February 2002 was not exactly a great month for capital-hungry entrepreneurs. The dot.com bubble had burst, driving away most of the funds specialised in high-risk finance. The days of burgeoning investment in high-tech start-ups had come and gone, and the founders of SecurityXperts needed a large amount of money to offer a competitive service in the final stage of their project: computer security outsourcing.

Joaquín Castillejo, general manager, was aware of the opportunity in the market due to the lack of specialised personnel in the field of professional security services. However, they faced many uncertainties.

**A WEEK IN THE LIFE OF A SECURITY MANAGER**

It was still dark when Juanjo Márquez dragged himself out of bed to start another day. Back to the nightmare that had been plaguing him for a week. Going over the previous days while he showered, he felt a mixture of panic and powerlessness. He was tired of the CEO’s stern face when he reminded him that it would be difficult to make this year’s sales budget, and warning about the potential consequences for investment plans, particularly IT. Juanjo had spent most of the year trying to convince the CEO that, by himself, he could not plug all the holes that arose on a daily basis. Once again, his request for funds to install an IDS (Intrusion Detection System), which would enhance the company’s security, had been turned down.1

Juanjo Márquez was head of security at the mid-sized Spanish company (400 employees, 10 billion in sales). Formerly head of systems, he had been given the additional responsibility for security following a number of events that had highlighted the need for someone specialised in computer security. The biggest event was when an intruder had hacked into the company network and stolen the client database, including full details of their business dealings with the company. What was surprising was that, instead of the latest and most sophisticated tools, the thief had had used an effective low-tech method: “social engineering”2: someone claiming to be from the IT Department had called José Salazar, a clerk in the Billing Department: “Hi, I'm calling from IT. We have a problem with your account that is pulling the network down. Could you log out and give me your user name and password so I can log in and fix it?” Salazar, who was preoccupied with the monthly close, complied without question.

---

1 An IDS monitors server or network logs and warns of potential intrusions/attacks in real time. There are two types of IDS: those which monitor suspicious activity on the host (HIDS - Host Intrusion Detection System) and those which monitor the network in search of signs of an attack, not necessarily aimed at the computer on which they are installed (NIDS - Network Intrusion Detection System).

2 Colleagues described legendary hacker Kevin Mitnick as "technologically incompetent". However, he is considered to be one of the greatest hackers of all time because of his mastery of "social engineering", i.e. the use of deceit and trickery to get access data (user names and passwords)
It only took the attacker a few minutes to log in and install a Trojan (a hidden programme under remote control) on Salazar's hard disk, enabling him to fully control the computer from any other computer connected to the Internet. When it was discovered that Salazar's machine had been used to send a compressed file containing all customer data, with all related financial information, the CEO nearly had a heart attack.

Following the incident, which became common knowledge among the company's best customers, the CEO decided to take action. The reprimand to the IT Department for failing to detect the Trojan called attention to a new problem whose future implications were unknown.

The letter from the Data Protection Agency to the legal department also had a salutary effect. It informed the company that it was under investigation, with risk of penalty, for breach of the law on protecting personal data. This was the result of a disgruntled ex-employee's plan to attack the company on an unguarded flank: he had registered his wife's name on the web site, which was proving very successful as a means of collecting data for online marketing campaigns, and had been outsourced to a specialised company. The personal data protection law grants individuals the right to access their personal data to modify or delete it, or object to it being processed (e.g. to object to receiving promotional mail). Aware of the company's ignorance in this area, the ex-employee sent a letter in his wife's name asking for access to the data in order to modify it (specifically, her address). When the letter arrived, nobody knew which department was in charge, so it languished in somebody's in-tray in the IT Department, while the legal deadline for responding came and went.

The ex-employee just had to wait until after the deadline and then file a complaint with the Data Protection Agency for violation of rights and for use of data without permission (online marketing campaigns). He had the satisfaction of hearing from ex-colleagues about the CFO's shock on hearing the amount of the fine.

Márquez inherited all these problems when he took charge of the company's security policy. The policy, which had been written in the past based on vague notions about the data protection legislation, had not been revised or adapted to the rigorous legislation on data protection. Obviously, it had not been communicated to the company's employees in the appropriate manner.

Márquez was not very comfortable in his new job. Although over ten years' experience as a systems engineer was an excellent qualification for the job, his specific knowledge of security was confined to a 30-hour course which the company had paid for. He was keenly aware of his new job's complexities: it filled him with a mixture of shock and awe, and he occupied a post of strategic importance in the company. Also, although he knew that only a small fraction of security incidents ever lead to complaints (see Figure 1), there was always the possibility of a leak to the media, which would impair the company's image.

