

IT Security Priorities in a Brave New World

An IDC White Paper
commissioned by Steria

Analysts: Daniel O'Boyle Kelly, Carla Arend

June 2003



46, rue Camille Desmoulins
92782 Issy-les-Moulineaux Cedex 9 - France
Tel. : +33 1 34 88 60 00
Fax : +33 1 34 88 62 62
www.steria.com



STERIA'S CUSTOMER TESTIMONIALS

RFV, THE SWEDISH SOCIAL INSURANCE ADMINISTRATION - PROVIDING SECURE ACCESS TO SENSITIVE DATA

17

CARELINK - FACILITATING INTEGRITY IN HEALTHCARE

19

A MAJOR EUROPEAN TELECOM OPERATOR - SIMPLIFYING NETWORK ACCESS

21

MINISTRY OF JUSTICE IN ANDALUCIA - ENABLING COLLABORATION

24

THE FRENCH MINISTRY OF ECONOMY, FINANCE AND INDUSTRY - BUILDING TRUSTED ENVIRONMENTS

26

SUMMARY

INTRODUCTION

3

A BRAVE NEW EUROPE?

4

The changing security paradigm

7

What is the holistic approach to security?

8

Where do I begin?

10

LAYING THE FOUNDATION

12

Secure infrastructure

12

Protecting the assets

16

Key to the door: secure access

18

FUTURE OUTLOOK

22

The age of enablement - secure e-business

22

Self-service solutions enabled by the web

23

Where to turn? Outsourcing versus in-house

25

CONCLUSION

29

Introduction

Present conditions are forcing organisations to rethink about their business goals and the environment they operate in. As the search for growth intensifies, it will increasingly involve extending the enterprise 'beyond the firewall' - be it with customers, suppliers, partners and even employees. Moreover, aligning business goals by leveraging technology involves doing so in a more secure manner as IT managers and CEOs alike recognise that doing business more openly creates opportunities yet opens up risks as well. Information security is about balancing these risks with the rewards of fostering trusted relationships. And because both opportunities and vulnerabilities are constantly changing, security has soared to the top of the corporate agenda.

This White Paper written by IDC and commissioned by Steria, examines the importance of securing and protecting an organisation's corporate assets and resources. The study identifies the issues organisations should consider and provides insight into how companies can utilise security both as a protector and as a business enabler. Through a series of case studies, leading organisations illustrate how they have overcome the challenges they faced in protecting their assets while recognising the inherent benefits of their security investment.

A BRAVE NEW EUROPE?

There is a growing realisation among organisations, be they large or small, that they need to focus on 'what they do best' but also explore new initiatives. More than ever, this dichotomy involves both productivity and revenue optimization yet can be somewhat unsettling. For instance, how do you leverage the relationships you have invested considerable resources in without 'opening' the door to unwanted guests? With the drive for new areas of growth, it is apparent that organisations need to protect themselves from potential financial and productivity losses, not to mention the downtime, caused by challenges with extending the enterprise.

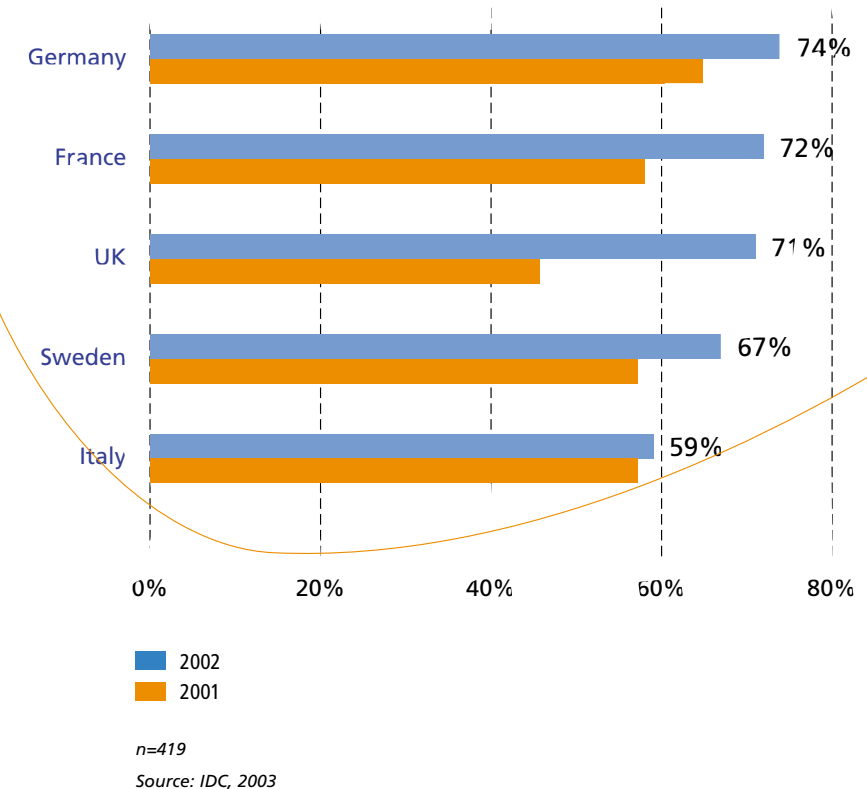
Three-quarters of organizations across Europe now rate IT security as significant or highly significant to their operations.

According to a recent European survey conducted by IDC, respondents were asked to state the challenge associated with a wide variety of potential IT issues and then subsequently rank these on a scale from 1-5, with 1 representing no significance and 5 for very high significance. Security was stated as the top challenge moving forward, with three quarters of respondents ranking it as significant or higher while a full 38% of respondents considering it as the highest significance (value 5). While the rush of the late nineties might have been to connect fast, the reality of today seems to be to connect securely. This heightened importance is reflected across major economies of Europe, as shown in Figure 1.

