PvIB Expert Letter – June 2009
ISSN 1872-4876, Volume 2 – No. 1

June 2009

Security architecture: a new hype for specialists, or a useful means of communication?

Henk Bel

Lucien Bongers

Lex Borger

Erno Duinhoven

Jo Koppes

Renato Kuiper

Tonne Mulder

Henny van de Pavert

Michel Ritskes

Kees Terlouw

Many organizations are struggling to translate their information security policy into concrete measures. Often the policy is defined in abstract terms. That makes it difficult for application or infrastructure designers to determine which policy statements have consequences for their areas of responsibility and how they should interpret them. There is no insight into the coherence of security measures.
A security architecture can provide this insight and reduce the complex number of possible directions for solutions on the basis of manageable models and principles.
The expert group has endeavoured to clearly map out what a security architecture is precisely, and when it is meaningful to develop a security architecture. Is it really a useful means of communication, or just another hype?

http://www.pvib.nl/
✉ expertbrief@pvib.nl

2

Introduction and Description of the Situation

Do organizations need a security architecture as well as their information security policy? This question applies to many information security officers but also to architects and managers. If we want to answer that question, we need a clear description of what we mean by security architecture. What is a security architecture precisely, what is its added value and who gains from it?

Most organizations experience a 'gap' between the security policy and its actual interpretation in practice. Often there is a security policy, but its contents are not directly applicable for architects and designers. The policy consists of a description at a high level of abstraction of the objectives to be achieved, but it does not indicate how they should be realized. Many people find it difficult to make the translation from policy to concrete, practical measures.
That partly has to do with the different ways of thinking between policy makers and designers, who have to draw up and realize specific solutions. Often business and ICT environments are also so complex that it is difficult to gain a proper insight into the connection between all the security measures in ICT and business environments. A clear insight is missing. As a result, sub solutions are not matched to each other as best as possible. Technical or procedural measures for a specific sub area are simply implemented in that case on the basis of 'best practice', requirements from auditors, general guidelines from product suppliers or standards frameworks from professional associations.
It remains unclear whether that actually means adherence to the policy of the organization. Translating a defined policy objective effectively and efficiently into concrete measures demands understanding of the arguments behind the objective and how it fits within the total context of the organization. As long as this understanding is missing and risks are not identified sufficiently, it remains difficult to determine where and when an objective is actually properly realized. It's not cost-effective to reinvent the wheel for every sub system or project.
The question is the extent to which a security architecture can bring some improvement to this situation.

Architecture is the realm where the basic assumptions, requirements of the interested parties, the basic principles to be adhered to, the structure and the mutual relationships of elements are represented to provide insight. By creating insight and overview, an architecture can bridge the 'gap' between policy makers and designers for a great deal. This need is emphatically present in the field of security. It also puts designers in the position of being able to work largely independently of each other. Architecture commonly serves as a means of communication between different parties to obtain overview and insight of the whole, and to present everyone's interests and position in the whole in an understandable fashion.

However, developing a security architecture also demands a coordinated approach, and requires investments that will need to be recovered. Before you can make a decision on this, you first need to know clearly what a security architecture is precisely, what it contains and how deep that information is, what the objective and scope are, who the interested parties are, etc. And if you want to develop a security architecture, how do you do it? Can you make a business case, are there fundamental conditions for making a security architecture meaningful, and how do you then tackle the whole matter? And is a security architecture the same for all organizations?

This expert letter aims at providing answers to a number of questions. The investigation questions the expert group posed themselves are listed below. The questions the expert group couldn't answer will be worked out further in a follow-up session.

RESEARCH QUESTIONS

The expert group tackled the following issues:

- What is a security architecture and what is its relationship with other architectures such as business, information, application and infrastructure architectures?
- Why a security architecture, and what is the business case? Is it important to have a security architecture, or is it just another new hype?
- Who does it give added value to?
- Are there circumstances or conditions that determine when it is meaningful or not to develop a security architecture?
- Which aspects and topics belong to a security architecture and with what depth?
- How do you develop a security architecture, and what basic architecture models can you use for that purpose? What are their strong and their weak points?
- How do you guarantee that a security architecture is introduced and maintained and that it will be used effectively?

The expert group realized in advance that it was unlikely to be able to answer all these questions in just one expert session. In the end, the group does want to find an answer to all these questions through follow-up activities.

