Volatility: No differentiator
Trustworthiness: Enabler, mission critical or safety critical

4.28.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.28.3 Forces

To be done.

4.28.4 Solution

Nobody can be trusted. The most loyal employee cannot be trusted if the reward of fraud is high enough and the change of being detected is low. The organization does not want to bring their employees into temptation. Four eyes 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.

4.28.5 Example

To be done.

4.28.6 Consequences

Positive aspects:

- Employees are protected against themselves
- Trust into the organisation will grow because of the reduced fraud risk
- The risks of financial loss for the organization itself or for others will be reduced

Pitfalls:

- Employees might feel themselves limited in performing their task
- Speed of business processes might slow down
- Cost for additional security controls can be a burden for the organization

4.29 Trust your employees

4.29.1 Context

4.29.2 Problem

Mindset paradigm patterns are quite interesting since they all address exactly the same problem: “What is the right (combination of) paradigm(s) to formulate the corporate security strategy in order to select and implement the appropriate set of security safeguards”.

4.29.3 Forces

To be done.

4.29.4 Solution

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 paradigm. Note that this solution can be found in day-to-day life. The pattern writers do not want to suggest that this paradigm is the first option to think of.

4.29.5 Example

To be done.

4.29.6 Consequences

Positive aspects:

- Employees feel themselves empowered
- Investments for security measures to control fraud are low
- Business processes can be fast (not a lot of additional checking)

Pitfalls:

- Fraud risk will increase
- Fraud can not be easily detected and prosecuted

5 PREVIEW ON ARCHITECTURE PARADIGM PATTERNS

5.1 Introducing Architecture Paradigms

Architecture paradigm patterns are quite interesting since they, just like the mindset Paradigm patterns, all address exactly the same problem:

What is the right combination of architecture paradigms in order to select and implement the appropriate set of security safeguards, given the formulated security strategy based on a combination of security mindset paradigms?

Just like the mindset Paradigm patterns, the architecture paradigm patterns differ in context. The context of the architecture paradigm pattern is determined by the combination of paradigms used to formulate the corporate or enterprise security strategy

5.2 Security guard

5.2.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a business issue, Need to know, Keep it simple.

5.2.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right combination of architecture paradigms in order to select and implement the appropriate set of security safeguards, given the formulated security strategy based on a combination of security mindset paradigms?”

5.2.3 Forces

To be done.

5.2.4 Solution

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.

5.2.5 Example

By funnelling requests for business services through choke points, you can more carefully secure those few points. You simply need to have fewer guards. Requests for business services that bypass these choke points make security much harder.

5.2.6 Consequences

Positive aspects:

- A security guard enables central security management
- The security guard can be enhanced with detection and response mechanisms
- Other parts of the infrastructure can be simplified if all request are screened by the security guard

Pitfalls:

- The security guard is as good as it's governance in terms of correctness of the rules and timely installations of security patches
- If all request are screened then performance will degrade
- It is questionable if the security guard can detect and prevent all malicious requests. The payload may be embedded into the request
- Change procedure might become more complex
- There is a risk that the security guard will be by-passed
- Creating and maintaining the rules for the security guard is a hard job that need a lot of support and commitment from the organization

5.3 Perimeter defence

5.3.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a technical issue, Risk avoidance, End to end security, Point solutions, Security by obscurity, Fail securely, Trust your security, Fortress mentality

5.3.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right combination of architecture paradigms in order to select and implement the appropriate set of security safeguards, given the formulated security strategy based on a combination of security mindset paradigms?”

5.3.3 Forces

To be done.

5.3.4 Solution

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.

5.3.5 Example

A DMZ is a good example.

5.3.6 Consequences

Positive aspects:

- A perimeter defence enables central security management
- The perimeter defence can be enhanced with detection and response mechanisms
- Other parts of the infrastructure can be simplified if all request are screened by the perimeter defence

Pitfalls:

- The perimeter defence is as good as it's governance in terms of correctness of the rules and timely installations of security patches
- If all request are screened then performance will degrade
- It is questionable if the perimeter defence can detect and prevent all malicious requests. The payload may be embedded into the request
- Change procedure might become more complex
- There is a risk that the perimeter defence will be by-passed
- Creating and maintaining the rules for the perimeter defence is a hard job that need a lot of support and commitment from the organization

5.4 Divide and conquer

5.4.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Need to know, Manage risk, Risk avoidance, Safety before security, Fortress mentality

5.4.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right combination of architecture paradigms in order to select and implement the appropriate set of security safeguards, given the formulated security strategy based on a combination of security mindset paradigms?”