FIGURE 1

EUROPEAN ENTERPRISES THAT RATE THE SECURITY CHALLENGE AS HIGHLY SIGNIFICANT

Q. How significant is Security [hacking, virus, denial of service, employee internet/email control, policy enforcement, etc] in terms of IT challenge?



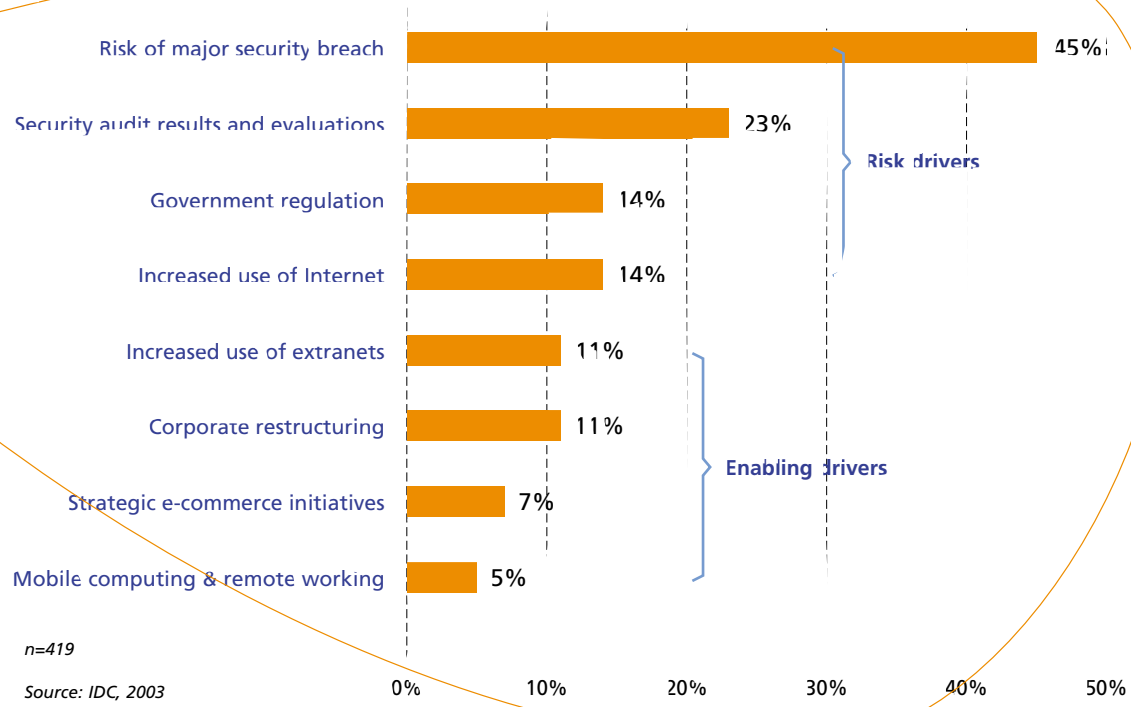
Security adoption however remains fear-driven in Western Europe thus far, with 45% of respondents quoting the risk of a major security breach as highly significant (rating 5 out of 5) while security audit results (identifying security gaps) shows considerable consideration in 23% of European organisations. (See figure 2)

Historically, investment in security has been very reactive. This can be attributed to a lack of awareness, as well as a lack of data and models to assist in justifying business cases and planned investment in security. Many investments in IT security are still in response to unauthorized access or malicious activity occurring, but there is evidence that security is increasingly being viewed as more strategic by select corporations, especially those that pursue an integrated Web-enabled strategy.

FIGURE 2

KEY SECURITY CHALLENGES IN EUROPE (% AS VERY SIGNIFICANT)

Q. Excluding physical security to the business premises, how significant would you say the following factors are in influencing your security infrastructure?



n=419

Source: IDC, 2003

As organisations recognise the security threat is more than just a virus or breach issue, we are seeing an increased appreciation of the breadth of the security challenge. Figure 2 shows another clear trend correlated to the types of challenges organisations face; that is, the distinction between threat-led and strategic-led security spending. For instance, risk drivers, being the most prevalent today, are reactionary and more operational in nature due to either an internal review of existing systems or external market forces.

Enabling drivers, on the other hand, are more aligned with forward-thinking objectives and thus could be considered more strategic investment than spending. Still, the way forward may not always be clear. Combined with the diversity of the individual technologies that are used to address these security challenges, organisations are facing an environment growing in complexity.

THE CHANGING SECURITY PARADIGM

Essentially, organizations are investing in IT security in an attempt to protect corporate assets and mitigate risk. To achieve these goals, however, organisations need to both identify the assets they are trying to protect and the level of risk they are willing to bear on those assets. By examining the risk factor according to business principles, organisations are better able to determine which assets are most valuable to them and how much they should spend on protecting them. This solution-based view of security has subsequently led to demand for services around consulting, assessment and management to address security risks.

Increasingly, organizations seeking competitive advantage from investments made to extend the enterprise will need to move away from a reactive into a more proactive mindset by designing a security culture that addresses the longer-term objectives of their business.

Security ROI

23% of IT professionals across Europe state that the return on investment on security software is significantly higher than anticipated.

TABLE 1

ASSET OPTIMISATION VERSUS RISK MITIGATION

Corporate Assets	Corporate Risks
Physical assets, such as hardware, software and networking infrastructure	Financial Risk – Direct costs and the cost of business lost through not being able to service customers.
Customer data	Legal Risk – Breach of privacy or loss of customer and/or supplier data.
Customer trust (or business goodwill)	Brand/ Image Risk – Loss of confidence about the organisation's ability to protect confidential information.
Intellectual property (IP) and confidential information.	Strategic Risk – Theft of IP and confidential information - this information is the company's lifeblood
Competitive information	Opportunity Cost – Reactionary security response moves resources away from competitive response.