WHAT IS A SECURITY ARCHITECTURE?

There are different definitions for what architecture is. Similarly, security architecture can be defined in different ways. The expert group chose a definition in simple and understandable language. Transmitting the essence is considered more important than a 100% scientifically correct and full representation.

> A Security Architecture is a prescriptive document that uses a set of coherent models and principles efficiently and flexibly to guide the implementation of the information security policy of an organization.

In other words:
A security architecture consists of a transparent and coherent overview of models, principles, starting points and conditions that give a concrete interpretation of the information security policy, usually without speaking in terms of specific solutions. A security architecture reduces a complex problem into models, principles and sub problems that can be understood, mainly on the basis of the well-known what, where, when, how, with what and who questions. The models and principles show where you take which type of measures, when the principles are applicable, and how they connect with other principles.

The scope of a security architecture is not fixed and can depend to a great extent on the target or the problem that an organization wants to solve with it. Is the focus primarily on confidentiality and integrity, or is availability also included? Protecting highly secret military information can be relevant to a defence organization, but not at all for an industrial environment. And one organization can restrict itself to general guidelines with a lot of

freedom for interpreting them, while another organization might want to specify the choice of measures in much more detail.
In many cases, the focus is aimed at a differentiation of those requirements from the information security policy that have to be implemented one way or another in the ICT environment or the corresponding organization and processes.
Security interests from business and legislation form the most important input for the security architecture, but interests not related to security from the general ICT architecture can also influence a security architecture greatly.

Target groups

A security architecture is actually an aid to communicating the security interests of the stakeholders in a structured and coherent way to the parties that must give a practical interpretation of them. But it can also improve the communication and the insight between stakeholders.
If it is to serve as a means of communication, it is important for concepts to be defined unambiguously and clearly for the different target groups. The coherence of the concepts provides a context for the users of the architecture.
Figure 1 shows diagrammatically how the interests of different stakeholders are combined, translated into principles and clustered so that they form a useful input for architects and designers of different aspect fields.

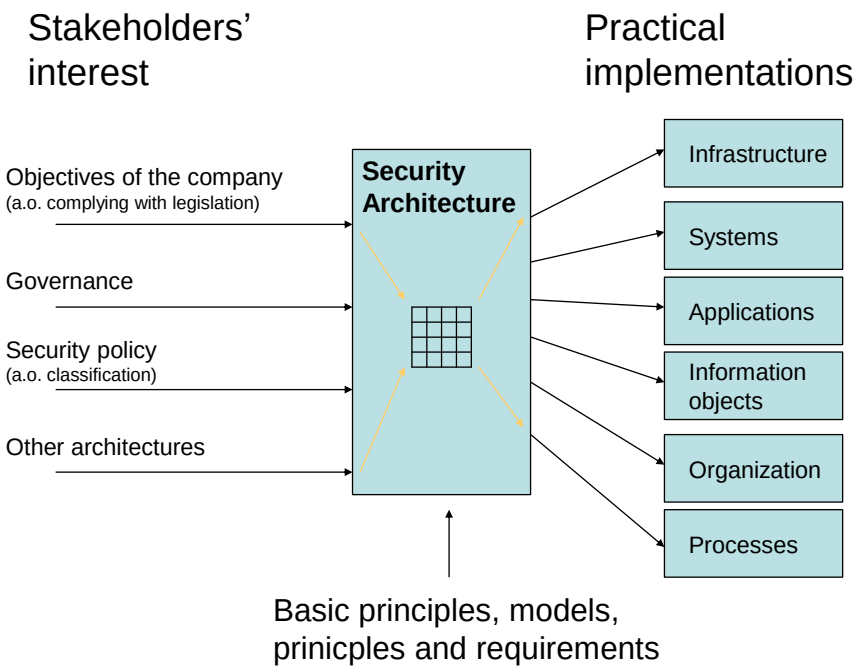

Figure 1 The position of a security architecture

The stakeholders and users (target groups) of an architecture must be properly distinguished from each other. Stakeholders are those people who want their (business) interests processed in the architecture and they generally take care of the funding, while the users have to use the architecture to realize something with it. Stakeholders can indirectly also be users.

