

Security Report



SECURITY IN THE **DIGITAL WORLD**

© Copyright 2003 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® and SQL Server® are registered trademarks of Microsoft Corporation.

IBM®, DB2®, DB2 Universal Database, OS/2®, Parallel Sysplex®, MVS/ESA, AIX®, S/390®, AS/400®, OS/390®, OS/400®, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere®, Netfinity®, Tivoli®, Informix and Informix® Dynamic Server™ are trademarks of IBM Corporation in USA and/or other countries.

ORACLE® is a registered trademark of ORACLE Corporation.

UNIX®, X/Open®, OSF/1®, and Motif® are registered trademarks of the Open Group.

Citrix®, the Citrix logo, ICA®, Program Neighborhood®, MetaFrame®, WinFrame®, VideoFrame®, MultiWin® and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc.

HTML, DHTML, XML, XHTML are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

JAVA® is a registered trademark of Sun Microsystems, Inc.

JAVASCRIPT® is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MarketSet and Enterprise Buyer are jointly owned trademarks of SAP AG and Commerce One.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies.

CONTENTS

Security in the Digital World	4
Management Summary	4
Preliminary Remarks	4
Objective of This Report	4
How Great is Security in the Digital World Today?	5
– The Four Levels of Security	5
– Security Awareness	7
– Security and Forms of Organization	8
– Implications of New Information Technology	9
Best Practices – How Can You Improve Security?	11
– Understanding the Business Case for Security Measures	11
– Security as a Quality	12
– Auditing and Risk Management	15
– Regulation vs. Deregulation	17
– Data Protection and Privacy	17
– Education and Training	18
Conclusion	18

SECURITY IN THE DIGITAL WORLD

MANAGEMENT SUMMARY

The topic of security in the digital world is a complex one. Although security concerns us all, the issue is often characterized by a general lack of awareness. New, cross-company business processes demand new security concepts to support them. The information technology market will favor application vendors who take security seriously as a quality characteristic. The main responsibilities for businesses implementing these solutions are to promote awareness among all those working with the solutions and to define clear areas of responsibility for improving security in operational areas. Regulations should be applied where protection of individuals is necessary, and large enterprises should be enabled to help themselves.

PRELIMINARY REMARKS

This report on security in the digital world was compiled at SAP AG, the world's largest vendor of enterprise management software. As of January 2003, SAP had some 28,000 staff, around 19,000 customers in industries ranging from apparel to military technology, and an installed base of more than 60,000 live systems. More than 60% of the global top 500 companies use SAP software to model and execute their critical business processes. SAP itself has become a multinational corporation, with development and support centers spanning the globe. Accordingly, security is one of the most important issues within SAP itself.

The author of this report is head of product management for security at SAP and, in this function, is primarily responsible for the security of the software SAP develops. In addition to product management for the security functions of SAP technology, which forms the foundation for all SAP business applications, the author is also responsible for defining the requirements for secure application development at SAP, in addition to driving the resolution of critical security issues in SAP software. The author is also involved in internal security management at SAP, so that SAP – as a “client” – also benefits from his experience.

This report represents a summary of observations that the author has made with a wide variety of SAP customers. Accordingly, the results – even though they are not based on a scientific survey – are broadly representative. These results have already been presented to a working group of the German federal government, where they will find consideration in the further activities of the legislature's “Security in the Internet” initiative.

OBJECTIVE OF THIS REPORT

Although IT security is the top subject of debate for IT-related issues, it alone is not a panacea for all security problems. The objective of this report is to illustrate the extent to which modern information technology and the processes implemented in modern software can be considered to be secure. It is not a collection of statistics on the use of security products, nor of discovered weaknesses or perpetrated attacks; such figures are available in many different publications. Deserving of particular mention are the annual U.S. survey conducted by the Computer Security Institute (CSI), www.gocsi.com, as well as the annual study of the GAS¹ countries carried out by KES Magazine (www.kes.de), both of which conduct detailed surveys of this nature.

Instead, this paper aims to draw a full picture of security issues in electronic data processing and to show which types of security have evolved in which areas; it also does its best to explain how and why such evolution has taken place.

In addition, this paper also investigates various options – currently the subject of much public debate – for increasing security. Its results are intended to empower decision-makers to determine the direction in which they intend to proceed. Its findings apply equally to the upper management of multinational corporations, general managers of small businesses, politicians, and ordinary citizens.

1) Germany Austria Switzerland

HOW GREAT IS SECURITY IN THE DIGITAL WORLD TODAY?

Security is a multifaceted, many layered issue. It begins with a single password and culminates in integrated risk management. The technology that has to be made “secure” includes components from every relevant IT area – including network infrastructure components, front-end technology, operating systems and e-business software. But security can also be seen to begin with the installation of an operating system and culminate in an internal or external audit of critical systems. Security can be voluntary – that is, strictly for business purposes – or mandatory, required by law. In short, security is a complex issue that permeates every aspect of modern life. The Gartner Group has developed the following definition of security² :

Security is achieved by a balanced focus on three factors: people, processes and technology. It can't be attained by focusing on any one of these factors to the exclusion of the others.

Any enterprise that wants to make significant improvements in security must take a broad view of its information assets and understand their value, and the threats and vulnerabilities to and of these assets. It's very easy for an enterprise to focus on countermeasures that address a specific, topical risk – for example, physical attacks by recently terminated employees – to the detriment of overall security. At best, such initiatives can divert resources; at worst, they can create a false level of confidence or even introduce new vulnerabilities. In short: an enterprise must not lose sight of the big picture.