Source: IDC, 2003

Without question, as more and more business opportunities lie “outside the firewall”, security needs increase as companies open their internal business processes to outsiders. This fact will force companies to develop a more holistic approach to security and it will push the demand for security expertise to deliver an all-encompassing solution based on business need – not the reverse.

WHAT IS THE HOLISTIC APPROACH TO SECURITY?

Holistic security means making security part of everything and not merely a separate function. This bottom-up approach ensures security isn't merely added to the enterprise; it becomes embedded in all processes that enable business goals to move forward. Rather than a necessary cost, in this way security becomes an enabler.

This has been driven by the need for enterprises to expand ‘trusted relationships’ with customers, partners, suppliers and channels. To improve security you will need to know more about who is being authorised and what they are authorised to do as well as have a level of assurance that all of this is being done properly. For instance, as security becomes ubiquitous, people will improve the processes that allow them to work more productively.

IDC's ongoing research amongst IT managers from establishments actively engaged in e-business reveals significant security solution “critical decision factors”. These factors are a reflection of the effort to balance widening access and effective security. These include:

- **Protecting** assets from hacking by avoiding embarrassing Internet exposure and maintaining reputation.
- **Integrating** the security infrastructure by ensuring that the typically wide range of security products work together seamlessly and without excessive administration overhead from a single point of accountability.
- **Enabling** widened access to formerly “inside-only” content and applications to valued stakeholders while preventing unauthorised access both externally and within the organisation by ensuring valid credentials.
- **Supporting** e-business openness by ensuring that security does not block key business objectives with, for example, ease-of-use issues for external users or time-to-market delays for e-commerce business managers.

What's needed, then, is a roadmap for developing a holistic approach to IT security not looking at IT security as a set of isolated tools designed to address specific issues as they arise, but rather as a total solution, which considers all aspects and addresses

corporate/organizational imperatives for business continuity, confidentiality and privacy, among other things. This brings security into the bigger picture of risk assessment and management in general. More specifically, a typical enterprise must address three distinct yet interwoven risk areas;

- **Physical Security**
- **Information / Transactional Security**
- **Business Continuity**

While this study sets out to address information security only, it is nonetheless essential to keep in mind security is part of a “greater” picture and as such, can move issues out of the IT department alone.

WHERE DO I BEGIN?

The place to start then is by undertaking an evaluation of risk both prior to implementing security processes and solutions, and on an ongoing basis afterwards. In formulating a proactive plan necessary to implement effective IT security, many professional security product and service vendors recommend a risk assessment exercise in order to identify assets, threats and vulnerabilities, and to develop a risk-minimized posture. In this way, the scope of the risk at hand and resources needed can be earmarked. By extending this then to the strategic goals of the organization, a plan can be drawn up to prioritize the move towards holistic security in a step-wise manner.

European organizations need to ensure that investment decisions are made as a result of co-operation between the business side and the technology side, that is between the CEO and the CIO. Because key issues around security investment are more strategic today

rather than the technological push of only a few years back, support of top management, including the board, is crucial to the success of any security initiative. This is particularly the case when considering the overall size of security investments. In general, as security moves from point solutions to holistic solutions, they quickly “outgrow” the decision making of IT departments in isolation. While technology may be the facilitator to a desired end state, it is overall senior management attention that will ensure strategic alignment.

The study now strives to reinforce the above views by looking at technologies, solutions and selected practical examples in the market today. To this end, the remainder of the white paper is divided in two distinct sections;

- **Laying the Foundation** looks at the here-and-now with security implementation levels today and solutions to address asset protection and secure access.
- **Future Outlook** then looks towards the design of new processes and future enablement most notably secure e-business and partnering.

LAYING THE FOUNDATION

SECURE INFRASTRUCTURE

Initially, as indicated by the challenges listed in Figure 2, enterprises look to lock-down infrastructure “holes” first before (or at most concurrently) exploring new areas to “open-up”. So where are European organisations placing their security technology spending today? The following two figures indicate security implementation today in Europe. Although technology focused, they offer an insight to the changing security paradigm underway, albeit at a very early stage. The solutions listed in Figure 3 can be considered more mature, particularly focusing on protection while solutions in Figure 4 align with newer technologies (or reborn in the case of PKI) where the focus moves more towards enablement.

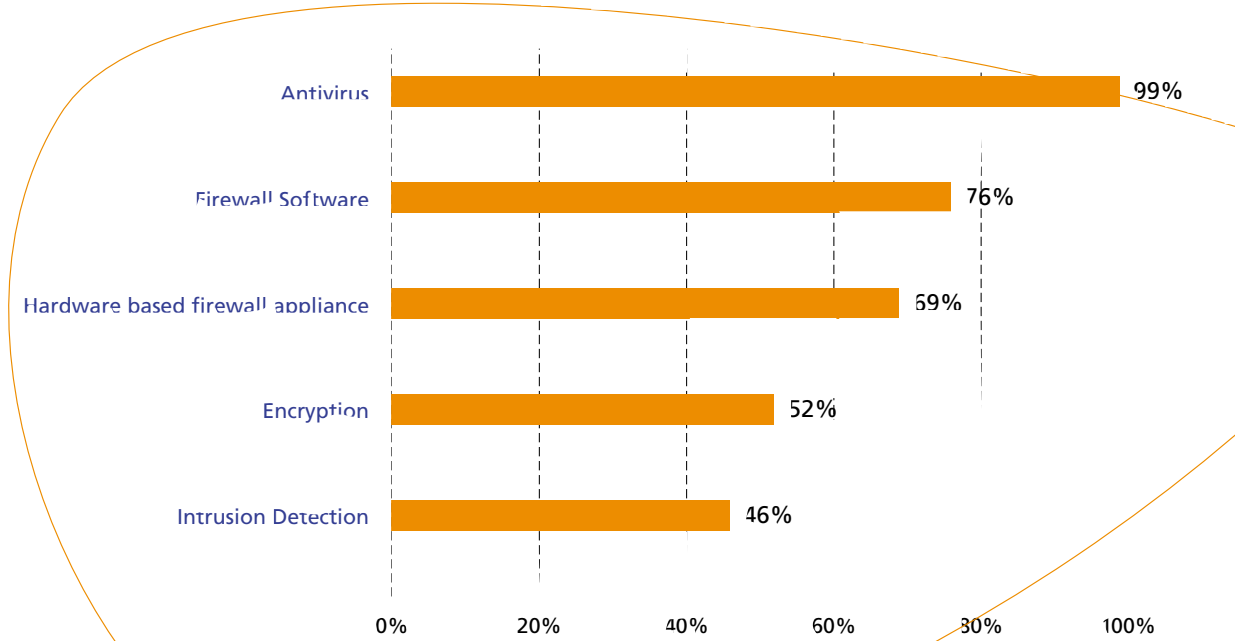
The profile of security adoption in figure 3 indicates almost all businesses in Europe deploy antivirus technologies. In the same fashion, firewall technology – both software and hardware based – is now a mainstream technology. However,