The major target groups are:

Primary target groups	
(ICT) Architects	They need the security principles to be able to define the correct building blocks at the right places with high-level security requirements.
Designers	They need the security principles to design building blocks and services in accordance with those principles in the context of the security architecture.
Security specialists	They use the architecture to give the organization consistent advice on security requirements that services and systems have to satisfy.
Secondary target groups include:	
Business managers	They fund the security, make the requirements and from the architecture can understand the main lines of how their business information will be protected. By working in a structured way in accordance with a security architecture they can better account for working systematically on proper protection of company data and information-processing systems.
Auditors	They can use the architecture as a testing instrument during their checks.

Depending on the organization, other specific target groups can also be identified, such as external supervisors.
It is important to make and articulate the structure of the security architecture such that any target group can access and understand it. One way of achieving this is creating views for the different stakeholders and target groups.

Security architecture in relation to other architectures

Is a security architecture a separate architecture in a separate document alongside other architectures? It can be, but it doesn't have to be. Essentially it is a view on the underlying business, information, application and technical architectures. Security aspects can be represented in a separate document, but they can also be described in each of the underlying architectures. Nor is the precise interpretation and division into architecture domains or their complete interpretation of essential importance. What is important, is that the whole fits together, thus guaranteeing the traceability from basic principles and requirements to measures.

Figure 2 shows this in diagram form.

6

Security Architecture in relation to other architectures

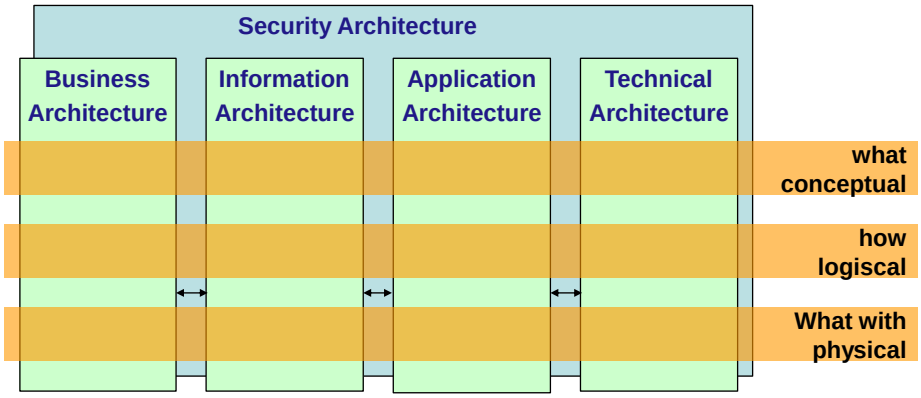

Figure 2 Relationship with other architectures

One advantage of establishing a security architecture as a separate architecture is that the overview and connection between all starting points, models, principles, choices and measures are better highlighted.

THE BUSINESS CASE

What criteria form the basis for an organization to decide whether it wants to develop a security architecture? Can we identify specific conditions and preconditions that determine this?

General advantages of working under an architecture include the control of complexity, cost-saving and the creation of uniformity/standardization. These advantages apply just as much to a security architecture. But the question is whether the advantages of working under an architecture are significant enough to warrant the investment. And how do you calculate that?

The quantitative approach

You can estimate the costs of developing a security architecture reasonably accurately, but it's much harder to estimate the benefits. Benefits can include cost-saving, for instance due to:

- 'Reinventing the wheel' less often in requirements-specifications procedures. Applying the guidelines of a security architecture can save considerable time in projects.
- Once-only setup and good reuse of generic building blocks. This can reduce the size and complexity of individual projects.

- Realization of new services faster and with less effort. Flexibility and time-to-market of new products and services are becoming increasingly important and can deliver business advantages.
- Limitation of destruction of capital through imbalanced and incompatible measures. An imbalance of measures can result in high costs and still provide insufficient security.
- Realizing a more uniform and better demonstrable level of security.

Many benefits are, however, hidden benefits, difficult to make visible. In addition, an impediment within the discipline of information security is that almost no key figures are available to indicate the extent to which cost savings can be realized quantitatively. The costs of specific security measures in ICT environments and processes are also often obscure, making it difficult to identify the savings there.

The availability of reliable starting data for a business case depends partly on the level of maturity of an organization. After all, as an organization controls its processes better, more detailed and reliable measurement data will become available about the costs and possible savings.
If an organization is continually incurring expenses for ad-hoc solutions to cope with security problems, it should consider whether investing in a security architecture might not recover those costs quite quickly.