Information technology is a key enabler for all enterprises, and successfully and securely implementing new technology is crucial to e-business and the net-liberated organization.

In other words, security can only be achieved by looking at the big picture. Accordingly, the detailed information provided in this paper must always be understood within the overall context; individual issues can never be completely isolated.

Security has many different levels. When different groups talk about security, each of them has a “different” security in mind. Roughly speaking, the following divisions can be defined:

- IT risk management: Security for managers
- Software security: Security for software vendors and users
- IT security: Security for network and system administrators
- Information security: Security for security managers

Each of these four levels is examined in detail below.

Moreover, this paper also examines the issue of security – and its four levels – from different perspectives:

- Awareness of security
- Security and enterprise structures
- Security implications of new technology

These different perspectives will enable you to appreciate the individual factors that are critical to understanding the big picture. In particular, combining these perspectives with the four levels defined above results in interesting observations that will help you comprehend the overall subject of “security in the digital world”.

The Four Levels of Security

We can distinguish between four different levels of security. These levels evolved into their current forms many years ago and have grown independently of one another ever since. Each area has its specializations and its own “community”. Very few people manage to bridge the divides between these specializations. Consequently, only very few people comprehend the big picture of how these different issues fit together to form a global context.

2) Source: Gartner Group

Each of these four levels is dedicated to, and largely defined by, a different target group, which has led to the perception and implementation of security differing from one group to another. The levels are arranged from the top down, from business processes down to individual items of information.

IT RISK MANAGEMENT

Managers feel secure when they can tame known risks. So when it comes to electronically modeled business processes, they feel secure when they can master the corresponding risks. IT risk management is a relatively new area, one that is promoted primarily by internal and external auditors. The main characteristic of IT risk management, in contrast to the other levels, is the immediate questions “What will it cost?”, “What will it do?”, and “Can I get the same results for less money?” There is an alternative interpretation, however, that defines the risk of violating certain safety or security regulations (such as FDA requirements of pharmaceuticals companies, data protection laws, and so on) as part of IT risk management, although security in itself is not the immediate purpose. Most members of this community focus on securing fully electronic business processes in integrated systems; the application of IT risk management to a secure e-mail system, for example, is still a fairly rare occurrence. An internationally recognized framework for this area has been defined under the name CoBIT (Control Objectives for Information and related Technology).

SOFTWARE SECURITY

Software security is concerned with security in (standardized) software products. The most visible part of this community focuses on Microsoft products, attempting to discover flaws in the “House of Gates”: primarily weak points in the operating system or server programs, which hackers exploit to wreak havoc or even take control of the targeted platform. Of course, other platforms (Linux, Solaris, and so on) and application programs (MS Word, MS Outlook, Apache Web Server, and so on) also attract their share of attention. To date, this community has only rarely targeted software for modeling electronic

business processes, probably due to the steep learning curve and high expense involved. The less obvious part of this community is attempting to make standard software secure from the start. To do so, good, sustainably “secure” concepts must be developed and implemented in all product components, insecure coding fragments must be removed, and so on. These Common Criteria (CC), which have been enshrined in an ISO standard (ISO 15408), provide a widely recognized international framework for ensuring the security of IT products both in their development and their use.

IT SECURITY

IT security is what most people spontaneously associate with security in the digital world. It involves activities and technologies aimed at achieving basic protection that is present in all applications and processes. The people who best know their way around this area are system administrators and network specialists (reflecting the large overlap between these two groups). It is difficult to imagine a PC/server or network without these essential standard tools: firewalls, anti-virus software, and virtual private networks. A major advantage in contrast to the other levels is that IT security is executed independently of the processes to be implemented; instead, it is a component of the infrastructure. The “Basic Protection Certificate”³ awarded by the German BSI⁴ targets this minimum level of protection.

INFORMATION SECURITY

The security managers at a company – those who are in charge of security – often have a far wider spectrum of responsibilities than just ensuring security in the digital world. Most of them are also responsible for the physical protection of the company. Therefore, it makes sense to extend the issue of data security to the physical world. Consequently, information security is often concerned with the security of information, whether in physical or electronic form. Because the physical protection of information requires the cooperation of staff, security guidelines – only some of which involve information technology to protect data – are developed and enforced.

3) *Grundschutzzertifikat*

4) *Bundesamt für Sicherheit in der Informationstechnologie;*
Federal Office for Security in Information Technology

Certification according to ISO 17799 attests to the effectiveness and implementation of information security guidelines within an enterprise.

The main difference between these four levels is the different objects they protect. The object to be protected ranges from an integrated, business-critical process and its data, to an individual item of information that can be classified as “confidential” (to determine the degree of protection required), but is also to be protected itself, detached from its application. The communities from the four levels apply different methods which themselves are derived from the various objects to be protected. Accordingly, they also have different approaches to the issue of security itself.

The most highly developed area is IT security, which has received the lion’s share of public attention over the past decade. The primary reason for this is the fact that security in this area can be achieved “after the fact”, by installing additional technology. There are limits to this approach, however, as you will read in the section “Implications of New Information Technology”. In my opinion, activities will increasingly focus on the “software security” area in the coming years.