5.4.3 Forces

To be done.

5.4.4 Solution

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 it's own specific security policy and derived procedures. If a domain does not have it's 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.

5.4.5 Example

To be done.

5.4.6 Consequences

Positive aspects:

- With security domains multiple levels of trust can be introduced
- Security domains enable standardization
- If the trust levels between security domains are well defined then drafting the window policies will be easier

Pitfalls:

- Security domains can be based on several characteristics they can even be nested. Defining the ideal domain architecture is a hard job needing a lot of expert knowledge and contextual information
- Boundaries of security domains might be by-passed by creative attackers
- By applying security domains one should be careful not to fall back to an ordinary fortress mentality mindset

5.5 The network as a battleground

5.5.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a business issue, Need to protect, Make it complex, Fail securely, Time Based Security

5.5.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right combination of architecture paradigms in order to select and implement the appropriate set of security safeguards, given the formulated security strategy based on a combination of security mindset paradigms?”

5.5.3 Forces

To be done.

5.5.4 Solution

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.

5.5.5 Example

Detect Attacks. Watch the security products. Look for signs of attack. Too often, valuable alerts from firewalls, servers and even Intrusion Detection Systems are simply ignored.

5.5.6 Consequences

Positive aspects:

- This approach make the organization less vulnerable for attacks
- A high level to trust and protection can be reached

Pitfalls:

- Ordinary companies are not familiar with military concepts so a lot of training is needed to apply this paradigm on a large scale

5.6 Peace or war

5.6.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a business issue, Need to protect, Fail securely, Time Based Security

5.6.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right combination of architecture paradigms in order to select and implement the appropriate set of security safeguards, given the formulated security strategy based on a combination of security mindset paradigms?”

5.6.3 Forces

To be done.

5.6.4 Solution

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.

5.6.5 Example

To be done.

5.6.6 Consequences

Positive aspects:

- In the “business as usual” state, security is easy and transparent
- A high level to trust and protection can be reached

Pitfalls:

- Ordinary companies are not familiar with this concept so a lot of training is needed to apply this paradigm on a large scale
- A lot of thinking needs to be done on the number of states, criteria for state transitions and things like “who is going to decide on what?”
- Multiple security states increases the complexity of the technology and related procedures

5.7 Immune system

5.7.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a business issue, Need to protect, Manage risk, Risk unawareness, Entity to entity security, Keep it open, Fail securely, Time Based Security

5.7.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right combination of architecture paradigms in order to select and implement the appropriate set of security safeguards, given the formulated security strategy based on a combination of security mindset paradigms?”

5.7.3 Forces

To be done.

5.7.4 Solution

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.

5.7.5 Example

To be done.

5.7.6 Consequences

Positive aspects:

- A high level to trust and protection can be reached
- A good immune system enabler the “Trustworthy computing” vision of a number of companies

Pitfalls:

- Ordinary companies are not familiar with this concept so a lot of training is needed to apply this paradigm on a large scale
- Especially the self learning aspects are subject to further research

5.8 Layered security

5.8.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a technical issue, Manage risk, End to end security, Safety before security, Keep it simple, Fail securely, Security goals before means, Fortress mentality

5.8.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right combination of architecture paradigms in order to select and implement the appropriate set of security safeguards, given the formulated security strategy based on a combination of security mindset paradigms?”

5.8.3 Forces

To be done.

5.8.4 Solution

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.

5.8.5 Example

To be done.

5.8.6 Consequences

Positive aspects:

- A number of security layers will make the security solution more robust
- The number of abstractions will make the security solution more clean as well

Pitfalls:

- Security products and components to be used might be incompatible with the abstractions the organisation likes to use

5.9 Defence in depth

5.9.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a business issue, Need to protect, End to end security, Make it complex, fail securely, Time Based Security

5.9.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) paradigm(s), given the appropriate (combination of) Mindset Paradigm(s), to formulate the right starting point in order to architect and design the appropriate set of security safeguards”

5.9.3 Forces

To be done.

5.9.4 Solution

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 paradigm can be an extension of the time based security paradigm.

5.9.5 Example

A detection mechanism is used to detect if a preventive security mechanism is compromised. Corrective actions are automatically started to prevent that the attack will be successful.

5.9.6 Consequences

Positive aspects:

- Security solution will be more robust

Pitfalls:

- The solution becomes more complex because one has to know; “what is protecting what and why?”