We can conclude, on the basis of the savings mentioned, that working with a security architecture has advantages for an organization as a whole, but not by definition for each individual project or system.
That is why a security architecture may not have a noncommittal character. Without a certain degree of obligation, the intended advantages of working under an architecture will not be reached, or only to a limited extent. It is important that this is communicated properly to all target groups. Higher management must also support this.

The qualitative approach
Experience teaches us that decisions about developing a security architecture are seldom made on the basis of purely economic reasons. It is much more important whether an influential stakeholder is present with a clear point of view and the conviction that working under an architecture is important.
This conviction can be based on previous experience or good advice, but it can also simply be inspired by the fact that sector colleagues also do it, or because it is a new trend you don’t want to miss out on.
The view that the organization will be safer by choosing a structured approach can also be an important motivation.

An organization with a low level of maturity often has little historical information available about project costs. In that case, the presence of an influential stakeholder is almost always the decisive factor in a decision to develop a security architecture.
In more mature organizations, a stakeholder can use a cost/benefit analysis to further support the conviction he already had.
We can conclude that having an influential stakeholder with a clear point of view and conviction, as well as the presence of a general architecture approach for ICT is more important than having balanced ROI calculations.

A security architecture is rarely the first architecture an organization will develop. If the trend for working in accordance with architecture principles has already been set, a decision to develop a security architecture as well will be taken more easily.
Specifically in the field of security, the need for a 'translation' of business needs and policy into concrete measures is greater than for functional specifications. The reason is that security is mainly seen as a non-functional quality aspect, and many people do not know enough about it. Business managers also often find it difficult to put their security demands and wishes into concrete terms and to indicate which legislation is important.
This need for a 'translation of policy' is not recognized in many cases by the stakeholders, who can also often be the budget holders. Furthermore, business managers often don't have enough understanding of what security can contribute to their result, and they are not held accountable for it either.

The advantages of having a security architecture depend on the complexity and organization of the ICT environment. The more complex this environment is, the greater the need will be to reduce the complexity. In the case of a highly distributed environment where it's difficult to obtain an overall picture, acknowledging clear principles and conditions is more important than in a simple environment.

Preconditions
Figure 1 mentions a number of sources that should provide the starting points for the security architecture. It is an important condition of laying down a good security architecture that the information from these sources is available. If the objectives and responsibilities are not clear, it is difficult to develop a meaningful security architecture.

- The objectives of the organization must be clear, as must the risk profile the organization chooses. After all, the degree of security must correspond to the value of the information and risks that the organization wants to take and is permitted to take. This risk profile is determined on the one hand by the organization's business model, and on the other hand by the threats and legislation applicable to the sector the organization is active in. Sometimes it is difficult to establish an unequivocal risk profile because different divisions of the one organization can have diverging interests and operate in different market segments.
- The organization must have a clear governance structure with clearly defined responsibilities. The depth of detail with which a security architecture can be worked out can be strongly influenced, for instance by the freedom enjoyed by decentralized organization divisions for making their own independent decisions.
- The organization must have a security policy that clearly sets out the basic principles for information security. The classification of information forms an essential element in that policy, so that security requirements can be differentiated according to classification group. After all, the costs of the measures to be taken and the burden of any extra measures have to be matched to the potential business risks that are encountered by each classification group.

> Classifications are often based on current levels of confidentiality, such as public, exclusively for internal use, confidential and secret, but they can also concern special properties such as medical secret. In addition, classifications can be defined for integrity and availability.

- Basic principles from other architectures, such as a general ICT architecture, can help determine which risks are relevant. An organization that provides its employees with laptops and portable media such as USB sticks and CDs to achieve flexibility and mobility runs different risks to those of an organization where the employees only have ‘dumb’ terminals at their disposal.

Growth model
If an organization has little experience in working under an architecture or does not want to invest too much in a security architecture, it can choose to create an initial ‘lean and mean’ basic architecture without too much detail. Even just laying down the most important basic principles can help an organization a long way in the right direction. The architecture can be given more depth at a later stage, or specific aspects can be added.
A security architecture can only be called such if basic quality requirements are fulfilled. You can judge the quality of a security architecture by the degree to which it fulfils the following aspects: an architecture must offer a total view, it must be transparent and balanced, and it must indicate the coherence in a clear manner.