Security Awareness

“Security awareness” refers to a permanent state of mind, in which all activities that involve information technology are undertaken with security in mind. Examples: When you send an e-mail, you automatically ask, “Should I encrypt it?” When you save a confidential document on a server, you think, “Wait a minute, who else has access to it?” If your company wants to join an electronic marketplace, you consider, “What will happen if other companies can see our order data?” Security awareness means looking at things from a different perspective. While there is a tendency in modern, western societies to focus on the positive aspects of an issue – the exciting, promising, inspiring aspects – looking at potential negative aspects is by no means a natural reflex.

MOTIVATION FOR SECURITY AWARENESS

One example: driving a car. From the invention of the first car, it took 20 years to achieve regular speeds of 60 mph, where crashes are almost always fatal. Yet another 80 years later, some people still refuse to fasten their seatbelts. It took the threat of drastic fines to get the general public to buckle up regularly. And even in inclement weather and on congested freeways, tailgating is still a regular occurrence. This example from a non-IT area shows that safety and security are by no means natural instincts. But how can people be persuaded to develop security awareness? The available options are limited:

1. Defining direct, negative consequences: This is the most extreme method and, at the same time, the most effective. It is the basic principle behind penalties to improve behavior, for example, imposing a fine on people caught driving without their seatbelts fastened.
2. Targeted education aimed at developing a feeling for the responsibility that each individual bears and for more security-aware behavior. Much less frequent than option 1, as it requires individuals to go against their natural instincts.
3. Developing intuition for hazards, including those in the IT area. This is fairly rare, as most individuals have lost this intrinsic capability as a result of cultural developments.
4. Some individuals are pessimistic by nature and paranoid where security is concerned.

There are no other options for promoting the development of security awareness. Option 1 is not very appropriate for improving or promoting security awareness among employees or the general public, as the intentional precipitation of calamities – along with the threat of draconian punishment – is morally reprehensible. Because options 3 and 4 are immune to external influence, only option 2 remains, which makes education the only practical method for actively promoting security awareness. Yet education is a difficult, lengthy process.

THE CURRENT SITUATION

With regard to the four security levels, the current situation can be described as follows:

- **IT risk management:** Awareness is fairly well developed among top-level managers; many have the intuition described in option 3. However, many of them perceive the danger as too abstract (“attack from the Internet”), or too far-fetched, to initiate any specific protective measures. Top-level managers thus tend to deny the existence of such hazards because they are not readily perceivable. If anything, they tend to underestimate the gravity of the risk involved. This results in the paradoxical situation that, although the awareness is there, conduct is not commensurate with the risks involved. Although security is considered to be the most important issue, funds are spent elsewhere.
- **Software security:** Awareness of software security is partially present, but is ignored in the very places where immense personal benefits can result. IT experts are very aware of the risks involved in opening one’s home PC to Internet access. The average surfer, on the other hand, appears to be largely uninformed. There have been too few serious occurrences and too little education. Aside from the few industry leaders (Microsoft, IBM, Oracle, SAP), awareness is also sorely lacking on the software vendor side. Yet even when vendors make corresponding security patches available, customers often fail to implement the updates (“too much effort involved”, “if it ain’t broke, don’t fix it”, and so on).
- **IT security:** Awareness is greatest in the IT security area. The people employed in this area have frequently either encountered the negative consequences first-hand (reinstalling a mail server, protecting Web servers, installing operating system patches) or were fervent security disciples in the first place. An outsourcing market has arisen for this area which has significantly reduced global risk.
- **Information security:** In the information security area, security managers have a high awareness level (improving security is their job, after all). Their charges, however – ordinary employees – tend not to. Employees frequently perceive security measures as obstacles, as restrictions on their

personal productivity. Therefore, it is tremendously important to promote enterprise-wide security awareness through special events, providing negative examples, and so on.

All in all, awareness is generally low. It is strongest among top-level managers (if somewhat displaced) and IT security specialists. Software security must continue to be demanded and promoted (see also the section “Security as a Quality”). General awareness of information security issues among employees and the population in general is still much too weak. Both company-internal and public programs and campaigns are required to promote risk education.

Security and Forms of Organization

THE STRATEGIC DILEMMA

Many companies suffer from a strategic dilemma that stems from the legacy separation of the different security levels. Simply put, the situation that blocks critical decisions in the security area is that the CFO⁵ is responsible for risk management, while the CIO⁶ is responsible for (IT) security. Consequently, the CIO has a handle on security in his or her areas of responsibility (usually infrastructure services and office/workgroup applications), yet there is no integration with the business systems (which are usually allocated to the user departments) and their security requirements (which are defined by the internal auditors, who answer to the CFO). As a result, infrastructure security is frequently well implemented (with firewalls and VPNs⁷), but security measures for the e-business systems – for automatic supply chain integration, for example – are implemented sparingly, if at all, because responsibility for the security measures has not been clarified.

And why not? Most likely for historical reasons. The levels “risk management” and “IT security” have their defined areas of responsibility, but who is responsible for the security of the business systems themselves? Ideally, software security. But this is still a fairly new concept. In the not-too-distant past, perimeter security – the separation of the “benign” internal network from the “evil” Internet – was the de facto security

5) Chief Financial Officer

6) Chief Information Officer

7) Virtual Private Networks

standard for IT landscapes. Because only a few companies have adapted their structures and areas of responsibility to the modern situation of (and opportunities for) e-business, only a few companies have managed to resolve this dilemma.