- **Antivirus** tools are essential for stopping viruses but they cannot prevent embedded or disguised threats in emails and attachments.
- **Firewalls** are great at providing access control but they do not protect against harmful content coming in and out.

FIGURE 3

SECURE & PROTECT: IMPLEMENTATION OF SECURITY SOLUTIONS IN EUROPE, (%)

Q. What security solutions are installed today within your enterprise?



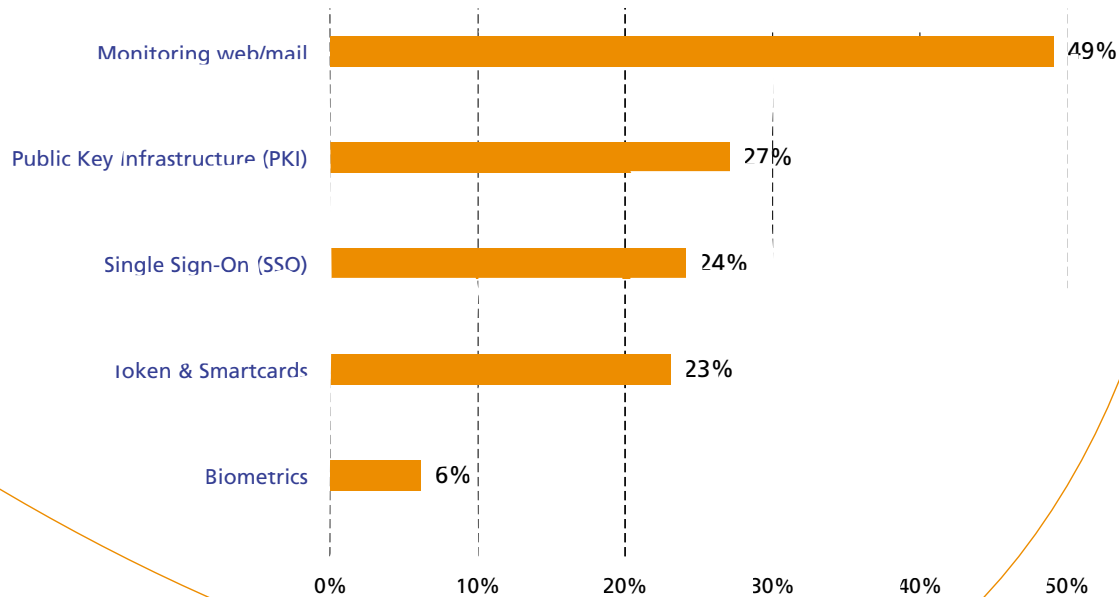
n=419, multiple responses allowed
Source: IDC, 2003

Without a holistic security solution in place, organizations relying solely on antivirus tools and firewalls to provide Internet, email and web security, are seriously compromising their business and network integrity.

FIGURE 4

SECURE & ENABLE: IMPLEMENTATION OF SECURITY SOLUTIONS IN EUROPE, (%)

Q. What security solutions are installed today within your enterprise?



n=419, multiple responses allowed

Source: IDC, 2003

Newer technologies, although still emerging, begin to address the greater scope of protection as well as enablement. Security is inherent in all the technologies but it is the less mature technologies that begin to see a more strategic implementation.

- **Software to monitor and filter employees Web and email usage** begins to address the fine line between protection and enablement. For instance, no one can dispute that the explosion of Spam is not only a security issue (as in corrupt unwanted files) but also a loss productivity issue.

- **PKI** deployment starts to make sense for many reasons not the least of which is the fact that many governments in Europe are launching PKI implementations that will allow citizens and businesses to exchange secure digital information with the public authorities.

- **Single Sign-On or SSO** is a key development to reduce complexity while boosting productivity for employees, customers, and other system users. Increasingly, we see coupling of technologies such as PKI and SSO to address identity management.

- Other security technologies address the more advanced business needs around hardware authentication, and we expect implementation levels to grow accompanied by products that are simpler to deploy and use than the current state of technology, mainly within **smart cards and biometrics**.

TABLE 2

NEW SECURITY SOLUTIONS: TOMORROW'S BUSINESS ENABLERS

Integrity	through effective and aligned risk management policy-making,
Productivity	through mastering internal workflows and administrative backlog,
Effective outreach	through new ways of working with mobile employees, suppliers and partners,
Credibility	through proactive secured business relations and brand enhancement,
Opportunity	through enabling new high value-added services such as e-commerce / e-business.

Source: IDC, 2003

The underlying theme that emerges with the newer technologies above is that the security aspects are considered a given - in other words many organisations begin to ask "and what else can it do for me". Again this moves an alignment of IT towards optimising business goals under constraint. In essence, the desired goals should fall under one or more of the points listed in Table 2 with security intrinsic in the offering.