---

3 The hidden programme acts as a server, obeying orders from a client on another computer; it can be used to register keystrokes, delete or edit files, launch attacks on other machines, etc.

4 Spain's Organic Law 5/92, dated 29 October, on the Automated Processing of Data, was repealed and replaced by Organic Law 15/99, dated 13 December, on the Protection of Personal Data.
To start with, there were a number of underlying problems: he was not an expert on each and every system and device in the company’s very heterogeneous architecture. No matter how up-to-date he managed to stay by means of bulletins on the latest security patches (many of them provided by the manufacturers themselves), he was unable to apply all the updates without compromising configurations that were essential to running the company’s applications correctly. Moreover, how many vulnerabilities were being exploited without the manufacturers’ knowledge? Vulnerabilities were not always publicised immediately; in fact, before the solution was released there was a time lag that could be exploited by any professional hacker.

He also had serious doubts about the security of some of his applications: he was particularly concerned about the application running his main web site, which was housed on the company’s web servers. The site design and programming had been outsourced since the company did not have staff specialised in web programming languages and for reasons of cost. However, the ASP\(^5\), which managed the data base of registered users did not offer much reassurance as regards security: the outsourcer, a well-known digital communications company, gave priority to design, page download speed and usability over security. Márquez had read in one of the bulletins that most attacks took advantage of errors (bugs) in application programming, particularly in validating data entered by users, and that any professional hacker could easily exploit them.

Another source of worry was that Márquez was directly responsible for the protection of personal data in the company. His most recent meeting with the Legal Dept. had made it quite clear that they didn’t have a clue about this area and, to make matters worse, the law’s technical complexity made it necessary to have a multidisciplinary team (technical and legal), which the company did not have; moreover, the previous fine imposed by the Data Protection Agency left little room for optimism.

There was also another important factor: hackers are no longer pimple-faced teenagers "messing around" in their bedrooms (see Figures 2 and 3). Intruders are increasingly professional and there is a black market in intrusion services, with a flourishing range of industrial espionage techniques.

\(^{5}\) Active Server Pages, Microsoft proprietary technology for data base programming. Not to be confused with Application Service Provider, a company that provides a number of remote services.
FIGURE 2
FROM THE GREAT HACKERS ...

Relative Technical Complexity


Hacking Tools
self-replicating code
exploiting known vulnerabilities
back doors
password cracking
sniffer/sweepers
stealth diagnostics
packet forging/spoofing
GUI

Average Intruder
password guessing
disabling audits

Source: GAO Report to Congress, 1998

FIGURE 3
... TO THE SCRIPT KIDDIES

Relative Technical Complexity

1998 1999 2000 2001

Hacking Tools
Windows Remote Control
Trinoo
DDoS Insertion Tools
Melissa
PrettyPark
Stacheldraht

Kiddie Scripter

Source: GAO Report to Congress, 2001
Márquez's day-to-day work included analysing server and firewall logs, applying the latest security patches, solving technical problem in his area, and overseeing internal and external data traffic, which included acting as a watchdog of user activities.

This was one of the things that Márquez hated most: that most users in the company looked on him as a form of "big brother". But there had been more than one occasion where it had proved useful. He still remembered the case of Javier Molina, a young intern who tried to get revenge on Marcos Bermúdez, HR Manager, because he was not going to be hired at the end of his internship. One of Márquez's first decisions as head of security had been to install an application on the proxy server that handled the company's internet access to examine content using keywords and prevent access to sites which company policy considered to be inappropriate. Molina prepared his revenge carefully: aware of Bermúdez's love of good wine, he sent him an e-mail purportedly from eventos@elvino.com as bait to get Bermúdez to read the message: it contained some lines of HTML code with links to inappropriate sites such as www.pedophiles.net, www.teensex.net and www.wildorgies.com.

The system on the proxy server alerted Márquez to the existence of those addresses in Bermúdez's mail account. Fortunately, Márquez checked the code of the e-mail and discovered that the addresses were not in the original mail and that it had been sent from a false address, avoiding some embarrassment for Bermúdez and Márquez himself.

The system under his responsibility included 12 Exchange servers and another 12 Microsoft IIS servers, the corporate firewall, 15 Solaris servers, the company's CRM system and ten application servers running Windows NT and Windows 2000. The mixture of systems was standard at the company, which had postponed the decision about implementing an ERP system until the economic crisis had receded.