SCOPE AND CONTENTS

Once you have decided to develop a security architecture, the question arises of what it should and should not contain. In other words: what are the scope and the contents?
And is there an unambiguous minimum list of the aspects that belong in a security architecture, and those that are ‘nice to have’? Are there critical success factors that turn a security architecture into an instrument that is useful or not useful?

Scope

One of the first aspects that must be established is the scope of a security architecture. You can use the following questions as a basis for determining the scope:

- Which security aspects do you include or leave out? Is it just about confidentiality, or do integrity and availability have to be included as well?
- Does physical security have to be included in its entirety, or only those matters that directly relate to the provision of information?
- How complex is the environment for which the security principles are to be determined, and which level of detail is desired? Will you decide for instance to remain at a high level of abstraction and only establish basic principles, so that divisions of the organization have a lot of room to fill in the rest (reference architecture), or do you choose a more specific architecture?

  For example, a large multinational with widely diverging divisions can choose only to describe how the divisions are to be linked to each other and how they should communicate, without laying down any details about how the divisions arrange this within their own ranks. In that case, the divisions must make their own more division-specific interpretation of the security architecture within the principles of the reference architecture.

Figure 3 shows this again in diagram form.

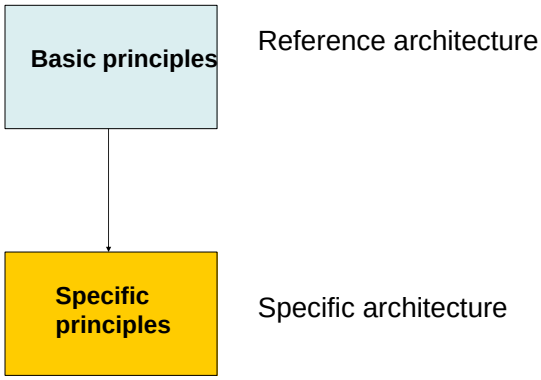

Figure 3 Architecture at different levels

- Which target groups is the architecture intended for? Is it enough to go as far as the logical architecture, or would it be desirable to prescribe choices for the physical layer as well? Designers often feel the need to make the architecture 'as concrete as possible'.
- Should only a blueprint of the target (SOLL) situation be described, or should a transition from the actual (IST) situation to the target (SOLL) situation be taken into consideration?

What comprises a security architecture?

There are various models for describing architectures, such as the Zachmann model, the TOGAF model from the Open Group, and the Integrated Architecture Framework. Models specific to security include the SABSA model, which is actually a security specialization of the Zachmann model, and the Enterprise Security Architecture from the Network Applications Consortium. Both these models also comprise process models for coming to a security architecture and maintaining it.

Although security architecture models differ, they are all layered to a certain degree. As explained earlier, how the different, related architectures are described or delineated precisely is not of essential importance.

What is important is to distinguish 4 layers:

- a business (context) layer,
- a conceptual layer,
- a logical layer, and
- a physical layer.

The business layer

The business layer describes the basic assumptions, starting principles and beliefs derived from the organization's mission, values and standards and governance principles. Furthermore, it describes in general lines the organization-specific business principles, business opportunities, compliance requirements, the legislation in force and threats that have been recognized for the specific business. Threats vary widely, depending on the location or

zone where information is processed, the nature of the business and the value of the information. That makes it sensible to specify the threats to certain environments and to the different kinds of business processes that an organization has.

The contents of the business layer are strongly related to the information security policy. After all, the information security policy is taken over as a starting point in the security architecture.
Drawing good dividing lines between what should be in the policy and what should be in the architecture is essential. Responsibilities and the required controls must be specified in the policy. The security architecture gives a structured interpretation of the policy. If it emerges that policy statements are missing when the security architecture is being drawn up, making it impossible for the architecture to interpret the policy correctly, it is better not to specify those policy statements in the architecture but add them to the information security policy. Establishing policy is, after all, not a competence of the architect.

The conceptual layer
Based on the information and value object classification defined in the policy, this layer describes models and concepts with information structures, flows and objects. The security principles and security norms for this information must be indicated for each classification. An adequate classification and a clear distinction between levels of measures per classification are an essential element of a security architecture. After all, not all the information and all the objects have to be protected the same way. The degree of protection depends on the required levels of confidentiality, integrity and availability. Classifying the information makes a first basic selection of the measures needed for adequate security.