The remainder of the study now shows how select organisations are actually achieving the inherent goals in Table 2. In many cases an organisation's greatest asset is the processes it has built to leverage data and information. "Access and interaction" thus becomes crucial for businesses that are looking to take advantage of the opportunities that extending the enterprise offers. The ability to use security technologies to enable greater access to corporate data deepens and stabilises relationships. These "trusted relationships" can yield numerous benefits, such as higher transaction rates with greater scalability, lower cost per transaction, and transference of personnel from low-value interactions to high-value personalised service.

PROTECTING THE ASSETS

The need to protect and preserve an organization's information has never been greater, as these corporate assets are becoming increasingly exposed with online channels being used for business processes and information is stored electronically.

With this growing pressure, coupled with the increasing complexity of legislation on how organizations should handle content and documents, companies are being well advised to move beyond infrastructure security solutions alone and look to privacy/data protection and "privacy" engineering.

IN FOCUS

RFV, THE SWEDISH SOCIAL INSURANCE ADMINISTRATION - PROVIDING SECURE ACCESS TO SENSITIVE DATA

Riksförsäkringsverket (RFV) – the Swedish Social Insurance Administration – handles the National social insurance scheme and is responsible for managing the greater part of the vast Swedish social security system. As with all governmental organizations, it has to balance ease of use around its IT systems with confidentiality of the type of transactions it processes. And RFV's infrastructure needs to be very secure indeed with activities grouped into three areas: processing and payment of social benefits, response to sickness and accident claims, and analysis/quality assurance of services. Thus, ensuring uniformity and quality in the processing of insurance and benefit cases is a key challenge

As RFV is dealing with very sensitive personal data, Mr. Anders Nordlander, head of security with the social insurance administration states, "the greatest responsibility of RFV is to comply with the Swedish law and regulative requirements for data security and to ensure the integrity and privacy of citizen data captured in RVF's systems". To support this goal, RFV's IT infrastructure has to provide a secure environment for all their 15,000 employees in RFV and the local social security offices. To ensure availability and integrity of data within services available, it was decided to implement a smart card identification system for RFV's employees and to integrate mainframe-based data into web-based applications, in attempt to balance the demands of both security and access.

This solution was chosen because, as Mr. Nordlander put it, "It was a proven technology and that was important for quick adoption, as we could draw on the provider's experience from comparable projects.

Another key issue was the flexibility of the platform and we felt that the solution had the most potential to integrate with future applications". When choosing this project, it was important to RFV that the solution fit into its roadmap for IT investments and development and that it can be used with other standard IT products. Although a return on investment calculation has not been done, the protection of citizen data while enabling more service offerings for citizens was the key driver for this project. "Security is a management priority because it has been identified as an enabler for RFV to provide better service to the citizens".

Organizational processes had to be defined and altered to fully take advantage of the new technology solution. Mr. Nordlander has realized that "80% of the project is the paper work and defining the processes and 20% is getting the technology in place. Education of users is key, to make them understand the advantages of the solution, especially when users with different levels of advancement are involved. The organization development spurred by this technology is tremendous". With the demand for providing citizen services online being pushed by e-government initiatives of the European Union, RFV is looking to upgrade its authentication and authorization technologies to increase the number of current services offered online. Once achieved, and with security measures fully operational, RFV will be able to supply Swedish citizens with access to the systems they require whilst maintaining a regulatory and robust level of data integrity.

Source: IDC, 2003

National governments across Europe are the single biggest security spenders in their respective countries.

It is not surprising that European governments and public administrations are carefully scrutinizing security solutions to protect their data and citizens' data. National governments across Europe are the single biggest security spenders in their respective countries and have become, somewhat unexpectedly, exemplars of rolling out secured network environments. While most of the focus has been on securing the flow of information among government department agencies, growth will come from other areas (citizen relationship management, one-stop portals, e-procurement). Commercial enterprises in turn can learn a great deal from these public sector initiatives.

For instance, the developments in telemedicine are driving growth of security solutions in healthcare. Today, computers store the medical information that is faxed back and forth from offices to hospitals. And it's common also for sensitive communications to be sent by email messages. Protecting patients' privacy is therefore a key issue of today's healthcare systems. Furthermore, regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the US are also expected in Europe.

By utilizing PKI, customer information and sensitive data can securely be processed and distributed to appropriate individuals. PKI certificates will also be a part of a greater enterprise identity management deployment of smart cards and USB tokens to ensure an even greater layer of integrity crosscheck.

KEY TO THE DOOR : SECURE ACCESS

Once infrastructure and data are sufficiently protected (in essence the lifeline of the organisation), the logical extension of this is to intelligently open-up environments to valued stakeholders. This is more complex than first witnessed, as many organisations have discovered. Within the enterprise, for example, there are many

IN FOCUS

CARELINK - FACILITATING INTEGRITY IN HEALTHCARE

Confidentiality of health information has always been a point-of-principal throughout the medical profession. Carelink is a public sector body responsible for initiating and supporting IT development in Swedish healthcare, so that patients, relatives, users and customers are confident that IT is implemented to increase accessibility, safety, quality and service.

"Communicating patient data amongst healthcare institutions in a secure way and ensuring the integrity of patient records and medical journals through digital signatures is a key issue", according to Mr. Allerstedt, project manager for the Carelink project. This is accentuated by regulatory conditions imposed on the Swedish healthcare sector. To support the Swedish healthcare sector in complying with these conditions, Carelink has taken on the task of implementing a nationwide PKI infrastructure and the roll-out of a smart card based authentication system.

The PKI to be implemented by Carelink uses two kinds of certificates: a primary personal ID certificate, which is issued by a trusted party in Sweden, i.e. the post office and telco Telia. The secondary certificate is issued by Carelink and authenticates employees of the Swedish healthcare sector, containing the role, the title and the place of employment. Both certificates are stored on a smart card and employees can use them both at work and in their free time.