Computer security managers do not have much free time. The day is a succession of problems, most of them due to lack of user training. For this reason, at the Management Committee meetings, Márquez insisted on the importance of system security training for end users. The most advanced technology is useless if users are careless with their passwords or open a malicious mail attachment.

Meanwhile, the day had got off to a good start. No user had called in any last-minute "emergencies" (e.g. problems with changing a toner cartridge or complaints about Windows 98 incompatibilities with the latest peer-to-peer programme for music sharing). Carlos Fernández, Deputy Purchasing Manager, had repeatedly been asked to explain a flood of data at his workstation. This was quite unusual for him as he did not normally use any of the internet-based specialised marketplaces. Once again, Márquez thought that the lack of control was due to the absence of a duly documented security policy, so that sporadic reprimands were futile for bringing wayward users into line.

He began to read his e-mail. Apart from a few new user registrations in the commercial network, the rest were daily bulletins about vulnerabilities discovered in applications and operating systems. "Damn!", he thought, "Bloody Microsoft!" A vulnerability had just been discovered by which an attacker could use an e-mail or web site to access a system and erase the data used to encrypt other data, such as e-mails. He would have to download the latest patch and configure Internet Explorer to defend against such attacks. He was not overjoyed with the system of constantly having to apply security patches to operating systems and applications; of course it was necessary in order to preserve corporate security, but patches occasionally caused problems with other applications, forcing him to put in endless hours of overtime on weekends so as not to impair user productivity during the week.

The next bulletin was no more reassuring: another Exchange server security hole had been discovered: "Incorrect handling of Exchange server annexes can execute a script containing

---

6 A proxy server acts as an intermediary between the end user and the Internet; it routes and optimises traffic in both directions, but it also filters content and monitors where users browse.
malicious code." "This is serious, he thought. He quickly downloaded the patch and installed it. However, just moments later, when he checked the performance of the other application servers, he discovered that the CRM application had stopped! He suddenly remembered the time someone had entered the mail servers and, in an attempt to erase his trail, had knocked out three other servers ... They had spent three days (and nights) checking all the corporate information in the backups to check whether any of the data had been modified. And they never found out who had broken in, or what they had taken ... It was a really professional job, but at least the incident had been a wake-up call for the company, forcing it to focus on security for the first time. "Just like 9-11", he thought. "People only understand the need for contingency and recovery plans after a disaster has happened." Likewise, on that occasion, the company set aside a small part of its IT budget to create a security manager position, which fell to him more for reasons of "affinity" than because of his qualifications.

"In 20 minutes I'll have all the sales reps on my back over the CRM," he thought. His anxiety mounted when another bulletin reported no less than seven new vulnerabilities in Microsoft Telnet for Windows 2000. That meant that the outside access to the company could be exploited at any time by someone who was aware of the vulnerability. His work was piling up, and he had to begin to assign priorities, as they had told him in that course on "stress management".

The next call set the priority for him: "Juanjo, what's wrong with the CRM?" It was a sales representative just about to go into a meeting with a customer: "I've got a meeting in ten minutes with one of our best customers and I urgently need to see our return on them in the last few months. What's the matter? Do we have connection problems again?"

"I'm working on it," replied Juanjo. "I hope to have it fixed shortly. I'll confirm to you by e-mail as soon as it's fixed", muttered Márquez, his resolve failing. He knew it was a matter of more than just ten minutes, but he needed to buy time before the big bosses came down on him.

Another bulletin saying that the patch he had just installed on the Exchange servers had a "regression error" which, in turn, would have to be patched. This was beginning to look like something out of the Marx brothers ("The party of the first part ...."). He felt a sharp pain in his temple, the sort he got in situations of extreme stress. He heaved a sigh and tried to relax: "I had an idea the first patch was to blame for the CRM problem, and this bulletin just confirms my suspicions." However, he wasn't so sure that "patching the patch" would solve the CRM problems.

An old college friend, who is in charge of security at a bank, called to warn him about the latest hole in Outlook Express, the mail client installed on all the company's desktop and laptop computers. "Juanjo", said his friend, "with this hole, the user doesn't have to execute the attachment in order to be infected with a virus: just the message header is enough to trigger the code".