The logical layer
Within the architecture, the logical layer provides a structured description of the controls needed for different aspect areas. What needs to be indicated are the controls required, where which controls must be deployed, under which conditions, who is responsible for management of the controls, etc. It is desirable to group the security controls into aspect areas.
Examples of these areas include:

- Identification and authentication (how you identify who someone is).
- Authorization (what someone is permitted to do and how this is managed in rough outline).
- Encryption (when and where should information be encrypted).
- Isolation (which zones or sub systems are distinguished and which controls must be implemented on the interfaces).
- Management (which issues must be arranged centrally and which ones decentrally).
- Logging and monitoring (what should be registered and how can this information be used usefully).

The logical layer does not yet specify which technical means are required, but does specify what they must satisfy on a functional and qualitative level. For instance, you can describe when strong authentication is necessary, requiring knowledge as well as a form of ownership, and when weak authentication is sufficient, where only knowledge is required. The technical means to realize strong authentication are not specified here. That is something for the physical layer.

With all these matters you must also weigh up the requirements with respect to ease of use for the users, and which measures can reasonably be expected of a customer or partner.
It is important to indicate the coherence of principles and measures clearly, so it becomes obvious how the whole offers the desired protection.

Users of the architecture can use this overview as a basis for determining which aspects need interpreting within their area of responsibility and which aspects should be filled in by other sub areas. Obviously this requires good demarcation of the areas of responsibility.

Many security architectures go no further than the logical layer, because the functional description of security controls is often sufficient as input for drawing up requirements. This applies to internal projects as well as to systems or services to be acquired externally. In the latter case, a functional description with conditions of connection of the security functions in an RFI or RFP is usually sufficient. The choice of physical implementation can be left to the supplier.

In the logical layer, you can make a further distinction between applications and infrastructures. However, with the increasing 'middleware', it is becoming increasingly difficult to draw this dividing line.

The physical layer
Sometimes there are reasons to define the implementation of logical functions more specifically as well, from a viewpoint of cost-saving through standardization or required interoperability, for instance. Thus an organization may want to implement a special choice of strong authentication, or requires specifically that only certain approved encryption algorithms are to be used. These matters can be described in the physical layer. The risk of too much depth and detail in a security architecture is that it can be experienced as a bureaucratic obstacle and not as a useful aid. The more detailed and large an architecture becomes, the greater the chance that users won't always have the time or the motivation to take in its important aspects.
Changes in technological possibilities must also be examined regularly for their impact on the security architecture.

Detailed definition

Is risk analysis part of the security architecture?
Risk analysis is a process performed in different places in development paths and operational processes. Before a security architecture is drawn up, it is desirable to set down the main outline of the threat profile for the organization. The architecture must show how processes and systems are to be protected against these threats. Principles must be written as much as possible in terms of stability of processes and systems (preventing malfunctions) and not in terms of measures against specific threats. Threats change faster than the update cycle of an architecture (generally 3 to 5 years), and the architecture must also offer protection against new threats.

One important reason for working with classifications is that you don't have to do complete risk analyses every time. When you work out the measures per classification, the main features of the risks are included implicitly.
In an implementation path it can be necessary to perform more detailed risk analyses, for instance to determine the most suitable physical implementation of a logical function. The

architecture primarily offers a set of principles and measures that have to be filled out in more detail.

We can conclude that risk analysis of the main lines is necessary for the definition of a security architecture, but that performing a risk analysis for a specific situation is not a part of a security architecture. Having a security architecture can make risk analysis simpler.

When is a security architecture good enough?
As we explained earlier in this article, working out a security architecture depends largely on the objective, the target group and the scope of the architecture.
Good acceptance means the security architecture must be usable for the target groups. Definitions must be unambiguous and the language must suit the needs of the target groups. There must be a 'view' for each target group.
Furthermore, the architecture must satisfy the quality requirements mentioned earlier.
The size and depth of an architecture depend greatly on the complexity of the business and (ICT) environment and the need of the target groups to reduce the complexity down to manageable models and principles.

The justification of principles and traceability from the information security policy are important to the insight of the user into the whole of the security architecture. For that matter, not every user is equally interested in this. A designer who simply has to implement the security measures for an application design will often be less interested in the why and the justification of the principles than an architect who must understand the connection of security principles with other architecture principles in order to make the specific choices.