LEVELS OF RESPONSIBILITY FOR SECURITY

But why is it so difficult for companies to adapt their security measures when so much advice is available from security experts and management consultants? To answer this question, you have to examine in more detail the areas of responsibility defined within a company. I have identified the following areas of responsibility that are involved in decisions affecting the automatic, software-supported execution of a business process (leaving aside issues involving data protection and auditing).

- Management: Top managers, who are interested in the company's general well-being
- Process owners: Those responsible for a business process, usually in the user department
- Central applications: The operators of the standard software used to implement the processes
- Infrastructure and other technology: The IT department that operates the infrastructure services
- Security services: The IT Security department, which conducts technical audits and penetration tests
- Security consulting: The department (usually outsourced) that develops the security concepts, drafts general action item lists and guidelines, and supports the implementation of new security technology

This list is characterized by the fact that any given area generally only communicates with the areas immediately above and below, but only rarely with groups that are two levels or more distant. As a result, security consulting frequently has the best holistic security concepts, but:

1. Generally has no understanding of the business process involved and
2. Never reaches management.

These factors are essential when automated, cross-company processes are involved.

Further observation shows that security is only seen as a responsibility in the levels "management" to "infrastructure and other technology." In the lower levels, security is perceived as a feature. That is, it is simply expected where necessary, but seldom made an independent issue. Consequently, if security is to be considered at higher levels, it must offer economic benefit – and not only in and of itself (such as firewalls, for example, which protect the company network by definition), but also in the quality of processes in a wider context. Project tests and hard evidence are absolutely essential.

It is therefore clear that, in this common structure, management cannot make decisions regarding the enabling security necessary for e-business. Managers are never even confronted with the decision, and – due to the strategic dilemma – management is the only level that can solve this problem today. The section "Improved Implementation through Organizational Changes" illustrates how this dilemma can be resolved.

Implications of New Information Technology

THE NEW IT: WEB SERVICES

More recent developments in IT systems and concepts for implementing electronic, cross-company business processes have two fundamental new attributes:

- The breaking down of processes into individual, modular, Web-enabled services and
- The standardization of interfaces to utilize these services.

The decisive benefit of componentization, or the breaking down of processes into individual, modular, Web-enabled services is that you can implement the services based on a "best of breed" model, instead of being dependent on a monolithic infrastructure that locks you into a single vendor in the long term. The new model enables you to swap over service implementations at short notice, giving you a permanent gain in flexibility. To achieve this, the corresponding interfaces that address or call the services must be standardized. This means that competing service vendors have to agree on a common syntax and – because a business application is involved – semantics.

The new principle is based on the following tenet: By freeing yourself from rigid, unwieldy procedures and pursuing an open integration strategy, you not only reduce the cost of future software enhancements, but can also exploit new fields of business that were previously closed to you. Because the individual services have been detached from space and time, specialized companies anywhere in the world can now render them. Likewise, you can add value to another company's services by contributing your own company's services. The true full potential of this principle is reached when different companies' services can be spontaneously combined with one another.

The software product families of two vendors are pursuing this very goal: Microsoft and Sun. In the past several years, each of these companies has developed a framework that should make it possible to develop such interoperable Web services quickly and easily. Microsoft's initiative is called .NET and uses the programming languages C# (a further development of C and Visual Basic, not dissimilar to Java), Visual Basic, and any other programming language that can be integrated in Microsoft's Common Language Runtime. On the other side, Sun is promoting its Open Network Environment with a Web server concept called J2EE, under which Java classes have also been standardized for professional server operations. The major difference between Microsoft and Sun is that Microsoft earns its living by selling software, while Sun is more interested in selling its hardware – the servers optimized for J2EE use. Consequently, both companies have profoundly different approaches to intellectual property issues, with the result that Sun has gathered a wide following of software developers while Microsoft is basically on its own. My forecast: J2EE will likely predominate in the tough B2B market, while .NET will probably win consumer-oriented services and the SME⁸ segment. Ultimately, however, the two frameworks should be interoperable, as both claim to implement inter-service communication with Web Service Description Language (WSDL), Simple Object Access Protocol (SOAP) and Universal Description, Discovery and Integration (UDDI).

8) Small and Midsize Enterprises

PORTALS/WEB APPLICATION SERVERS/EXCHANGES

Integration takes place at two different levels: users and processes. User-based integration is implemented through a portal that takes existing services that have been prepared for user interaction, and groups them together in an overall context. Object-oriented data transfer technology enables the user to use different, logically related services in sequence extremely efficiently. Process-oriented integration is implemented through so-called "integration hubs" or "exchange infrastructures" which enable the automated cooperation of services within a company and beyond company boundaries. This integration represents a common, standardized further development of marketplace technology and enterprise application integration (EAI) software.

FROM THE MIDDLE AGES TO MODERN TIMES

The step from monolithic structures to integrated, service-based process implementations is, figuratively speaking, equivalent to the transition from the Middle Ages to modern times. Whereas in the Middle Ages, all essential processes (mainly commerce and administration) took place within a castle, the dawn of modern times saw the formation of a new type of settlement, the city. While the city features a number of small, individual, private homes, commerce and administration take place on public squares and in public buildings. The standardization of a monetary and legal system made this possible.