Márquez was already aware of the latest generation of viruses, designed to exploit vulnerabilities and, therefore, knock out the majority of users. Though they had a service for the automatic update of virus definitions supplied by a major antivirus company, the vulnerabilities required the immediate installation of the corresponding patch, making it necessary to reconfigure every single desktop and laptop. And although a new tool enabled all the desktop machines to be updated remotely, he would still have to talk to all the laptop users to plug the gap as soon as possible.

Thinking of laptops reminded him that he had an appointment with Luis Perales, head of marketing, to get a full explanation of the recent robbery of the latter's laptop computer. At least he had time to get a cup of coffee before the meeting with Perales. "What a day!", he thought. Resisting a feeling of pessimism, he pulled himself together and headed for the meeting with the marketing manager.

Perales received him after a short wait:

—Good morning, Mr. Perales. Thank you for making the time to see me.
—Don’t mention it, Juanjo. You know I am a great admirer of your work. And, please call me Luis.

—OK, Luis. I heard you lost your laptop. How did it happen?

—Well. I was on my way home from work when I remembered that my wife had asked me to buy some cleaning materials. When I got back to the car with the items, the laptop was gone.

—Where did you leave it, Luis?

—On the passenger seat. In fact, they didn’t damage the car at all: I must have forgotten to lock it.

—Luis, you know you should always leave the laptop in the trunk when you’re travelling, don’t you?

—Yes, but it was a bit of a pain on such a short trip. After all, I was just going home...

—Did you have anything confidential on the laptop?

—No, I don’t think so. Nothing important. Well, now that you mention it: a spreadsheet with data for a 100 million euro bid we are preparing for an electric company.

—I presume the data was encrypted.
—Ehhh... no.

—But, didn’t you have an encryption programme to protect that sort of sensitive information? You know that’s one of our recommendations.

—Of course, but it’s a bit complicated to use. To be frank: I was afraid I’d screw up and not be able to decode the information later.

—Didn’t you put a backup copy on the company server, as required?

—The fact is I find it much more convenient to handle the information on my hard disk. Sometimes it takes too long to get the information off the server.

—Well, at least you had a password to start up the computer and another to access the hard disk.

—Yeah, something like that.

—What do you mean?

—I set it to log in automatically; I have too many passwords to remember.

—Luis, does that mean you did the same with your passwords for remote access to the company server and the virtual private network?

—Good God no! That would be stupid! But I must admit I keep the whole slew of passwords in a Word file on my laptop.

—I hope that file was hidden, at least?

—No, it’s called “Passwords” and I keep it in “My Documents”.

—And what passwords do you keep in that file?
—Ehhh... all of them, of course: the one for remote access, the virtual private network, my mail account, and the HAL server access.

—You mean HAL where we keep all the company’s confidential information?

—I’m afraid so.

—it’s a good thing that access to HAL requires a token with a digital certificate. You’ve got it, haven’t you?

—Oh! It was in the laptop case. I kept it there just in case I forgot.

—You’ve got to be kidding! And when you called the Help Desk this morning to change your passwords, did you follow the standards in creating new ones?

—What do you mean?

—You know: passwords must be at least eight characters long; you must use at least one upper case and one lower case character, a number and a special character [& % $ · " ^ * ]; and the resulting word must not be in any dictionary.

—I just used the names of my wife and kids. They’re easy to remember; I just can’t manage so many passwords! I kept them on the hard drive so I would know which one went with each account. By the way, Juanjo, what did you mean about changing the passwords in case of danger?

—You know a password has to be changed every 60 days and immediately if you become aware that someone else may know it. Because of the robbery yesterday, first thing this morning you should have changed the passwords that the Help Desk gave you for others that only you know.

—Well, Juanjo, the fact is ... the laptop wasn’t stolen yesterday. It was two weeks ago, but I was so busy with the new marketing campaign that I didn’t have time to call the Help Desk or change my passwords. I should have, shouldn’t I?

—You certainly should have, Luis. By the way, why did you take so long to report the robbery?

—I imagined you would have more important things to do and I didn’t want to bother you.

—OK Luis, that’s all. I hope this has nothing to do with the news item I read this morning. Apparently the competition got the contract because they undercut us by 10,000 euro. Don’t you think the robbery of your laptop might be connected?

Márquez was almost dizzy as he left the meeting. He felt powerless; while he was fighting for a bigger security budget, most of the staff disregarded the most basic security precautions. He would insist on this issue at the next management committee meeting, but he wasn’t very optimistic.