Mr. Allerstedt describes the advantages of the possibility to sign documents digitally: "The law requires the doctors to sign medical records. Today this is done on paper, but we want to do it electronically, as it is much more cost efficient. It shortens the process times when you do things electronically by not sending paper around. This is one of the great advantages of this solution". At this stage, the results have differed from county council to county council as there is a variety of organisations in the healthcare sector which have different routines. Still, lessons learnt across the region can be disseminated in order to have a climate of continuous improvement.

The smart card and PKI solution enable the county councils to be more accessible for citizens. "Most county councils have portals to communicate with the citizens and patients. And this is a driver to identify the users of these portals in a secure way, in order to ensure interaction, like the transmission of medical records. Security is necessary when you have to communicate in the healthcare sector. The sender and recipient of medical records have to be authenticated, otherwise they will be prevented to communicate more sensitive details. If a doctor receives an email from the patient, she has to be sure about the identity of the sender of the email, otherwise she is restricted as to the level of response. And neither the public nor healthcare officials want to be restricted by the technology", adds Mr. Allerstedt.

Source: IDC, 2003

disparate directories across which access attributes, policies, and preferences cannot flow. This lack of continuity, at a minimum, has users needing to log in to each application or data store separately. Therefore, more usernames and more passwords to remember will inevitably lead to a call to the help desk for a memory/password refresh.

Enabling employees, for instance, to log in just once and have access to all necessary information and functionality provides a more seamless work environment. Moreover, with a reduced list of usernames and passwords, the help desk should receive fewer calls. Additionally, there are solutions that facilitate the management of employee self-service for password reset, which will diminish help desk calls as well.

IN FOCUS

A MAJOR EUROPEAN TELECOM OPERATOR – SIMPLIFYING NETWORK ACCESS

A major mobile telecom operator could see a growing concern with something as seemingly straightforward as logging onto the network. Access to network resources is something that is taken very seriously in the telecom industry. If a network goes down, its not only the employees that suffer from loss of productivity but also potentially disruptive service to over 20 million customers the operator now serves. Within the organization, it is also of the utmost importance to have the right solution in place, not only to protect against security breaches, but also to allow efficient access to the right applications without delay and cumbersome password management. Aggressive corporate expansion has resulted in only intensifying potential challenges with the complexity of melding together resources across eight divisions. "Employees were overwhelmed with the number of passwords they create to access different applications on the network. As a result, we could see they were using trivial passwords like 1234 which caused us a lot of anxiety that the network could easily be breached" explained the Telco's operations manager. "So we looked to a solution to better manage and more securely get people connected".

The firm decided to implement a Single Sign-On System in the Operation & Maintenance division. The AccessMaster based system installed now supports 720 Client Systems (Linux, Sun Solaris, Windows NT), 15 applications and 500 users. The strength of the structure is that as additional applications are added there is no need to change the existing architecture. In the case of a partial network failure, redundant components take over the jobs concerned until fault recovery. In the future, the additional use of smart cards guarantees that only the owner of a smart card in combination with an individual PIN code is given access to the IT infrastructure.

Still, while the security technology solutions proved to be robust, it was actually employee behaviour that needed to change to make the project a success. Indeed, some network administrators were sceptical to begin with as the expertise needed was not a "plug and play" solution due to different subsidiary structures, details, and processes. For this reason, the network-engineering department now sets security policies based on usage while the security department audits implementation based on technologies. This balanced approach of technology/behavioural acceptance is key to any project and should be a key consideration when designing a rollout schedule, especially if involving external parties.

Immediate payback is something that is not easily quantifiable in monetary terms. However, with a reduced number of breaches to the IT infrastructure and with the visible robustness of single passwords increasing, potential cost avoidance can be rationalized. This is particularly true within an organization that previously had somewhat uncontrolled provisioning. Indeed, the results at this early stage of the project have been noticeable. "Quality and security aspects have both shown major improvements which has been key for us to gain support as increased security has become a key criteria for top management", said the respondent. "Also, it fits in well with a parallel initiative to allow remote vendor access". Once the security features and processes become embedded in policy, the firm plans a second phase to build out more sophisticated user management including user profiles, provisioning and advanced identity management.

Source: IDC, 2003

FUTURE OUTLOOK

THE AGE OF ENABLEMENT - SECURE E-BUSINESS

While early Internet usage centred on information sharing and Web-site access, today the Internet environment provides the platform for an immense number of e-business activities. Suppliers, customers and employees are blended into an integrated IP-based business fabric and a growing array of data sources, applications, transaction types and resource support this environment. This evolution of Internet and Intranet usage has expanded both opportunities and security requirements exponentially.

The issue is not just to meet security requirements but also to develop a culture of security within the organisation

Security breaches, for instance, raise a crucial concern, one that could have potentially long term effects damaging an organisation's brand name. In this way part of the loss is indirect, that is, confidence lost to both customers and suppliers. But by turning this scenario around, companies could actually emphasise that they are an enterprise serious about security, thereby **strengthening** their image and the likelihood of future opportunities. Again, nowhere is this more evident today than with public authorities as those have actually been able to offer new services by strategically embedding their security solution.

For instance, as much of the information exchanged between citizens and the public administration is of a personal or confidential

nature (medical, financial, legal etc.), security is vital to ensuring successful uptake. Furthermore, the development of e-government makes public administrations both potential exemplars in demonstrating effective secure solutions and market actors with the ability to influence developments through their extended-service decisions.

The issue for public administrations is not just to procure information and communication technology systems with security requirements but also to develop a culture of security in the organisation. This can be accomplished through the establishment of "organisational security policies" tailored to the needs of the institution.