As far as security is concerned, the question now is how to go from protecting a castle to protecting a city. While security in a castle can largely be ensured by having only one heavily protected entrance, the very definition of the city makes this approach impossible, so new, previously unknown mechanisms must be implemented in order to ensure security. To describe this in more detail, consider what security in a city implies. The security of a city is based on measures that have different objectives, yet similar or even identical execution: protecting the community against external threats and safeguarding internal order. In today's terms, the former objective is guaranteed by the army and the latter by the police, and both

are bound to uphold a defined set of rules (treaties, laws, and so on). The ever-increasing – and entirely intended – permeability of city limits makes it more and more difficult to differentiate between a city’s citizens and non-citizens, at the same time blurring the boundaries between the responsibilities of military and police. The preservation of “order”, regardless of whether internal or external, is now the focus.

The same thing applies to Web services. Because the differentiation between internal and external Web services is becoming less and less significant from a technical standpoint, and because the same questions – such as “What is this service allowed to do?” and “Who is authorized to use this service” – apply to internal and external services alike, there is no longer any reason to differentiate between internal and external services at all, as long as the authorization issues are clarified and the results of authority checks can be generated and safeguarded.

To put it in a nutshell, highly integrated e-business processes have decisively changed the granularity of security requirements: *Instead of perceiving companies as secure fortresses, the individual people and services now have to be protected from one another to maintain “order” in e-business transactions.*

The new technologies have a major influence at two security levels: software security and IT security. While the nature of risk management and information security remains constant (changes merely affect the specific technology implemented), a Web services architecture requires a complete reevaluation of software security. If the standardization that everyone is striving for – to enable secure communication between different vendors’ Web services – fails to be achieved, the software industry will suffer a major setback (which goes some way towards explaining the implosion of the New Economy on global stock markets). By contrast, the new technology will render IT security obsolete in the medium term. This level can either offer more support to software security components and cooperate more intensely, or it will be swallowed by software security – at both the conceptual and organizational level.

BEST PRACTICES – HOW CAN YOU IMPROVE SECURITY?

In addition to the recommendations named in the previous sections, various approaches of a basic nature can be pursued in order to improve security. The following approaches are described in detail below: auditing and risk management, security as a quality, security measures as a business case, and regulation vs. deregulation.

Understanding the Business Case for Security Measures

Security can only be successful when considered as part of the big picture. Because business cases reflect a general attempt to isolate issues, tasks, and problem areas in order to better evaluate their economic value, a business case evaluation of security seems difficult, if not impossible. Hence the common assertion that “security only incurs costs.”

Nonetheless, a business case evaluation is possible if you classify the issues. You can divide the topic into two dimensions:

- Differentiation between short-term and long-term benefit – in other words, the time frame within which an investment in a given measure pays off.
- Differentiation between added value and optimization. Whereas the objective of adding value is to increase revenues, optimization aims to increase profits at the same revenue level by reducing costs.

This results in a two-dimensional breakdown of the various business case types:

	Short term	Long term
Added Value	New business areas (customers, product variants, and so on) resulting in new revenues	Maintaining and augmenting intangible assets
Optimization	Process optimization through automation, reducing the number of process steps, and so on	Risk minimization, preventing or at least limiting long-term damage, such as third-party claims

Different rules apply to the existence of a business case, depending on which category an objective is assigned to. This becomes especially clear when considering security. Normally, the benefits of security will arise on the long-term side, although there are cases where the use of security technology or organizational measures can also help you achieve short-term goals. Under this consideration, security plays more of an “enabling” role in achieving short-term objectives (that is, it represents a supporting element), although it can also have an intrinsic value (in the sense of risk avoidance and conservation of value) on the long-term side.

A few examples of where security can represent a benefit in each category are described below. Of course, the criteria have to be applied to each company individually, as the specific underlying conditions strongly influence the business case.

- New business areas: security as a component of product requirements (when purchasing an enterprise portal, for example), secure programming (use of reliable browser technology), establishing a secure partner network, secure online ordering by customers, and so on
- Intangible assets: corporate governance, digital rights management, intellectual property protection, use of secure e-mail
- Process optimization: identity management, use of digital signatures, Web service security
- Risk minimization: risk management, internal and external audits, intrusion detection, firewalls

These divisions are not always crystal clear. For example, setting up a secure partner network can also be considered to be part of risk management. Therefore, if you intend to draw up a business case for security, it is important to know which of the categories it should apply to. Only then can you find the responsible organizations within the company that will help promote implementation.

Interestingly, it is the long-term business cases that have already been implemented, while the short-term cases (which are popular due to the rapid success they allow) tend to lag behind. In IT risk management, in particular, benefit is largely only seen in long-term security activities. The IT security area is by definition more a long-term security benefit, as it neither helps to optimize processes (or only indirectly, by providing infrastructure such as a virtual private network), nor does it open new business areas. Information security is also long-term, as it is too distant from the processes to support their short-term success. For this reason, only software security can immediately promote short-term success.

Security as a Quality

When you perceive security as a quality component of a solution, things become much easier. In the past (and the present as well, in many companies), security was perceived as a technical service that could be rendered after the fact, and thus as detached from the “regular” process. As a result, security – although encouraged and recognizably important – was always defined as a requirement, in contrast to a benefit that promised personal or corporate gain. In other words, security was largely reduced to the status of a strict cost factor.

THE MARKET FOR SECURITY ADD-ONS

Many vendors of security solutions recognized this situation and, instead of making an effort to seek integration with the applications to be protected, they developed add-on security solutions that appear to make the applications secure. This category includes such critical components as firewalls, anti-virus software, virtual private networks and extranet access management software. Alternatively, it would have been possible to develop secure operating systems, secure e-mail systems, secure networks, and secure Web services in the first place...