On the way back, he noticed the staff in Accounts had their user names and passwords stuck to their monitors on Post-it notes. They never learn. It was becoming increasingly urgent to get senior management to take a stand. Back at his desk, he was afraid to check his mail for fear of even worse news. Just as he feared: another urgent bulletin (“Please! No! Not on Friday afternoon!” he implored) reported another security fault in the SQL servers, the ones that manage the company’s data bases; it brought back memories of past dangers. It was clear that he would have to break the promise to his wife about a quiet Sunday in the country.
On arriving home, he thought about the Sales Manager’s rude call demanding that he fix the CRM, and informing him of how much money the company was losing for every day it was down. And the headache throbbed on, immune to the pills he had taken during the day. Fortunately, it was Friday and, although he was going to have to work all weekend, at least he had two days ahead to solve the problem without any impertinent phone calls.

Halfway through Saturday afternoon, after reviewing the server configurations one by one, he discovered that, as suspected, the first patch was what had hung up the CRM. "So", he said to himself, "the patch is clearly incompatible with the CRM. If I remove the patch, the CRM should work, but the company will be open to a hacker attack". While trying to decide what to do, he started going through the over 300 mail messages in his inbox in the vain hope that he might find time to answer them all. Some of them reminded him of other urgent problems such as the one with Microsoft Telnet. Nevertheless, after checking the documentation, he concluded that the problem did not affect his systems; he heaved a huge sigh of relief.

He decided to postpone the decision about the CRM. Now it was more important to patch the SQL servers. First, he installed the latest version and spent three hours checking that all the data bases worked with the patch installed.

At last, a piece of good news! All the data bases were working normally. This gave him the courage to tackle the CRM problem. After all, it was nice to work without the day-to-day pressure; his headache was gone and he could think clearly. This, of course, was after the (fully justified) reprimand from his wife, combined with complaints that he had turned into a workaholic.

He checked the latest Microsoft documentation to see what the "error" announced the day before actually consisted of. He saw that the first patch contained files that had not been updated and could be the cause of the problem with the CRM system; he installed the replacement patch and replaced some of the outdated files. Suddenly, with his habitual mixture of uncertainty and amazement, Márquez observed that the CRM was back on line! At least he could have Sunday off.

His joy was short-lived. The first news on Monday morning was that he had to install the latest service packs\(^{11}\) on the Windows 2000 servers, and they would interfere with the security patches he had installed over the weekend! In desperation, he began to consider the job offer as a gardener that his father-in-law had made a few months before.

Once again, he was overwhelmed by events. His agenda showed an appointment with the Legal Department to design an action plan for the process review required by the Data Protection Law. He just didn't have time to combine his responsibility for the company’s systems with the ongoing supervision a good security policy call for. Márquez realised he urgently needed outside help to design the right strategy and keep constant tabs on the company’s information flows.

**INDUSTRY SITUATION**

As companies become obliged to review their strategies in order to adapt to the needs of e-business, there is increasing concern about security at companies that are "open for business" on the internet. Developing and managing security requires a high degree of technical specialisation and enough time to ensure a sound, disciplined approach to this area. At the current speed of development in information technology, those two factors are scarce or non-existent. Consequently, many companies consider outsourcing part or all of their security infrastructure as one way of solving the problem.

By 2005, consultants such as IDC estimate that the Internet security market will be worth 6.5 billion euro, compared with 2.7 billion euro in 2002 (see Figure 4). Concern is growing (Fig. 5), and the number of incidents reported (Fig. 1), though grossly understated because of companies’ reluctance to publicise attacks they have suffered, leaves no doubts about the situation.
**FIGURE 4**

![Bar chart showing security costs over time](chart1.png)

Source: IDC. European Security Market (2001)

**FIGURE 5**

![Bar chart showing security angst ratings](chart2.png)

Security “Angst” Rating (1-10)

Source: IDC Survey N=12,000, Fall 2001, IDC #IS01j
In a much longer-term forecast, Gartner Group also projects a sharp increase in spending on IT protection. According to Gartner, in 2010 companies and governments will spend ten times more on security: 4% of their budget, up from 0.4% today. Gartner also estimates that, in 2003, 50% of SMEs using the Internet for anything other than e-mail will suffer successful attacks from the outside, such as web hacking and viruses.

In 2001, the FBI alone reported 525 million dollars in verifiable losses due to IT security breaches (more than double the previous year's figure). Accordingly, with ever more companies connected to the Internet and the proliferation of simple intrusion tools, those losses will continue to mount. Fear? It doesn't look like that: many network administrators, particularly at SMEs, are still reluctant to implement that most basic security precaution, a firewall.