SELF-SERVICE SOLUTIONS ENABLED BY THE WEB

As governments across Europe launch initiatives to encourage increased access to services on the Internet, public trust in the security of information exchanged over the Internet plays an essential role in this changeover. Services such as applying for benefits, permits and license applications, change of address and business registration are all becoming a reality over the Web.

Public Key Infrastructure (PKI) and managed PKI services ensure that such services and the exchange of sensitive government documents and transactions are protected online. Most European countries have chosen PKI as the underlying infrastructure for citizen/business to government transactions which in turn allows government agencies to address a variety of secure transaction challenges including:

MINISTRY OF JUSTICE IN ANDALUCIA - ENABLING COLLABORATION

Junta de Andalucía, the regional government of Andalucía (Spain), has to juggle availability of information with confidentiality and security. It has a corporate network for all its departments and a part of it belongs to the Regional Ministry of Justice, which serves all its entities (courts) in Andalucía. The integrity of juridical information is absolutely crucial for the integrity and privacy of citizens. And the ministry takes this responsibility seriously: "We perceive security as an obligation to the public, so that private, sensitive information of lawsuits is well protected", says Mr Julio Ubeda, CIO for the Regional Ministry of Justice.

When a new overall case management application for all judicial bodies of Andalucía needed to be implemented, security of the solution was paramount. Mr Ubeda states: "The need for a security solution was based on the highly sensitive nature of the data in the new case management application. This is a distributed application with 173 individual but interconnected implementations across the whole judicial system in Andalucía and to enable such as distributed system, we needed a thorough security solution". In essence, this new application could not have been enabled without the secure element being woven into the solution.

The Regional Ministry of Justice under the Junta de Andalucía decided to implement a PKI and VPN solution, combined with smart card authentication. The Regional Ministry of Justice required the confidentiality of the communication between its 150 sites through virtual private networks (VPN) and the integrity of the data through electronic signatures and strong authentication of users with personalized smart cards. Mr. Ubeda describes the solution: "Generally speaking, every server and office line is encrypted using a Virtual Private Network. And every privileged user (Magistrates, Clerks of the Court and Public Prosecutor) is authenticated using an encrypted card, inserted into a special card reader attached to each PC. The user then inputs a pin code and gains access to the system".

The ministry is very satisfied with its security solution, as it enabled it to implement the new case management application and thus to enhance the collaboration between its 150 sites. In short, the security element was a necessity and it ensures the ministry complies with the strict privacy requirements of the law. Moreover, and possibly of greater benefit, it is the key enabler for the implementation of the case management solution which has yielded high productivity gains.

Source: IDC, 2003

- Controlling access to intranets and extranets,
- Authenticating senders and recipients in commercial transactions and confidential e-mail exchanges over the Internet,
- Implementing Virtual Private Networks using the IPSec protocol for confidentiality and data integrity as well as attaching legally enforceable digital signatures to electronic forms.

It is of course important to realize the implications that online self-service brings. They are, in fact, new processes that did not exist before. For instance, immediate online validation of forms, something that could have taken weeks before, allows more focus to be levied towards value-added activities. Immediate customer feedback based on monitoring and web analytics to hone offerings can reduce "hit and miss" product launches and even go-to-market spending. Again, these are not new applications in isolation but their success can now be attributed, in great part, to the level of trust embedded. And as is well understood, trust has a lingering effect that will positively impact relationships well beyond the technology at hand.

**WHERE TO TURN?
OUTSOURCING VERSUS IN-HOUSE**

As with any technology solution, an ongoing debate can be whether to treat security as a wholly internal issue or to outsource. In an environment of competing demands and limited resources, an organization may consider outsourced security services. Outsourcing can provide a turnkey managed security service that reduces the pressures and challenges that IT organizations face in attempting to manage security internally. It provides three key elements: technology tools, policies & procedures, and a staff of security experts monitoring the enterprise's network on a continuous basis.

IN FOCUS

THE FRENCH MINISTRY OF ECONOMY, FINANCE AND INDUSTRY - BUILDING TRUSTED ENVIRONMENTS

The French Ministry of Economy, Finance and Industry initiated a new program to illustrate its e-administration policy in action. The program, named Copernic and managed by the General Tax Office (DGI) and the General Public Accounting Office (DGCP), aims to carry out a recasting of the current fiscal information system, and externally set-up simplified fiscal accounting processes. The Copernic programme thus allows citizens to have a multichannel access to two new services: tax declaration via the Internet with an electronic signature, and on-line access to their tax file.

These services enable citizens to access this information much simpler than before. But given the significant number of potential external access points to the Information System, the robustness of the security is critical for uptake. In this context, the role of the Copernic team is to guarantee an optimal quality of service in order to establish and maintain the citizen's trust. Thus, taxpayers have to utilise certificates delivered by referred authorities. Without it, the new service could not exist.

To support this goal, the Copernic team has set to build a completely secured environment for their constituents, as embedded security is an integral part of the programme. "It's not only a technical matter, but it is also a legal and organisational challenge" as stated by the Copernic Team. To this end, the security policy is set "globally" for all government services and then defined (and made operational) at the Copernic programme level. Further decisions as to what degree security policy is applied are then scrutinized on a project-to-project basis. This is holistic security in action; that is, policy driving implementation in leveraging current processes while enabling wholly new ones. The security solutions deployed in the context of the Copernic programme meet the need for confidentiality requested for this kind of services, and they still remain evolutionary and adaptable to new uses and environments.

Providing new and various on-line services to citizens falls within the French government's will to develop ongoing e-administration initiatives. In this context, the French Ministry in general and the Copernic team in particular, work to improve the security around the tax information system, especially the authorization and authentication, so that new services could be proposed as adoption gains traction thereby deepening the relationship with each citizen.