From the perspective of vendors and consultants, the advantages of such solutions are clear: it is simple to quantify the costs for security, a seemingly impossible task in the latter case. Yet this approach has a problem that has long lain dormant and is only slowly emerging. Only a certain degree of security can ultimately be achieved; this approach will not lead to secure applications per se.

SECURITY AT APPLICATION LEVEL

Security can only be sensibly provided by – or in close cooperation with – the application itself. From personal experience, I maintain that those add-on solutions for security currently available have reached their apex. That is, even extensive additional investment in this category of technology will fail to produce a major leap in the level of protection provided. A major improvement will not ensue until the applications themselves assume responsibility for security. In reality, however, this transition has only taken place in a few areas (such as specialized ERP systems).

Why haven't mainstream applications generally assumed responsibility for security so far? There is a simple explanation. Security is perceived as a bothersome obligation, a requirement – but not a benefit. Software is generally sold on the promise of optimizing business processes, achieving cost savings or generating new business opportunities. The security of these business processes has a lower priority, the primary focus being on more money (whether earning or saving it). Of course, customers also expect software vendors to attend to their security needs. In turn, vendors try to keep the cost of providing this security as low as possible, either by implementing the bare minimum required to continue selling their products, or by entering into a partnership with a vendor of one of the add-on products listed above, thus relinquishing responsibility for the security of their applications.

SECURITY AS A QUALITY CHARACTERISTIC

Considering the above information, this requirement means that security is of vital importance for the entire software life cycle process for software vendors, from specification through to online support. Especially global companies such as IBM, SAP, and Microsoft must completely transform their product strategies, which in the past have focused on maximum functionality and speed. Microsoft's Bill Gates has announced that security will be more important than new functionality in future. SAP has established a new quality assurance program that is binding for all development departments and all subsidiaries, and security is a component of this program. Only IBM has a more conservative approach: security in IBM products will continue to be provided by the infrastructure (primarily Tivoli products).

Security as a quality characteristic is particularly important in the software life cycle process. Secure default installation, automatic security updates, and secure software change management processes are major requirements for today's software industry, which is mainly focused on producing as much functionality as possible.

How will this landscape change – with regard to the new, open, integration-friendly IT architecture – under the pressures of further development?

My predictions:

1. Fewer and fewer companies will be capable of implementing the necessary security requirements themselves, due to the high costs involved. Likewise, companies that neither possess this knowledge themselves nor can depend on reliable partners will vanish from the market, because insecure Web services will not be marketable in the long term. Potential partners include sufficiently equipped software vendors or ASPs⁹ that consolidate security expertise for several clients.

9) Application Service Providers

2. Consulting firms will be expected to sell security as part of their product as a matter of course; those firms that ignore this demand will cease to exist. Especially during the upcoming migration phase, until the necessary software vendors and ASPs have established themselves, these consultants will receive a major slice of the project pie.
3. Application vendors who do not involve security in their products from the beginning will vanish, because the cost of subsequent integration is too high.
4. The market for security software will consolidate. Specialized companies will either seek integration/partnership with the application developers or will largely vanish from the market.

This will be true especially for software companies targeting the end user and small and midsize businesses. In these market segments, there is little or no extra money for add-on products or additional services. Only complete solutions including the required security mechanisms will be successful. For example, the use of digital signatures within applications is mainly requested by companies in the SMB market, whereas large companies are prepared to buy add-on products.

AREAS OF RESPONSIBILITY FOR PROJECTS

Where security is truly a core requirement of a specific project (for a bank, for example), there are three different options for achieving this goal:

- A vendor exists who can offer truly secure applications
- One of the vendor's upstream project partners can provide the necessary expertise
- The customer has the skills required to build secure applications from the modules provided

In the second case, specialized consulting firms provide both the project expertise and security expertise. As an immediate consequence, however, the customer has a long-term tie to the project partner, who in turn can point out deficiencies in the

vendor's applications and then sell the solution to these problems as a further project. The risk of an indeterminate cost spiral ensues. This is the most widespread variant today. Consulting firms such as PriceWaterhouseCoopers, Deloitte&Touche, and Accenture have specialized in this solution approach, due not least to their experience with audit projects.

The last solution is currently the most successful, as well as the most expensive. The customer is in charge of the requirements and their successful realization, has drafted strict security guidelines, and implements them consistently in the project. The demands on the product vendors are correspondingly high, as they have to implement the requirements perform, generally ad hoc, without any strategic integration in their product plans. By its nature, this approach is limited to very large enterprises and organizations. Moreover, these parties are frequently concentrated in just a few industry sectors that already associate data security with business value, even without a Web services architecture: banks, pharmaceuticals manufacturers and governments (for example, the German "Bund Online 2005" project demands across-the-board support of digital signatures for binding transactions; the supplying software vendors are responsible for implementing the corresponding requirements).

If the first case were available, it would surely be the fastest way for customers to achieve their goals. Because the application itself already features the necessary security measures and the application vendor has likely trained its field organization in their use, this approach should be the least painful way for customers to implement secure applications. The question is, do such application vendors exist? SAP is taking initial steps in this direction, and Microsoft has also recognized their necessity – but by no means has security thoroughly penetrated the available applications in general.