For a long time, security has been addressed from the simplistic approach of protecting against data loss, which has done much to prevent companies from perceiving the real extent of the problem. The general feeling is that, after all, attacks are difficult (if not impossible) to avoid and, if there have been no attacks (or at least, none have been detected), then why worry? Why invest in preventing something that depends more on luck than on security?

This attitude is now a thing of the past thanks to growing concern for security and increasing legal requirements. More and more companies, particularly those involved in e-commerce, are realising that security is a critical factor in their marketing strategy. Concern for information privacy is now practically universal. Many studies show that one of the main obstacle to widespread use of online shopping is the perception of a lack of security when making transactions or supplying financial information. Therefore, more than a form of protecting against hypothetical threats, security now represents a global vision regarding the general approach to protecting information stored and transmitted via networks. Security needs to be addressed from a number of angles: technical, operational and legal.

SECURITYXPERTS: THE COMPANY

When Joaquín Castillejo began to understand the complexities of networks, Spain was still in the pre-Internet age. In 1988, online contact between people interested in computer security was confined to the legendary BBSs (Bulletin Board System), the precursors of modern-day forums and chat rooms. A large number of BBSs was grouped into Fidonet, an amateur equivalent to the Internet, which was not open to normal users at the time. Fido was a network of BBSs (nodes) that was founded in 1984 and consisted of thousands of aficionados of online communications throughout the world, who provided access to a range of services free of charge; message areas (forums) were the most prominent of these services. Castillejo had been a sysop (system operator) of a BBS specialised in security matters, and it was through the BBS that he came to know some of the people with whom he would later found SecurityXperts.

As an intern in the computer centre of Madrid's Polytechnic University, he had perfected his knowledge of computer security that he had acquired as a sysop. The experience in the computer centre taught him about larger networks and, in 1990, he was exploring the Internet (pre-web) when it was only accessible in terminal mode and was the domain of a few collectors of FTP sites. While at university, Castillejo organised numerous meetings and talks about computer security within the annual Art Futura event.

Computer security was beginning to create a buzz, at least in certain circles. By 1993-4, the media were referring to him as an expert in the field. As an intern at the computer centre, he was recommended for a job at Telefónica Sistemas as a specialist in network security to design Spain's first Internet network. The first specific security products, both hardware and software, were beginning to appear, and Castillejo was one of the first beta testers.
In the first half of the 1990s, security basically consisted of usernames and passwords, which could be circumvented quite easily; it was not difficult to access most UNIX systems using the default username and password (guest/guest). Then the first firewall solutions began to appear, such as firewall toolkit (FWTK) by Marcus J. Ranum, giving birth to a burgeoning industry.

Poor security continued to be the norm in the second half of the 1990s, and the gradual shift to e-business took place without the appropriate security. The first news reports began to appear about security failures and intrusions in company systems (the Citibank robbery, the Morris worm, the AT&T system crash, etc.).

Until 1995, Castillejo was in charge of developing and implementing security solutions. At the end of 1995, he transferred to Telefónica Transmisión de Datos where, among other functions, he was in charge of supervising the security of the network designed in the previous stage, thus continuing his specialisation in IP network security. Subsequently, he became part of the network and services team, providing specialist advice on the launch of such networks as Infovía and Infovía Plus.

In 1999, he decided to make a change. He transferred to the Marketing Department, where he was in charge of developing various information security services. In that period he began to detect numerous opportunities in the security market in Spain, where a new era was beginning in which it was not enough to be defensive about security: now, a constantly pro-active approach was required. Looking at the US, he observed that 20% of US companies outsource their security (see Figure 6).

**FIGURE 6**

![Graph showing outsourcing intentions](source: CG&EY. Intention to outsource ICT services (2001))

**DESCRIPTION OF THE BUSINESS OPPORTUNITY**

Organisations today are under considerable pressure:

- on the one hand, the need to improve profitability and generate new business opportunities through the intensive use of information and communication technology (ICT), by opening up to employees, customers, partners and suppliers;
on the other hand, the need to improve their bottom line, involving major pressure to cut costs and concentrate on key value-creating activities.

The big business opportunities are accompanied by similarly large risks. Successfully seizing these opportunities means having to respond to growing challenges related to protecting one's information assets:

- increased complexity of information systems and security mechanisms;
- attacks that are increasing in number and sophistication;
- consumers' growing awareness about questions of privacy, which is generating a demanding regulatory environment in the area of privacy (e.g. the Data Protection Law).