5.10 Watch the Watchers

5.10.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a business issue, Need to know, Risk avoidance, Entity to entity security, Violate the law, Fail securely, Trust nobody

5.10.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) paradigm(s), given the appropriate (combination of) Mindset Paradigm(s), to formulate the right starting point in order to architect and design the appropriate set of security safeguards”

5.10.3 Forces

To be done.

5.10.4 Solution

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 paradigm.

5.10.5 Example

To be done.

5.10.6 Consequences

Positive aspects:

- High levels of security can be reached

Pitfalls:

- Complex and costly to implement

5.11 Enlist the Users

5.11.1 Context

The organisation has formulated its security strategy based on one of the following security mindset paradigms; Security as a business issue, Need to protect, Uncontrolled access, Manage risk, Entity to entity security, Obey the law, Safety before security, Safety unawareness, Time Based Security, Trust your employees

5.11.2 Problem

Architecture paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) paradigm(s), given the appropriate (combination of) Mindset Paradigm(s), to formulate the right starting point in order to architect and design the appropriate set of security safeguards”

5.11.3 Forces

To be done.

5.11.4 Solution

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. User are asked to report security incidents and weaknesses immediately. The users are the (human) sensors of the protection system.

5.11.5 Example

To be done.

5.11.6 Consequences

Positive aspects:

- If users are enlisted the weakest link in the security chain will be stronger

Pitfalls:

- Making users aware and feel responsible will cost time and especially management commitment
- The culture of the organisation might be incompatible with this approach
- Making users aware and alert is difficult to keep them aware over a period of time is even more difficult

6 PREVIEW ON EXECUTION PARADIGM PATTERNS

6.1 Introducing Execution Paradigms

Execution paradigm patterns are quite interesting since they, just like the mindset Paradigm patterns, all address exactly the same problem:

What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?

Just like the mindset Paradigm patterns, the execution paradigm patterns differ in context. The context of the organisation, described in the dimensions mentioned before (connectivity, volatility, trustworthiness), determines the solution: so these are exactly the contextual parameters for the Mindset paradigm, so the Mindset paradigms for the “To Be” position of the organisation are the first ingredient for the context of the execution paradigm.

The culture of the organisation is the other important part of the context for the execution paradigm, which is described in the following table:

Value	Explanation
Hierarchical/Formal	Decision procedures are formal and strict; everybody obeys the management of the organisation. Roles and responsibilities are clearly defined.
Informal	Decisions are made on the fly or it is not clear how decisions are made. Everybody would like to be consulted before a decision is made. Roles and responsibilities are not clearly defined.
Business driven	The goal of the organisation is making money. Decisions are made based on a sound business case. Everything that is not core to the organisation is a candidate for outsourcing.
Cost driven	The goal of the organisation is not making money but supplying a service (to the public) based on a given budget. Quality and speed is the main variable in here,
Flexible/Professional	It is easy for (the people in) the organisation to adapt to other circumstances. The employees are well educated and eager to learn and improve.
Static/Bureaucratic	Decision procedures are formal and take an enormous period of time. There are a lot of rules that must be obeyed and a lot of forms need to be filled in and approved for every little change and improvement. Making no mistakes is much more important than make process.
No differentiator	Culture is no major differentiator for the selection of this mindset paradigm.

6.2 Return on investment

6.2.1 Context

Note: Some discussion is needed to define the context of the execution paradigms, options are among others, the security maturity level and/or cultural and/or managerial aspects.

Mindset: No differentiator

Culture: No differentiator

6.2.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.2.3 Forces

To be done.

6.2.4 Solution

Every security solution should have an economic justification. Risk analysis techniques are used to calculate the “cost” of the solution versus the “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.

6.2.5 Example

To be done.

6.2.6 Consequences

Positive aspects:

- The cost of security measures can be justified if the analysis can give the complete picture

Pitfalls:

- In practice it is not easy to calculate the cost of security measures accurately. This is because a lot of costs are hidden
- The same holds for the benefits of measure measures. What is the benefit of a situation where nothing happens?
- A lot of benefits can't be expressed in money. For example what is the value of a good image for the organization

6.3 Security at any price

6.3.1 Context

Mindset: No differentiator

Culture: No differentiator

6.3.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.3.3 Forces

To be done.

6.3.4 Solution

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

6.3.5 Example

Protection of governmental information of the highest classification

Protecting a nuclear plant.