Source: IDC, 2003

TABLE 3

OUTSOURCE VERSUS IN-HOUSE

	Outsourcing	In-House
Advantages	<ul style="list-style-type: none"> • Access to seasoned security expertise • Greater availability of systems/solutions • Can be cost effective 	<ul style="list-style-type: none"> • Maintain control of critically important assets • Tailored to specific needs & processes • Increased security 'culture' throughout org.
Risks	<ul style="list-style-type: none"> • Less control of sensitive company assets • Solution may not fit the business process • Sustainability of solution provider 	<ul style="list-style-type: none"> • May not have knowledge needed • Could be expensive while maintaining staff • Complexity

Source: IDC, 2003

Still, outsourcing isn't the right answer in every situation and as such a review of the underlying business objectives behind any technology solution should be considered. In this analogy, outsourcing can be used when the technology does not, itself, add value, or when the technology involves a specialised skill that internal resources are lacking. In certain cases, network security doesn't meet the test of adding value to business operations any more than a physical security guard or alarm service adds value to a firm's premises.

With outsourcing, however, comes anxiety and risk. For employees, outsourcing could carry the threat of skill erosion. For management, outsourcing of critical functions or sensitive data can feel unsettling. Yet when properly implemented, outsourcing of managed security should be well matched with a company's risk

profile to the point where the burden of continuously “patching” possible weaknesses is lifted to allow IT staff to concentrate on more valued activities. Nevertheless, control should still reside within the organisation’s IT department. In this way, collaboration should involve mutual training, education, and assistance throughout the relationship so that in-house staff skills do increase.

As a consequence, outsourcing could actually benefit in-house technical staff and management as keeping abreast of products, solutions and risk management techniques can be daunting for most IT departments. While a company may appear prepared “on the surface”, the quality of a service is never tested until it is needed.

As a consequence, outsourcing could actually benefit in-house technical staff and management as keeping abreast of products, solutions and risk management techniques can be daunting for most IT departments. While a company may appear prepared ‘on the surface’, the quality of a service is never tested until it is needed.

CONCLUSION

Security – no longer just a peripheral technology - is becoming a critical enabler of business continuity and is directly linked to the survivability of an organisation. Furthermore, in this time of heightened regulatory and compliance responsibility, most companies find themselves under scrutiny by government agencies, clients or third-party business partners. As firms renew contracts, more and more they are coming across language about security practices included, plus requests for statements of policy, practice and technology strategy. At the very least, an organization needs to;

- Develop a holistic security policy taking into account future business needs. Begin to develop a roadmap of how you can integrate security into all elements of the technology and the business processes.
- Determine the level of security you want to dedicate to each asset based on the value it brings to the organisation. Ensure the resources are in place for internal checks and make the completion of this part of measurable objectives. Explore new ways to impact the bottom line either through productivity gains or revenue enhancement by weaving rather than layering security into the new initiatives.

- Decide whether you have the resources and skills internally to implement and manage security and if not, determine whether a partner can help.

While security priorities may have been visualized as “surrounding” the enterprise in armour in the past, it is actually in its extension where the true opportunities lie. Again, the first wave of e-business euphoria brought with it seemingly limitless possibilities. Yet, rationalism has caused many to tread more cautiously in this brave new environment. Without question, opportunities under the banner of the e-business mindset still exist but the march forward fundamentally requires an organization to protect the interests of all parties involved. Those enterprises that find the right balance will spearhead the next wave of growth; after all, it is difficult to gain market share by cost cutting alone.

About the Research

IDC conducts enterprise and consumer surveys globally on a continuous basis. Support data for this document was drawn from IDC's infrastructure survey conducted in the latter part of 2002. A total of 419 interviews were completed in Germany, France, Italy, the Nordics and the UK. All of the respondents were individuals responsible for IT within the organization they represented. The organizations were selected to provide a balanced perspective across countries, industries and size. Within each country and industry, companies were selected to provide a representative sample across the spectrum of company sizes so as to avoid skewing the results of the other categories. The In-Focus sections were drawn from in-depth interviews with organisations provided by Steria. The interviews were conducted by IDC with the key decision-maker on the implementation of specific security solutions in the first quarter of 2003.

About Steria (www.steria.com)

With 2002 revenue of €1.018bn and more than 8,000 employees, Steria is one of the top ten IT services companies in Europe. Present in 12 countries worldwide, the Group is positioned as an end-to-end IT services operator within its three core businesses: consulting, systems integration and managed services.

Its acknowledged expertise in managing large-scale projects and its range of industrialised solutions in Europe enable Steria to offer its customers a reliable service with commitment to cost and risk control. The Group has strong sector-based expertise in the Public Sector, Banking and Insurance, Manufacturing/Utilities/Transport and Telecommunications markets. Created in 1969, the Steria group is a pioneer in employee shareholding, with 31% of its capital being held by employees. Steria is listed on the Premier Marché of the Paris Stock Exchange and in the SBF 120 index.

In order to help European companies and government agencies to meet their security challenges, Steria proposes an **end-to-end security offer**, including consulting (with several hundred dedicated European consultants), systems integration and managed services in five areas: physical access control, secure infrastructures, secure on-line services and messaging systems, secure document management and inter-community exchanges.

Steria has managed major security projects in Europe and established, for example, a close partnership with La Poste in France via Imelios, a subsidiary specialising in electronic exchanges and information exchange security.

About IDC (www.idc.com)

IDC is the foremost global market intelligence and advisory firm helping clients gain insight into technology and e-business trends to develop sound business strategies. Using a combination of rigorous primary research, in-depth analysis, and client interaction, IDC forecasts worldwide markets and trends to deliver dependable service and client advice. More than 700 analysts in 43 countries provide global research with local content. IDC's customers comprise the world's leading IT suppliers, IT organizations, e-business companies, and the financial community.

IDC is a division of IDG, the world's leading IT media, research and exposition company. All product and company names may be trademarks or registered trademarks of their respective holders. Additional information can be found at www.idc.com.

COPYRIGHT NOTICE

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2003 IDC. Reproduction without written permission is completely forbidden.