However, IT system risk management poses major difficulties for organisations:

- sizeable investment in products and services, whereas security budgets continue to be tight, but they are growing (5%-10% of total ITC budgets - see Figures 6, 7, 8 and 9);
- in particular, prohibitive labour costs involved in maintaining security in-house; scant in-house know-how; specialist resources which are hard to find, with high levels of turnover and demanding needs for ongoing training.

As a result, organisations are steadily outsourcing to specialised providers (>22% in 2001). Consequently, the computer security services market is booming (27% CAGR 01-02) and will grow from 220 million euro in 2002 to over 650 million euro in 2006 (Fig. 7).

**FIGURE 7**

**COMPUTER SECURITY IN SPAIN**

![Computer Security in Spain](image-url)
FIGURE 8
SECURITY SERVICES IN SPAIN

Million euro

2001 2002 2003 2004 2005 2006

- Consulting
- Implementation
- Management and maintenance
- Training

FIGURE 9
OUTSOURCED FIREWALL MANAGEMENT (SPAIN)
CONCLUSION

Is the growing concern about security justified? Is this a new form of outsourcing? Is the market ripe for SecurityXperts? To what extent do companies see internal security management as core business? How important are non-technological factors in an organisation’s security? What is the significance of security in business in terms of return on investment? (see Fig. 8).
EXHIBIT 1

% that have suffered

- Virus: 95% in Financial Sector
- Unauth Use
- Denial of Service: 54% detected after the fact or not at all
- Unauth Modification: 43% in Public Sector
- Web Vandalism


EXHIBIT 2

Worldwide Spending

$ Billions

2001 2002 2003 2004 2005 2006

0 20 40 60 80 100 120 140 160

Hardware

Software

Services

18.2% 20.6% 17.5%

Source: IDC 2002, IT Security/Business Continuity Market Model V2.1
EXHIBIT 3

Threats of the Web

I.D & Credit Card Theft  
Cookies & Web Bugs  
Advertisers & Spammers  
Web Site Logs  
Monitoring by your boss or ISP  
Malicious Code  
Hackers & Cyberstalkers  
Banner Ads & Popups

visited websites

Source: www.anonymizer.com

EXHIBIT 4
WHERE ATTACKS COME FROM

Attacks from the internal network
Attacks from the internet
Negligent or malicious use
Viruses or Trojans
Faults in the PC
Direct attacks from outside
## INTERNAL DEVELOPMENT

### ROI CASE

#### Minimum scenario (8 x 5h support)

<table>
<thead>
<tr>
<th>Professional services (external)</th>
<th>Year 1</th>
<th>Following years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consultancy</td>
<td>14,400</td>
<td>14,400</td>
</tr>
<tr>
<td>Audit</td>
<td>14,400</td>
<td>14,400</td>
</tr>
<tr>
<td>Implementation &amp; integration</td>
<td>7,200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HW/SW platforms</th>
<th>Year 1</th>
<th>Following years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management software</td>
<td>15,000</td>
<td></td>
</tr>
<tr>
<td>Management server</td>
<td>15,000</td>
<td></td>
</tr>
<tr>
<td>Communications equipment</td>
<td>3,000</td>
<td></td>
</tr>
<tr>
<td>Management console</td>
<td>1,500</td>
<td></td>
</tr>
<tr>
<td>HW/SW maintenance</td>
<td>6,900</td>
<td>6,900</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Human resources (internal)</th>
<th>Year 1</th>
<th>Following years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security specialist</td>
<td>64,909</td>
<td>64,909</td>
</tr>
</tbody>
</table>

| Total                             | 142,309| 86,209          |

#### Standard scenario (round-the-clock)

<table>
<thead>
<tr>
<th>Professional services (external)</th>
<th>Year 1</th>
<th>Following years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consultancy</td>
<td>14,400</td>
<td>14,400</td>
</tr>
<tr>
<td>Audit</td>
<td>14,400</td>
<td>14,400</td>
</tr>
<tr>
<td>Implementation &amp; integration</td>
<td>7,200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HW/SW platforms</th>
<th>Year 1</th>
<th>Following years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management software</td>
<td>15,000</td>
<td></td>
</tr>
<tr>
<td>Management server</td>
<td>15,000</td>
<td></td>
</tr>
<tr>
<td>Communications equipment</td>
<td>3,000</td>
<td></td>
</tr>
<tr>
<td>Management consoles</td>
<td>6,000</td>
<td></td>
</tr>
<tr>
<td>HW/SW maintenance</td>
<td>6,900</td>
<td>6,900</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Human resources (internal)</th>
<th>Year 1</th>
<th>Following years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security manager</td>
<td>64,909</td>
<td>64,909</td>
</tr>
<tr>
<td>Security operators</td>
<td>162,273</td>
<td>162,273</td>
</tr>
</tbody>
</table>

| Total                             | 309,082| 248,482         |
### MANAGED SECURITY SERVICE PROVIDER (MSSP)