6.3.6 Consequences

Positive aspects:

- Theoretically a high level of security can be reached

Pitfalls:

- The cost will be very high in terms of time and money spend, even if the trust level needs to be very high one should always be open for alternative paradigms that addresses the same goal

6.4 Security in every change

6.4.1 Context

Mindset: No differentiator

Culture: No differentiator

6.4.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.4.3 Forces

To be done.

6.4.4 Solution

The most effective way to incorporate security is at the moment an information 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 an integral aspect of change procedures and project management methodologies. Risk analyses techniques are used to determine the right level of protection that is aligned with the business needs. Security requirements can even influence important design considerations.

6.4.5 Example

To be done.

6.4.6 Consequences

Positive aspects:

- It is easier and more cost effective to change or create information assets the right way from the start than afterwards
- Security is an integral aspect of change procedures and project management methodologies
- A process oriented approach will give more assurance that security objectives will be reached

Pitfalls:

- Incorporating security in every change pays itself off on the longer term but might slow down development on the short term especially if resources are scarce

6.5 Security as a desert

6.5.1 Context

Mindset: No differentiator

Culture: No differentiator

6.5.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.5.3 Forces

To be done.

6.5.4 Solution

Information assets and business processes are created based on the functionality they need to full fill. There is no attention for security during the creation of change process of an information asset or business process. The organization has the perception that security can be bolded on the solution if this really necessary. It's more like hiring more agents as soon people feel that the situation becomes unsafe.

6.5.5 Example

To be done.

6.5.6 Consequences

Positive aspects:

- Investments in security in terms of time and money are postponed to a moment later in time
- De business solution is simpler and more clean if security complexity can be skipped

Pitfalls:

- Building in security afterwards is more expensive and it might even be impossible to build it in later because of a number of reasons
- As long as security controls are not operational the organization might be at risk. Sometimes it will take months and even years before a security backlog can be eliminated

6.6 Proactive governance

6.6.1 Context

Mindset: No differentiator

Culture: No differentiator

6.6.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.6.3 Forces

To be done.

6.6.4 Solution

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.

6.6.5 Example

To be done.

6.6.6 Consequences

Positive aspects:

- The number of vulnerabilities on the technical level will be reduced significantly

Pitfalls:

- Patching IT components is very time consuming and might threaten business continuity
- There will be always a risk that an attacker can exploit a vulnerability faster than the IT-components can be patched

6.7 Ignore security patches

6.7.1 Context

Mindset: No differentiator

Culture: No differentiator

6.7.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.7.3 Forces

To be done.

6.7.4 Solution

Security patches issued by solution providers are installed to late (after a major virus or worm incident has happened) or not installed at all. Short-term business continuity is much more important than the actual security level. Patching security has no priority. Business managers are unaware that security patches should get priority over “getting the job of today done”.

6.7.5 Example

To be done.

6.7.6 Consequences

Positive aspects:

- No time and money spend on security

Pitfalls:

- The vulnerability for attacks will grow through time
- If the organisation is hacked, it's computing resources will be a threat to other organizations as well

6.8 Mature through time

6.8.1 Context

Mindset: No differentiator

Culture: No differentiator

6.8.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”.

6.8.3 Forces

To be done.

6.8.4 Solution

The organisation is proactively seeking for ways to improve its security in a fundamental way. Maturity models are used to identify the current level of security; targets for future security levels are set and agreed. There is a formal planning, execution and reviewing process to make sure the new security level is reached. Security is not an all or nothing subject but something that can has multiple comfort levels.

6.8.5 Example

The new versions of COBIT, anti-virus maturity model

6.8.6 Consequences

Positive aspects:

- The organization is seeking for continues improvement
- A security improvement programme can be divided in smaller steps
- It will enable organisations to benchmark themselves against similar organisations or organisations operating on the same level of trust

Pitfalls:

- Maturity levels for security are still subject to further research. The authors of this pattern think that even security CMM is only one part of the solution.

6.9 Wait for the auditor

6.9.1 Context

Mindset: No differentiator

Culture: No differentiator

6.9.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.9.3 Forces

To be done.

6.9.4 Solution

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.

6.9.5 Example

To be done.

6.9.6 Consequences

Positive aspects:

- Investments in security in terms of time and money are postponed to a moment later in time
- De business solution is simpler and more clean if security complexity can be skipped

Pitfalls:

- Building in security afterwards is more expensive and it might even be impossible to build it in later because of a number of reasons
- As long as security controls are not operational the organization might be at risk. Sometimes it will take months and even years before a security backlog can be eliminated

6.10 Issue driven

6.10.1 Context

Mindset: No differentiator

Culture: No differentiator

6.10.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.10.3 Forces

To be done.