Therefore, my recommendation is to demand security as a quality factor in your decisions for projects and software products.

Auditing and Risk Management

An audit is the supreme test of secure solutions and applications. Only if the audit confirms that the implemented processes do not pose a risk to an enterprise's finances can the solution be considered "secure" from an economic perspective. What does an auditable solution look like? It is a solution where auditors can prove the existence of specific security characteristics. A traditional example from the ERP environment is the segregation of duties, or division of responsibilities. This tenet demands that subtasks that could be critical to a company if they were performed by the same person (such as placing and approving orders, for example) cannot be assigned to the same person, or that the auditors can at least prove that none of these critical authorization combinations exist.

Finding proof that none of these critical combinations exist in an ERP system that has been configured and customized for a specific customer is a major component of auditing a system. Similarly, taking the example of online marketplaces, you could demand proof that no other companies in a given marketplace have access to your company's order data.

In this approach, the security of the application has to be as independent as possible from the security of the infrastructure; otherwise the infrastructure risks can directly and indirectly impact the security of the application.

RISK MANAGEMENT INSTEAD OF RISK AVOIDANCE

The measures required to prove security can be infinitely complex, as the above examples show. As a result, many companies – especially smaller ones – perform only few of these tests, if any. Yet even large corporations have a certain

amount of room to maneuver in conforming to the German Corporate Governance Code (KonTraG). The defined objective of the KonTraG is to contain risks, not to avoid them completely.

These risks, including those posed by the use of new information technology, can be quantified with the probability and potential amount of loss. If you could calculate both figures with sufficient precision, you would have clear information to support decisions as to how much you need to invest in the protection – including proof – of your electronic business processes, as well as the point from which additional investments would no longer pay off. But when information technology is involved, neither probability nor potential amount of loss can be quantified with any certainty, because the large number of factors that flow into such an estimate can easily distort the results.

Even though it is difficult to determine the probability of loss due to a failure to implement security measures, companies may on occasion decide to deliberately refrain from implementing certain security measures, where the risk is regarded as one worth taking in the light of the potential gain arising from this decision. For example, it might make sense for a memory chip manufacturer to participate in a marketplace that does not supply an authorization concept for ordering data, because the potential loss from not participating in the procurement platform is considered to be greater than the risk of industrial espionage. One approach that has its advocates (who received a particularly large amount of attention during the recent e-business craze) claims that speed is everything, and that the risk posed by being too slow is much greater than the risk of being spied upon. After all, by the time the competition has analyzed your company and figured out what you do, you're already doing something completely different. This applies less to traditional industry sectors such as chemicals/pharmaceuticals

or fabricated metals, as the losses here can run to billions of dollars, or even a significant share of a national economy. Of course, this varies from industry to industry, and possibly even from company to company.

AUDITS

Discussion reveals that this issue has to be approached as a whole, yet individually for each company. Every enterprise needs to define the level of security it wants to achieve for each individual business process that it implements, estimate the cost involved, and compare this with the corresponding risk of not realizing the desired level of security. But whatever method used, it must be possible to test the measures that have been chosen and implemented.

In an isolated ERP system, this is possible with relatively straightforward mechanisms – after all, the main feature of an ERP system is that it integrates the different processes within a single system. Accordingly, the critical transitions from one partial process (creating a sales order, for example) to the next (update) can be proven through clean logic in the system and suitable authorizations (process audit). If this approach is not possible due to the configuration of the system, you can also manually trace a sample process by displaying the data from that process at various points (sampling audit).

In distributed landscapes, however, this ceases to be a simple task because the integration no longer takes place in subsystems that are dedicated to specific activities (such as CRM and FI), but instead in special integration components (application integration) that use standardized protocols to address the different application components (Web services). Because the integration components house the actual process logic, a process audit of distributed processes that are implemented with Web services must extract data from the respective application systems, follow the process logic from the integration

systems, and logically merge the two together. Ideally, the integration component itself will support this sort of combination in the form of an “audit warehouse”, as the logic is already present there.

In current systems, however, it is likely that not even a process audit is possible yet, because the participating systems do not support it. Although the strictly functional technology is there, the lack of audit capability means vendors of e-business software have to create it and integrate it in their products. After all, even if no special security technology is used in a system, it must still be possible to prove that the processes have been implemented correctly.

RISK MANAGEMENT: THE LINK BETWEEN TECHNOLOGY AND MANAGEMENT

The ability to prove security is not an end in itself. In fact, the ability to prove security represents the connection between pure technology and economic measurements. Because a company’s business success is the goal of all activities (with the possible exception of e-Government, where the individual interests of citizens and/or political interests of a sovereign state also play a role), the ability to prove security is the driving force behind not only risk investigation and audit, but also the selection and use of the security technology.

As a result, you have a pragmatic, three-level procedure that can be applied to any process, provided it is considered from the very beginning:

1. Risk investigation: Which data/processes deserve protection, and how much money am I prepared to spend for the required protection level?
2. Implementation: Demand the required security characteristics from the vendor or implementation partner
3. Audit: Proof of successful implementation and alignment with protection requirements

These three steps enable you to implement nearly any security-critical application. Steps 1 and 3 should be carried out by the user department as a component of the specifications (with the assistance of the security and risk management departments, of course), while step 2 is implemented by the IT department, just as the technical scalability and administration concepts normally stem from this area.