Can you make a security architecture without knowing the other architectures?
Theoretically you could draw up a security architecture without knowing the underlying business, information, application and technical architecture and the risk profile, but it wouldn't be cost-effective and it would result in unnecessary work. Quite soon, too many principles would have to be described because something has to be written down about the many possible scenarios. That can make the security architecture very big and less accessible to those people who have to work with it.

This actually also answers the question of whether it is possible to make a generic 'blueprint' of a security architecture that could be applied to a large variety of organizations. Preferably not!

It is possible to make an architecture 'proposal', without knowing the business and information layers precisely. By making assumptions or basing your work on basic models related to these layers, you can make an architecture oriented toward infrastructure. This can be a useful choice for large multi-nationals with business units that operate in markets that differ greatly. In that case, it is not possible to trace measures from the business requirements, making it uncertain whether the architecture offers enough to hold on to.

Which architecture models are usable?

Different architecture models have already been mentioned above, each with their own pros and cons.
A good model is important for identifying the elements necessary for a security architecture in a structured way. However, you can also use elements from different models.

The expert group has not been able to form any strong opinion about the pros and cons of the models mentioned, and which model would be the most suitable in which situation.

CONCLUSIONS AND FOLLOW-UP

The expert group was able to find answers to many of the questions posed.
We gave a definition of security architecture and described the main lines of the contents. We also indicated what was important for coming to the decision of developing a security architecture. This decision won't be made quickly on the basis of just one hard business case with costs and benefits. It is more important to find influential stakeholders with a vision for working under an architecture.

One general conclusion is that a security architecture is useful as a means of communication and contributes to better insight into the security requirements for parts of the ICT environment and the organization. A security architecture can also provide better insight into the balance and consistency of the information security of the entire organization and can contribute to setting up new (business) services in a more flexible and faster way.
The degree to which these advantages are expressed depends on various factors, including the complexity of the ICT environment (and therefore the need to reduce that), the business risks, the dynamics of an organization, etc.

Critical success factors for developing a security architecture are having a policy and a classification system for security, the usability for the target groups and the experience that having a security architecture reduces the complexity and can realize better security.
Drawing up a generically applicable 'blueprint' of a security architecture does not appear to be practically feasible. Security architectures can be filled out in very different ways, depending on the objective and scope.

The questions of how you develop a security architecture and how you guarantee that a security architecture will be used effectively and consistently have not been answered sufficiently.
The expert group will attempt to answer these questions in a follow-up session. The expert group is keen to know if this expert letter had added value for you, and is happy to receive your comments.
You can send your reactions to expertbrief@pvib.nl. Even if you valued this expert letter, we always appreciate an e-mail!

LITERATURE

The workgroup consulted the following literature in creating this expert letter:

Aaldert Hofman, *Inbouwen in plaats van aanbouwen, Informatie May 2004*

Win Sonnemans and Renato Kuiper, *Beveiligingsarchitectuur ICT, Openbare orde en veiligheid. ITSMF seminar 14 September 2005, www.itsmf.nl*

Network Application Consortium, Enterprise Security Architecture, A Framework and Template for Policy-Driven Security , 2004, http://www.netapps.org

Lucien Bongers, *Security binnen enterprise architecture. Radboud Universiteit Nijmegen, 10 February 2006.*

John Sherwood, Andrew Clark, David Lynas, *Enterprise Security Architecture, A Business-Driven Approach, 2005. Uitgeverij CMPBooks, ISBN 1-57820-318-X*

John Sherwood, Enterprise Security Architecture, SABSA, September 2003. www.sherwoodassociates.co.uk

Henny van de Pavert, *Security architecture Rabo groep. ISF O&G Chapter meeting 23 May 2005.*

Renato Kuiper, *Architecten debat, 21 June 2006, PI/GvIB theme afternoon. www.pi4ib.nl*

Nico Visser and Renato Kuiper, *Artikelen serie Beveiliging bouwen onder architectuur. Informatiebeveiliging number 7,8-2002 and number 1 of 2003, www.pvib.nl*

Leo van Koppen, *Ontwikkeling van een security architectuur voor de Haagse School. MSIT thesis* TIAS Business School Eindhoven, 2005.

Network Applications Consortium, *Enterprise Security Architecture, a framework and template for policy-driven security, 2004*

Open Group, *The Open Group Architecture Framework (TOGAF)*

Sherwood Associated Limited, *SABSA (Sherwood Applied Business Security Architecture)*