6.10.4 Solution

The organisation recognizes that securing all the things that need to be secured is a job that is not feasible. Resources (time, people and money) need to be used in the most effective way. Every difference between the “As Is” and “To Be” position is administered as a security issue. Security issues are prioritised and clustered based on risk management techniques and synergies with already existing change processes and projects. The most important and/or the easiest to solve security issues get the highest priority to be solved.

6.10.5 Example

To be done.

6.10.6 Consequences

Positive aspects:

- Time and money on security is spend efficiency given the backlog in security that is already there
- A approach based on solving important security issues as soon as possible enables an organization to improve it's security over time

Pitfalls:

- Building in security afterwards is more expensive and it might even be impossible to build it in later because of a number of reasons
- As long as security controls are not operational the organization might be at risk. Sometimes it will take months and even years before a security backlog can be eliminated

6.11 Top Down Approach

6.11.1 Context

Mindset: No differentiator

Culture: No differentiator

6.11.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.11.3 Forces

To be done.

6.11.4 Solution

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

6.11.5 Example

To be done.

6.11.6 Consequences

Positive aspects:

- The approach is structured and it's intention is to reach a level of completeness

Pitfalls:

- The problem with this approach is that it does not work in practice. For larger organizations it might take a lot of years before that all activities are completed only ones for the first cycle.
- Some top down approached do not stress enough that security awareness is the key to success

6.12 Just do it together

6.12.1 Context

Mindset: No differentiator

Culture: No differentiator

6.12.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.12.3 Forces

To be done.

6.12.4 Solution

The organisation tries to follow the top down approach more or less but recognizes that performing a pure top down approach including formal risk analysis will simply take too much time and will be too expensive. Awareness is an issue as well and all security controls can't be implemented at once. Therefore a more practical approach is taken. A very thin security baseline is drafted and implemented. Security analysis is performed on information systems that are really important for the organization. Workshop techniques are used to mobilize people, make them aware and speed up the process. In this way in only 20 percent of the time, 80 percent of the security controls are identified and implemented.

6.12.5 Example

To be done.

6.12.6 Consequences

Positive aspects:

- Fast result and relatively good quality
- Awareness is raised for all people involved in the analysis

Pitfalls:

- The quality of the results is heavily dependent on the knowledge of the people involved and the experience of the facilitator of the process

6.13 Paralysis by analysis

6.13.1 Context

Mindset: No differentiator

Culture: No differentiator

6.13.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.13.3 Forces

To be done.

6.13.4 Solution

Thinking about security is much more important than really making things more secure. People spend so much time and money in analysing threats and designing the security solution that there is no time or money to implement the solution. What also might be the case is that as soon as the “eureka” effect is there, the world has been changed and the solution is outdated or not needed anymore. There is no real pressure on concrete results; security is only an intellectual challenge like solving a puzzle.

6.13.5 Example

To be done.

6.13.6 Consequences

Positive aspects:

- We couldn't think of any positive aspects

Pitfalls:

- This approach is not aiming to implement security measures so the world will not become more safe with this paradigm

6.14 Respond on security incidents

6.14.1 Context

Mindset: No differentiator

Culture: No differentiator

6.14.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.14.3 Forces

To be done.

6.14.4 Solution

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.

6.14.5 Example

To be done.

6.14.6 Consequences

Positive aspects:

- The organization becomes self-learning
- A high level of security can be reached

Pitfalls:

- There is a change that organizations see this as the dominant paradigm to reach the right security level.

6.15 Ignore security incidents

6.15.1 Context

Mindset: No differentiator

Culture: No differentiator

6.15.2 Problem

Execution paradigm patterns are quite interesting since they, just like the Mindset Paradigm patterns, all address exactly the same problem: “What is the right (combination of) execution paradigm(s), given the appropriate (combination of) Mindset Paradigm(s) and culture of the internal organisation?”

6.15.3 Forces

To be done.

6.15.4 Solution

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.

6.15.5 Example

To be done.

6.15.6 Consequences

Positive aspects:

- We couldn't think of any positive aspects

Pitfalls:

- Building in security afterwards is more expensive and it might even be impossible to build it in later because of a number of reasons
- As long as security controls are not operational the organization might be at risk. Sometimes it will take months and even years before a security backlog can be eliminated