IMPROVED IMPLEMENTATION THROUGH ORGANIZATIONAL CHANGES

Direct, personal responsibility for security must be defined. Perhaps contrary to your initial intuition, this responsibility should not be assigned to the IT department, but instead to the user departments – supported by risk management and security management. This approach will guarantee that the corresponding measures and/or technologies for security will be implemented whenever they provide benefits in the greater context – for example, when they represent a business case. The IT department is involved in this process as a supplier, while the risk management department can rate the performance of the IT department (in the form of an acceptance test or an audit) and confirm the quality of the rendered work. The areas of responsibility are clearly defined. The department that is responsible for a given process is also exclusively responsible for the security requirements of that process. These security requirements must be derived from the risk analysis of the process definition. The user department is also responsible for the associated risks.

This approach can resolve the strategic dilemma described earlier in this paper, while enabling the short-term benefits to be considered in a business case analysis as well. This approach involves two critical concepts that cannot be applied by companies that think along old lines: identity management and Web service security. Identity management requires an integral approach to user, role, and authorization management that is

simply impossible under the traditional department/level-based approach. Web service security, the protection of data and transactions at the output level, turns the traditional concept of data ownership on its ear. Both of these concepts are essential prerequisites to conducting e-business, and neither can be implemented in a company that is organized along traditional lines.

Regulation vs. Deregulation

You should also consider the extent to which regulation can help to achieve security. In general, it can be said that regulation is required wherever security cannot be achieved on its own momentum. Specifically, this means that especially private citizens and small businesses – who generally find it difficult to even find out the extent of the problems involved – have to be protected by regulation. In all other areas, regulation is largely useless or even harmful.

Data Protection and Privacy

One of the most important areas that requires regulation is the protection of individual privacy. For example, there is no economic reason not to save the data of customers or general contacts, even if such data does not provide any immediate benefit and might only be used in the future. As a result, data protection cannot be self-regulating, which makes legal requirements necessary.

Although government agencies may store citizens' personal data in order to safeguard internal security, access to such data must also be strictly regulated in order to prevent its abuse.

The heterogeneity of international data protection laws poses a particular problem at present. Whereas Europe (particularly Germany) is rather over regulated by a series of different laws, some overlapping, others contradictory, other countries (such as the U.S.) address the use of personal data inconsistently across different business contexts. Standardization and simplification of these regulations is sorely needed, and would benefit both vendors and consumers.

FDA, HIPAA ET AL.

There are a number of industry-specific regulations that involve IT security. Most of these have been introduced in order to protect the consumer and should be retained. For example, the Food and Drug Administration's "Code of Federal Regulations 11" on "Electronic Records" describes a series of security measures for IT systems that must be implemented at the application level, such as the requirement for digital signatures to release batches of pharmaceuticals following quality tests. Another example: In 1996, the U.S. "Health Insurance Portability and Accountability Act" was passed, which declares personal data in the health industry to be deserving of protection, and defines the corresponding requirements for electronic processing.

OPEN SOURCE, PATENTS, AND SECURITY

The term "open source" is often mentioned in the context of increased software security. This is because software whose code is publicly accessible is considered more secure than "closed source" software, which is not immediately visible. In my opinion, this belief is a fallacy. Although revealing the source code makes it fundamentally possible to detect security weaknesses, it does not actually require anyone to search for such weaknesses systematically. In this regard, open source software is no better than commercial products. The critical factor is the existence of a process to guarantee that security gaps – when discovered – are corrected in the first place, before the software is shipped, bringing us back to the concept of security as a quality.

Another aspect of open source software that is especially important for cross-company business processes is the fact that it can be used free of charge. As a result, interoperability of the protocols can be achieved much more quickly, because communication on both sides is usually based on the same (open source) software. This attribute is not a unique selling point of open source software itself, however. The real reason for its rise in popularity is the definition of open standards (through OASIS, IETF, and so on) that makes it possible to

create proprietary implementations without the risk of making yourself liable to prosecution for patent violation, for example. In this context, it would be better to ignore the "regulation" provided by patented procedures, at least where security functions are involved, and better still to do away with such regulations completely.

Education and Training

A number of initiatives are aimed at supporting the complex subject of security in the information society with improved education and training offerings. Germany, for example, has defined an apprenticeship program as "IT Security Coordinator". This development is positive and important. *However, as you have read, the issue of security permeates all other areas as well. As a result, security can only achieve its ultimate effectiveness if each operative area bears its own share of the responsibility. Accordingly, it is even more important to consistently emphasize the issue of security in all relevant IT careers and education programs.* For example, IT risk management should be a required subject for every business data processing specialist, just as the authoring of secure software should be a requirement for every software engineer.

CONCLUSION

The topic of security in the digital world is a complex one. Security means thinking in terms of "what could work?" instead of "what works right now?" Consequently, security is more of a state of mind. Security concerns us all, but the necessary awareness is insufficiently developed. New, cross-company business processes demand new security concepts to support them. The information technology market will favor application vendors who take security seriously as a quality characteristic. The main responsibilities for businesses implementing these solutions are to promote awareness among all those working with the solutions, and to define clear areas of responsibility for improving security in operational areas. Regulations should be applied where protection of individuals is necessary, and large organizations should be enabled to help themselves.

THE BEST-RUN BUSINESSES RUN SAP



SAP AG

Neurottstraße 16

69190 Walldorf

Germany

T +49/18 05/34 34 24*

F +49/18 05/34 34 20*

* Subject to charge

www.sap.com