<table>
<thead>
<tr>
<th>Management &amp; maintenance</th>
<th>Year 1</th>
<th>Following years</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Professional services</strong></td>
<td>Cost</td>
<td>Cost</td>
</tr>
<tr>
<td>Consultancy</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Implementation &amp; integration</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td><strong>Subscription of managed services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscription of firewall services</td>
<td>6,000</td>
<td></td>
</tr>
<tr>
<td>Subscription of other services (web server)</td>
<td>6,000</td>
<td></td>
</tr>
<tr>
<td>Subscription of e-mail/proxy services (antivirus)</td>
<td>6,000</td>
<td></td>
</tr>
<tr>
<td><strong>Recurring services (Year 1)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recurring firewall services</td>
<td>18,000</td>
<td>18,000</td>
</tr>
<tr>
<td>Other recurring services</td>
<td>18,000</td>
<td>18,000</td>
</tr>
<tr>
<td>Recurring e-mail/proxy services</td>
<td>18,000</td>
<td>18,000</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>72,000</td>
<td>54,000</td>
</tr>
</tbody>
</table>

### Management & maintenance + round-the-clock response

<table>
<thead>
<tr>
<th>Management &amp; maintenance + round-the-clock response</th>
<th>Year 1</th>
<th>Following years</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Professional services</strong></td>
<td>Cost</td>
<td>Cost</td>
</tr>
<tr>
<td>Consultancy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation &amp; integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Subscription of managed services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscription of firewall services</td>
<td>6,000</td>
<td></td>
</tr>
<tr>
<td>Subscription of other services (web server)</td>
<td>6,000</td>
<td></td>
</tr>
<tr>
<td>Subscription of e-mail/proxy services (antivirus)</td>
<td>6,000</td>
<td></td>
</tr>
<tr>
<td>Subscription of intruder detection (added for level 2)</td>
<td>6,000</td>
<td></td>
</tr>
<tr>
<td><strong>Recurring services (Year 1)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recurring firewall services</td>
<td>18,000</td>
<td>18,000</td>
</tr>
<tr>
<td>Round-the-clock option</td>
<td>8,000</td>
<td>8,000</td>
</tr>
<tr>
<td>Other recurring services</td>
<td>18,000</td>
<td>18,000</td>
</tr>
<tr>
<td>Round-the-clock option</td>
<td>8,000</td>
<td>8,000</td>
</tr>
<tr>
<td>Recurring e-mail/proxy services</td>
<td>18,000</td>
<td>18,000</td>
</tr>
<tr>
<td>Round-the-clock option</td>
<td>8,000</td>
<td>8,000</td>
</tr>
<tr>
<td>Recurring hacking detectors</td>
<td>18,000</td>
<td>18,000</td>
</tr>
<tr>
<td>Round-the-clock option</td>
<td>8,000</td>
<td>8,000</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>128,000</td>
<td>104,000</td>
</tr>
</tbody>
</table>
### Case

#### Costs

<table>
<thead>
<tr>
<th></th>
<th>Internal</th>
<th>MSSP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Year 1</td>
<td>Following years</td>
</tr>
<tr>
<td>8 x 5h supervision</td>
<td>142,309</td>
<td>86,209</td>
</tr>
<tr>
<td>Round-the-clock supervision</td>
<td>309,083</td>
<td>248,483</td>
</tr>
</tbody>
</table>

#### Savings

<table>
<thead>
<tr>
<th></th>
<th>8 x 5h supervision</th>
<th>Round-the-clock supervision</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>49%</td>
<td>59%</td>
</tr>
</tbody>
</table>

#### Total costs in 3 years

<table>
<thead>
<tr>
<th></th>
<th>Internal</th>
<th>MSSP</th>
<th>% of saving of MSSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 x 5h supervision</td>
<td>314,728</td>
<td>180,000</td>
<td>43%</td>
</tr>
<tr>
<td>Round-the-clock supervision</td>
<td>806,048</td>
<td>336,000</td>
<td>58%</td>
</tr>
</tbody>
</table>